

SECRETARÍA JURÍDICA DISTRITAL

OFICINA DE CONTROL INTERNO

TEMA : SEGUNDO SEGUIMIENTO A LOS 114 CONTROLES DE SEGURIDAD DE LA INFORMACIÓN CON CORTE A 30 DE NOVIEMBRE DE 2019

CONTROL	DESCRIPCIÓN DE LA EVIDENCIA	UBICACIÓN	CONTROLES IMPLEMENTADOS	CONTROLES NO IMPLEMENTADOS
1.Conjunto de políticas para la seguridad de la información	Se encuentran descritas en el manual de Políticas de Seguridad de la Información y Protección de Datos, el cual debe ser aprobado por la Dirección.	Están publicadas en la WEB http://www.secretariajuridica.gov.co/transparencia/planeacion/politicas-lineamientos-y-manuales/manual-politicas-seguridad-la-informacion	SI	
2. Revisión de las políticas para la seguridad de la información	Se revisan y se actualizaron el el Manual de Seguridad de la Información y Protección de Datos Personales CREACIÓN DE POLÍTICAS	Actualización del Manual de Seguridad de la Información y Protección de Datos Personales	SI	
3.Asignación de responsabilidades para la segur. de la información	6. Políticas y Lineamientos de Seguridad de la Información 6.1.2. Roles y responsabilidades	Página 21,30,33,37 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
4.Segregación de tareas.	No se definió, por tareas sino por perfiles de los aplicativos	Para los Sistemas de Información Misionales existe la Resolución 104 de 2018 http://sisjur.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=81226	SI	
5.Contacto con las autoridades.	6.1.2 Contacto con las autoridades	Se encuentra definido en el manual numeral 6.1.2 Contacto con las autoridades página 21.	SI	
6.Contacto con grupos de interés especial.	6.1.3 Contactos con grupo de interés especial	Se encuentra definido en el manual numeral 6.1.3 Contacto con grupos de interés social página 22.	SI	
7.Seguridad de la información en la gestión de proyectos.	6.1.3 Seguridad de la información en gestión de proyectos	Página 22 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
8. Política de uso de dispositivos para movilidad.	6.1.4 Política de Dispositivos Móviles	Página 23 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
9. Teletrabajo	Se realizaron las inspecciones técnicas	Se anexan las evidencias del trabajo realizado por los Ingenieros quienes realizaron las visitas técnicas a los diferentes sitios de vivienda de los funcionarios que realizarán teletrabajo.	SI	
10.Investigación de antecedentes.	7. Seguridad de los Recursos Humanos 7.1.1 Selección de personal	Página 23 - 25 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
11. Términos y condiciones de contratación.	7.1.2. Términos y condiciones Laborales	Página 24 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
12.Responsabilidades de la Dirección	La Dirección además de aprobar la política, el manual, contrató un Oficial de seguridad,	Contratación de un Oficial de Seguridad	SI	
13.Concienciación, educación y capacitación en seguridad de la información.	7.13. Durante la ejecución del Empleo - Entrenamiento, concientización y capacitación Se han realizado dos capacitaciones sobre seguridad de la información a los funcionarios de la entidad y se envían mensualmente tipos de seguridad.	Página 24 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
14.Proceso disciplinario.	7.1.5. Proceso disciplinario	Página 25 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
15.Cese o cambio de puesto de trabajo	7.1.4. Política de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios y personal provisto por terceros .	Página 25 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
16. Inventario de activos.	8. GESTIÓN DE ACTIVOS	https://secretariajuridica.gov.co/content/ru%C3%ADa-registro-y-la-clasificaci%C3%B3n-activos-informaci%C3%B3n	SI	
17. Propiedad de los activos.	Propiedad de los Activos	https://secretariajuridica.gov.co/content/ru%C3%ADa-registro-y-la-clasificaci%C3%B3n-activos-informaci%C3%B3n	SI	
18. Uso aceptable de los activos.	8.1 Política uso aceptable de activos	https://secretariajuridica.gov.co/content/ru%C3%ADa-registro-y-la-clasificaci%C3%B3n-activos-informaci%C