

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 1 de 17
		Vigente desde: 27/08/2019	

Informe de Auditoría Interna

**Sistema de Gestión de Seguridad de la Información - SGSI
Proceso Direccionamiento de las Tecnologías y las Comunicaciones - DTIC**

Vigencia 2020

Bogotá, D.C., 12/11/2021

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 2 de 17
		Vigente desde: 27/08/2019	

TABLA DE CONTENIDO

INTRODUCCIÓN	3
1. Objetivo de la Auditoría:.....	3
2. Alcance de la Auditoría:	3
3. Criterio(s) de la Auditoría:	3
4. Resultados de la Auditoría:.....	3
4.1. Hallazgos y/o No Conformidad	15
5. Fortalezas y Recomendaciones:.....	15
5.1. Fortalezas	15
5.2. Recomendaciones.....	16
6. Conclusiones:	16
Anexo 1. Cuadro Consolidado de Hallazgos y/o No Conformidades	17

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 3 de 17
		Vigente desde: 27/08/2019	

INTRODUCCIÓN

La Oficina de Control Interno, con base en el programa anual de auditorías año 2021 aprobado por el Comité Institucional de Coordinación del Sistema de Control Interno, determinó realizar la Auditoría Interna al Sistema de Gestión de la Seguridad de la Información – SGSI.

Por lo anterior, con el presente informe se da a conocer los resultados de dicha auditoría interna basados en el análisis y la evaluación objetiva de la información suministrada por los auditados, en donde se determinó el grado de cumplimiento de los criterios establecidos en el Plan de auditoría, describiéndose las fortalezas y formulando recomendaciones para la implementación de acciones que conlleven a la mejora continua del Sistema.

1. Objetivo de la Auditoría:

Determinar el grado de cumplimiento del Sistema de Gestión de Seguridad de la Información de la Personería de Bogotá D.C., frente a la normatividad vigente y a los lineamientos establecidos por la entidad.

2. Alcance de la Auditoría:

Verificar el Sistema de Gestión de Seguridad de la Información de la Personería de Bogotá D.C., en todos sus componentes a la vigencia 2020.

3. Criterio(s) de la Auditoría:

- Normatividad legal vigente
- Normas y documentos al interior de la Personería de Bogotá D.C.
- Caracterización del Proceso Dirección de Tecnologías de la Información y las Comunicaciones
- Requisitos de la organización, legales, cliente y las partes interesadas
- Documentación del Sistema de Gestión de Seguridad de la Información de la Personería de Bogotá

4. Resultados de la Auditoría:

La Personería de Bogotá D.C., implementó el Sistema de Gestión de Seguridad de la Información – SGSI y estableció su alcance para todos los procesos, con el

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 4 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

propósito de garantizar y mejorar la seguridad de la información, para lo cual evaluó los riesgos e implemento controles de conformidad con el Modelo Integrado de Planeación y Gestión MIPG. En virtud de la Resolución 406 de 2020 de la Personería de Bogotá D.C., en especial el “ARTÍCULO 6. *“Composición del Modelo Integrado de Planeación y Gestión – MIPG”*: El Modelo Integrado de Planeación y Gestión –MIPG, está compuesto por siete (7) dimensiones operativas y cuatro (4) sistemas de gestión a saber...” Y su “Parágrafo 1. *Cada dimensión operativa del Modelo Integrado de Planeación y Gestión – MIPG- se desarrolla a través de una o varias políticas de gestión y desempeño institucional señaladas por la normatividad vigente.*” De lo anterior, la presente auditoría está enmarcada por la tercera Dimensión del MIPG: Gestión con valores para resultados a través de las políticas Gobierno Digital y Seguridad Digital.

Metodología

La presente auditoría se desarrolló de manera remota, conforme al Plan de Auditoría allegado en su oportunidad. Se realizó la solicitud de información pertinente a la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, a través de cuestionarios remitidos con memorandos, correos y entrevista, los cuales fueron diligenciados en su totalidad y se aportaron las evidencias que corroboraron el cumplimiento de los criterios definidos para la auditoría.

A continuación, se presentan los resultados obtenidos en el proceso de auditoría, las fortalezas, recomendaciones, hallazgos y/o no conformidades y conclusiones para la mejora continua del mismo.

POLÍTICA GOBIERNO DIGITAL

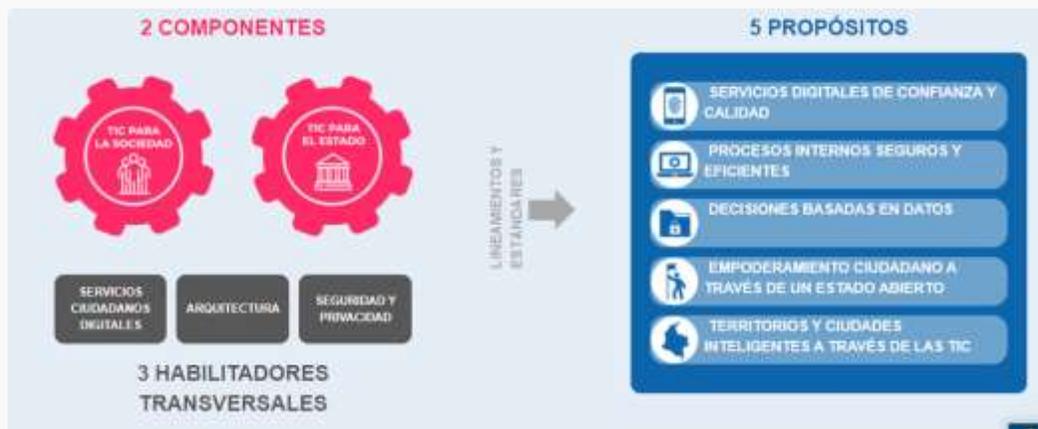
Para el MIPG, Gobierno Digital es la política que busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones - TIC, con el fin de consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

En este sentido, para la implementación de la Política de Gobierno Digital, se han definido dos componentes y tres habilitadores transversales que determinan lineamientos y estándares para el desarrollo de servicios digitales de confianza y calidad, procesos digitales seguros y eficientes, datos e información de calidad para tomar decisiones, promoción de la apropiación de la tecnología para empoderar al ciudadano.

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 5 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

El siguiente esquema muestra los componentes y habilitadores transversales y cómo su articulación permite alcanzar los propósitos de la política, los cuales sirvieron de base para el desarrollo de la presente auditoría en cuanto a la política de Gobierno Digital.



Fuente: Manual de Gobierno Digital Min-TIC Versión 6, 2018.

Componentes de la Política de Gobierno Digital:

En cuanto a la relación con el estado desde el año 2020 la Personería de Bogotá cuenta con un sistema de gestión electrónica de documentos (SIRIUS), ha realizado fortalecimiento y desarrollo al sistema de información Misional SINPROC, ha renovado los portales institucionales, adoptó una herramienta para la gestión del Sistema de Gestión de la Calidad (ISOLUCION). La entidad apropió las herramientas en línea de trabajo colaborativo y mantuvo las certificaciones de Calidad y de Seguridad y Salud en el trabajo, adicionalmente, se encuentra trabajando en los aplicativos del Distrito de BogData y Si capital y desarrollando el OCDI Módulo de Control Interno Disciplinario y la Web Service con la Registraduría Nacional.

En lo relacionado con la sociedad, la Personería de Bogotá pone a disposición de ciudadanos y entidades diversos servicios, medios y acceso a la información de su actividad misional para su aprovechamiento por parte de sus grupos de interés, como son la sección transparencia, portales institucionales, expedición de Antecedentes en línea, informes de Rendición de Cuentas transmitidos en vivo, Tutelas en línea, Conciweb, WhatsApp Institucional, Requerimientos ciudadanos, actividades a través de redes sociales, con el fin de fomentar la participación y el uso de medios electrónicos y virtuales.

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 6 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

Habilitadores transversales de la Política de Gobierno Digital:

En lo relacionado con el habilitador transversal Arquitectura, a través del entendimiento de los procesos misionales se logra identificar los proyectos estratégicos que, apoyados en tecnologías de la información, aportan para la consecución de los objetivos institucionales. . A la fecha, por medio del ejercicio de arquitectura empresarial se identificó la necesidad de realizar la sistematización del Proceso Disciplinario en su primera fase, durante la presente vigencia se está realizando entrevista de entendimiento a los procesos.

Para lo concerniente al habilitador transversal de seguridad de la información, mediante el desarrollo e implementación de las metas y entregables establecidos en el Modelo de Seguridad y Privacidad de la Información de MINTIC y la adecuada gestión de riesgos de seguridad de la información, acorde con lo establecido en la Guía de Administración de Riesgo de la Personería de Bogotá, D.C., la Dirección DTIC, implementa controles de seguridad con el fin de mitigar los riesgos que puedan afectar la disponibilidad, integridad y confidencialidad de la información administrada por el proceso Direccionamiento TIC, tales como:

- Implementación de seguridad perimetral (Firewall de red, firewall de aplicaciones web, herramienta de gestión de eventos de seguridad)
- Ejecución de copias de respaldo de datos, servidores y servicios administrados por el proceso Direccionamiento TIC.
- Implementación de servicio de nube office 365.
- Herramienta de antivirus en equipos de cómputo y servidores de la entidad.
- Implementación de VPN para conectividad remota a la red institucional.
- Implementación de políticas y procedimientos de seguridad de la información.

Por último, para el habilitador transversal de servicios ciudadanos, la Personería de Bogotá ha desarrollado e impulsado servicios como el de Audiencia Virtual de Conciliaciones, expedición de antecedentes en línea, Tutelas/impugnación/desacatos en línea, portales web, chat institucional, formulario electrónico de PQRS, Formulario Express Línea 143, solicitud de certificaciones contractuales de manera no presencial, expedición de antecedentes en línea.

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 7 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

Ejecución de la Política de Gobierno Digital:

Mediante la Resolución 406 se establece en su *ARTÍCULO 22: Responsables de los Sistemas de Gestión*, al Director de Tecnologías de la Información y las Comunicaciones como responsable del Sistema de Gestión de Seguridad de la Información - SGSI. Quien como líder de la adopción e implementación de la Política de Gobierno Digital coordina, gestiona y ejecuta los recursos técnicos y humanos que le permiten llevar a cabo los proyectos estratégicos de tecnología más relevantes para la entidad por medios del Plan Estratégico de Tecnologías de la Información - PETI y el cual se actualiza anualmente.

Dentro de las iniciativas para el mejoramiento de la provisión de servicios digitales de confianza y calidad, el fortalecimiento de las capacidades de gestión de tecnologías de la información en la entidad, y la toma de decisiones basadas en datos se encuentran:

- Sistematización del Proceso Disciplinario fase I
- Fortalecimiento del sistema de información Misional SINPROC
- Expedición en línea del certificado de Antecedentes Disciplinarios con validación de datos de la Registraduría Nacional
- Actualización del ejercicio de arquitectura empresarial par la vigencia 2021
- Optimización de la infraestructura tecnológica
- Adopción del Sistema de Gestión de Documentos Electrónicos – SIRIUS
- Adquisición de licencias de Power BI para la creación de tableros de control, que permitirán consolidar y analizar información en tiempo real.

La Entidad viene implementando un modelo de Gobierno de TI que permite la adopción de las mejores prácticas en la gestión de proyectos. Así mismo, a partir de la actual vigencia se adoptó una metodología de gestión de proyectos PMO con el fin garantizar la adecuada gestión de los recursos humanos y técnicos y se desarrolla una matriz de canvas para cada uno de los proyectos en el cual se identifican los patrocinadores, interesados y propietarios y beneficiarios de los proyectos.

De igual manera, para el levantamiento de requerimientos funcionales, pruebas y puesta en producción, este se realiza con el feedback de los usuarios líderes del proyecto o desarrollo. Adicionalmente se inició la proyección de la nueva estrategia de uso y apropiación de la Personería de Bogotá con el apoyo del proveedor Forsecurity, y el entendimiento de la gestión del cambio para alinearla con los nuevos proyectos a desarrollar.

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 8 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

La Dirección TIC está liderando para la actual vigencia la actualización de la Arquitectura Empresarial para plasmar la arquitectura actual, la de transición y la arquitectura futura sobre el nuevo modelo presentado por MinTIC, identificando las brechas de TI y la definición de proyectos estratégicos que apoyen el cumplimiento de los objetivos institucionales.

El proceso direccionamiento TIC como responsable del Sistema de Gestión de Seguridad de la Información, ha adoptado estrategias para la implementación del modelo de seguridad y privacidad de la información, las cuales involucran aspectos claves como el compromiso de la alta de la dirección, asignación de recursos, fortalecimiento de la infraestructura tecnológica, contratación de consultorías externas, designación y capacitación de personal propio para el desarrollo de las actividades y elaboración de productos entregables que hacen parte de las fases del MSPI (planes, guías, procedimientos, formatos, políticas, etc.) en concordancia con la norma ISO 27001 de 2013.

De igual manera, la entidad cuenta con una serie de canales y medios de prestación de servicios no presenciales, seguros y eficientes que apoyan al ciudadano en la protección de sus derechos. Servicios como Tutelas en línea, expedición Antecedentes disciplinarios, solicitudes de conciliaciones en línea, Línea 143.

El Plan Estratégico de Tecnologías de la información – PETI de la Personería de Bogotá para la vigencia 2021 fue presentado y aprobado en el mes de enero 2021 por parte del Comité Institucional de Gestión y Desempeño y se incluyó dentro del Plan Estratégico Institucional – PEI en la siguiente meta estratégica:

"4. Fortalecer la gestión institucional a través del uso y apropiación de tecnologías de la información y las comunicaciones, la aplicación de buenas prácticas, un Talento Humano y una infraestructura adecuados para la prestación del servicio."

Para la medición del Sistema de Gestión de Seguridad de la Información - SGSI, se cuenta con tres (3) indicadores, a los cuales se les realiza el seguimiento periódico correspondiente:

- Indicador de Tratamiento de eventos de Seguridad de la Información
- Indicador de cumplimiento del Plan de Comunicación, Sensibilización y Capacitación del SGSI
- Indicador de porcentaje de actividades ejecutadas de acuerdo con el plan de seguridad de la información

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 9 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

En la gestión de la información con relación a los dominios a la fecha se está realizando la actualización del ejercicio de Arquitectura Empresarial liderado por la Dirección TIC, incluyendo el entendimiento de los procesos, sus necesidades, gestión del cambio, uso y apropiación, definición de la arquitectura actual y futura.

De otra parte, a través del PETI se contempla la proyección de la estrategia de uso y apropiación el cual incluye la medición del impacto de los proyectos de TI.

POLÍTICA DE SEGURIDAD DIGITAL



En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

El Manual de Políticas de Seguridad de la Información 03-MN-01 V.6 de la Personería de Bogotá D.C., determina un conjunto de políticas y lineamientos acordes a los requisitos de la norma NTC-ISO-IEC 27001 de 2013, para el uso adecuado de la información institucional y de los recursos y servicios tecnológicos que la soportan, que se constituyen en la base para el diseño y ejecución de procedimientos, protocolos, controles y en general el desarrollo de las actividades diarias de los funcionarios(as) y contratistas y personas que interactúen con la información institucional; y tiene como objetivo establecer las políticas de seguridad de la información para la entidad, con el fin de cumplir con los requisitos

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 10 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

de seguridad, definidos en un SGSI (Sistema de Gestión de Seguridad de la Información) y el MSPI, (Modelo de Seguridad y Privacidad de la Información) de la política de Gobierno Digital, que ayudarán mediante su implementación a preservar la confidencialidad, integridad y disponibilidad de la información en la Entidad.

Sobre los principios del Sistema de Gestión de Seguridad de la Información – SGSI, se evidencia los diferentes mecanismos que se han implementado en la entidad para lograr el cumplimiento de la normatividad en materia de seguridad de la información, tales como:

- Documento Manual de Políticas de Seguridad de la Información
- Procedimiento de Seguridad de la Información:
- Procedimiento de Gestión de Usuarios
- Guía para la identificación y valoración de activos de información
- Matriz de Inventarios de Activos de Información
- Guía de Administración del Riesgo
- Mapa de Riesgos Institucional
- Formato de registro de eventos e incidentes de seguridad de la información
- Formato Reporte de Incidentes - CSIRT Gobierno V3
- Plan de Seguridad y Privacidad del SGSI
- Plan de comunicación, sensibilización y capacitación del SGSI
- Plan de Seguimiento y Revisión del SGSI

Al igual se constató el fortalecimiento de la cultura de la seguridad de la información a través de las actividades desarrolladas en el Plan de Comunicación, sensibilización y capacitación del SGSI, con el fin de mantener informados y capacitados a los funcionarios y contratistas de la Personería de Bogotá para el adecuado manejo de la información institucional y la prevención de los riesgos existentes para la seguridad de la información y los datos personales.

Es de anotar, que, si bien es cierto, la Entidad cuenta con la Matriz de Riesgos Institucional, se considera pertinente por parte de la DTIC, como responsable del SGSI, gestionar una Matriz propia para la respectiva administración de los riesgos de la seguridad de la información.

En cuanto a los objetivos estratégicos de la Personería de Bogotá D.C., estos se encuentran alineados con los objetivos de seguridad de la información. De igual manera se constata que con la definición de los roles y privilegios se refuerza la

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 11 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

gestión para la atención a todos los requerimientos relacionados con la Seguridad de Información.

La Entidad cuenta con el Manual de Políticas de Seguridad de la Información que permite implementar los mecanismos para salvaguardar la información contenida y transmitida mediante el uso de dispositivos móviles a quienes se les autoriza el acceso a los recursos tecnológicos de la Entidad. Se corroboró lo anterior con el servicio de almacenamiento en la nube de Office 365, y la definición de roles y privilegios de usuario que protegen la información contra la pérdida de disponibilidad y acceso no autorizado, atendiendo principalmente los eventos de pérdida o robo de los dispositivos móviles e inactivando los usuarios que se retiran de la Institución.

En el cumplimiento de mantener la confidencialidad de la información de los funcionarios y contratistas que ingresan a la Entidad, la Dirección DTIC solicitó a la Dirección de Talento Humano la implementación y uso del formato de confidencialidad para funcionarios y contratistas y la actualización del procedimiento 8-PT-23 Vinculación de Servidores(as) - V2; sin embargo, se considera pertinente por parte de la DTIC, como responsable del SGSI, gestionar con la Dirección de Talento Humano y la Subdirección de Gestión Contractual, acciones que refuercen la utilización del Formato de Confidencialidad de la información al momento del ingreso de funcionarios y contratistas, con el fin de reforzar y salvaguardar la seguridad de la información.

Respecto a la manera se salvaguardar los activos de información que son devueltos de funcionarios y contratistas por retiro definitivo, cambio de puesto de trabajo de la entidad, suspensión y/o finalización del contrato, es responsabilidad de cada Proceso, realizar los protocolos de entrega de los activos de información de acuerdo con los procedimientos establecidos.

La Personería cuenta con el servicio de almacenamiento en la nube de office 365 para que se mantenga la información institucional en estos repositorios, de tal manera que se proporcionen las medidas de seguridad, respaldo y disponibilidad requeridas.

Para el uso y administración de medios informáticos removibles, la entidad cuenta con protocolos, procedimientos o acciones implementadas, a través de la herramienta de antivirus para la protección de la información almacenada y el servicio de almacenamiento en la nube de Office 365, con el fin de que se mantengan copias de la información institucional; reforzando dicha medida con la implementación de controles de seguridad perimetral como firewall de red, y firewall de aplicaciones, y el servicio de antivirus se protege la información

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 12 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

institucional contenida en medio removibles, contra los riesgos por ataques informáticos y malware y/o virus informáticos que puedan afectar la seguridad de la información.

En cuanto a la Política de Control de Acceso, se evidencia que la trazabilidad de las acciones ejecutadas para llevar a cabo el acceso a los activos de información se realiza mediante la recolección de los logs de eventos que se registran en los sistemas de información y que presentan los datos de auditoría relevantes sobre el acceso y las acciones realizadas en los sistemas. Y para garantizar que los usuarios o perfiles de usuario sean habilitados o eliminados, mediante el cumplimiento del procedimiento gestión de usuarios, se manejan las diferentes novedades de usuarios (creación, eliminación, actualización). Para usuarios contratistas la fecha de terminación de contrato queda registrada en el sistema como fecha de caducidad de la cuenta, inactivándose automáticamente al cumplirse la fecha registrada. Por último, en cuanto a los mecanismos de cifrado de la información, la Entidad hace uso de herramientas gratuitas normalmente utilizadas en el mercado como winzip, 7-Zip, WinRAR, entre otras.

En el marco de la Política de Seguridad Física y del Entorno, las áreas destinadas al procesamiento o almacenamiento de información sensible se encuentran aseguradas y con acceso restringido, mediante:

- El bloqueo automático de la sesión de trabajo de los equipos de cómputo, parametrizada a través del controlador de dominio de la red.
- A través de la sensibilización permanente mediante tips de seguridad enviados a los usuarios por medios de comunicación institucionales.
- Con la asignación de puestos de trabajo con gabinetes seguros en los cuales se puede guardar la información.

En lo relacionado con la operación y administración de la información institucional, esta se realiza a través de los procedimientos de:

- Procedimiento de gestión de usuarios
- Procedimiento de ingreso a centros de cómputo
- Procedimiento de Gestión de cambios
- Procedimiento de Backups
- Procedimiento de desarrollo de aplicaciones

En lo concerniente a las medidas conducentes a garantizar la protección contra códigos maliciosos, estas están dadas mediante la administración de la herramienta de antivirus, adicionalmente se cuenta con el servicio de soporte de una firma contratista quien realiza las actividades de soporte y mantenimiento de

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 13 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

segundo nivel sobre dicha herramienta. La entidad cuenta con el software de antivirus McAfee debidamente licenciado, el cual posee una consola de administración mediante la cual se despliegan y monitorea el estado de instalación del software de antivirus en los equipos de la Personería.

En lo referente a la realización de pruebas de restauración, la entidad no cuenta con ambientes especiales para esta actividad, sin embargo, se valida el correcto funcionamiento cuando se requiere la recuperación de alguna información y por los diferentes logs del aplicativo que realiza la copia donde se verifica el resultado del backup.

El mecanismo para la instalación de Software autorizado en los equipos que hacen parte de la estructura tecnológica de la entidad se gestiona a través de mesa de ayuda dispuesta en la intranet o correo electrónico dirigido a la dirección DTIC. Dicha instalación de software se realiza por personal del grupo de soporte de la dirección DTIC autorizado que cuenta con roles y privilegios de administrador. Si la solicitud de instalación proviene de una dependencia diferente a la dirección DTIC, se valida que el software cumpla con los requisitos de seguridad mínimos en términos técnicos y legales, en caso de determinar la viabilidad de uso del software se procede a autorizar la solicitud y el personal de soporte se encarga de la instalación del software.

Referente a las revisiones periódicas de las vulneraciones y debilidades técnicas de los sistemas de información y estructura tecnológica, se realizan actividades de análisis de vulnerabilidades y hacking ético a los sistemas de información e infraestructura tecnológica.

Para gestionar los mecanismos y controles sobre la prestación del servicio de redes de datos y comunicaciones, la Entidad cuenta con lineamientos de seguridad en las Políticas de Teletrabajo y Trabajo en Casa, y la Política de Controles en la Red de Datos y Transferencia de Información relacionadas con el acceso remoto a la red institucional de la Personería. El acceso remoto a los equipos conectados a la red institucional se realiza a través del servicio de VPN, el cual establece un túnel seguro mediante conexión de internet, lo que garantiza la transferencia de información cifrada. De igual manera los administradores de equipos y servicios de TI cuentan con roles y privilegios de acceso especiales que permiten la operación segura de los equipos para mayor control de la seguridad. De otra parte, se ha implementado el protocolo de comunicaciones HTTPS en aplicaciones web publicadas en internet que garantizan el tráfico seguro de información, el Firewall de red y firewall de aplicaciones WEB, ubicados en datacenter del nivel central y en nube de azure para proteger el tráfico de la información a través de la red y entre aplicaciones web, la herramienta de antivirus para proteger equipos de cómputo y servidores de las amenazas de malware, el

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 14 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

servicio de almacenamiento en la nube de office 365 y Oracle y se cuenta con servicios en la nube de Oracle y de Azure, para garantizar la disponibilidad y canal de conectividad redundante.

Dentro de la Política de Controles en la red de datos y transferencia de información se establece la prohibición de utilizar el correo electrónico personal, para el envío y recepción de información institucional clasificada, reservada o sensible. De otra parte, el servicio de acceso a internet para las tareas propias de la función desarrollada en la Personería de Bogotá se controla a través del firewall perimetral, cada funcionario tiene diferentes permisos de acceso a internet según el rol establecido (Directivos, prensa, permisos especiales y usuarios normales).

Para los proyectos de adquisición o desarrollo de nuevos sistemas de información, el responsable del SGSI vincula al personal del grupo de seguridad de la Dirección DTIC y se tienen en cuenta los requisitos de seguridad establecidos en los estándares de desarrollo seguro y buenas prácticas de TI, generalmente aceptadas internacionalmente, y se incluyen en los anexos técnicos de los pliegos de condiciones de los contratos a realizar.

Los principios de confidencialidad, integridad y disponibilidad de la información se preservan en la relación con los proveedores mediante la suscripción de contratos y acuerdos de confidencialidad y no divulgación de la información.

Para asegurar la continuidad del negocio se realiza el análisis, identificación y evaluación de los riesgos de seguridad de la información y se definen las acciones de tratamiento correspondientes para cada proceso, acorde con lo establecido en la Guía para la Administración del Riesgo de la Personería D.C

Para el cumplimiento de requisitos legales y contractuales relacionados con la seguridad de la información:

- Se cuenta con un formato de acuerdo de confidencialidad el cual debe ser diligenciado por las partes interesadas.
- Existe la aprobación y divulgación permanente de la Política de derechos de propiedad intelectual, antipiratería y antifraude.
- Se imparten instrucciones al personal de soporte para la identificación y desinstalación de software no autorizado en equipos de cómputo de la Personería.
- Se cuenta con un control de acceso y descargas de internet a través del firewall perimetral, cada funcionario tiene diferentes permisos de acceso a

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 15 de 17
		Vigente desde: 27/08/2019	

4. Resultados de la Auditoría:

internet según el rol establecido (Directivos, prensa, permisos especiales y usuarios normales)

Respecto a las revisiones de seguridad de la información, estas se realizan a través de:

- La evaluación de la efectividad de controles
- El seguimiento periódico a la ejecución de los planes del SGSI.
- La actualización periódica de los documentos del SGSI.
- Ejecución de auditorías al SGSI
- La medición y seguimiento de los indicadores del SGSI
- La revisión periódica de las valoraciones de riesgos

Por último, para el buen uso de los datos personales, la entidad cuenta con la Política de Protección de Datos Personales y la implementación de textos en los formularios de los aplicativos SINPROC y Portal Web, donde se le informa al petionario sobre la protección de datos personales Ley 1581 de 2012.

4.1. Hallazgos y/o No Conformidad

Durante el proceso de auditoría interna no se presentaron No Conformidades.

5. Fortalezas y Recomendaciones:

5.1. Fortalezas

- Compromiso, disponibilidad y profesionalismo por parte del responsable del Sistema y su equipo de trabajo en la realización de la auditoría interna.

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 16 de 17
		Vigente desde: 27/08/2019	

5. Fortalezas y Recomendaciones:

- Se cuenta con un ambiente propicio y un alto nivel en las competencias funcionales, lo que conlleva a la optimización de las diferentes actividades del Sistema.
- Apropiación de las herramientas existentes en la Entidad, garantizando el cumplimiento de los objetivos de la seguridad de la información.

5.2. Recomendaciones

- Gestionar una Matriz propia para la respectiva administración de los riesgos de la seguridad de la información, por parte de la DTIC, como responsable del SGSI.
- Gestionar con la Dirección de Talento Humano y la Subdirección de Gestión Contractual, acciones que fortalezcan la utilización del Formato de Confidencialidad de la información al momento del ingreso de funcionarios y contratistas, con el fin de reforzar y salvaguardar la seguridad de la información, por parte de la DTIC, como responsable del SGSI.
- Reforzar el SGSI con el fin de dar continuidad al cumplimiento de las políticas y lineamientos establecidos por MinTIC para el logro de la Certificación de la Norma ISO:27001.

6. Conclusiones:

- Una vez realizada la auditoría al Sistema de Gestión de Seguridad de la Información, se evidenció que cumple con la normatividad vigente y los lineamientos establecidos en la Personería de Bogotá D.C. y cuenta con un avance del 60% en el desarrollo de los autodiagnósticos.
- Para obtener los resultados esperados, son aspectos vitales garantizar la confidencialidad, la integridad y la disponibilidad de los activos de información, y lograr el compromiso de todos los integrantes de la Entidad con el SGSI.
- El obtener la certificación en ISO 27001 le daría un valor público a la Entidad, generando mayor confianza a las partes interesadas y ayudando

PERSONERÍA DE BOGOTÁ, D. C.	FORMATO INFORME DE AUDITORÍA	Código: 16-FR-06	
		Versión: 11	Página: 17 de 17
		Vigente desde: 27/08/2019	

6. Conclusiones:

a disminuir la probabilidad de ocurrencia de incidentes que generen grandes pérdidas para la Personería.

Anexo 1. Cuadro Consolidado de Hallazgos y/o No Conformidades

Ítem	CRITERIO DE AUDITORÍA	HALLAZGO Y/O NO CONFORMIDAD	RIESGO IDENTIFICADO

EQUIPO AUDITOR

Firma:

Sandra P. Camargo R.

Nombre: Sandra Patricia Camargo Rodríguez
Empleo: Profesional Especializado 222-05 (E)

Firma:

[Firma manuscrita]

Nombre: Pedro Hernando Caicedo Barrero
Empleo: Profesional Universitario 219-01

APROBÓ

Firma:

[Firma manuscrita]

Nombre: Sandra Milena Cáceres González
Empleo: Jefe Oficina de Control Interno (E)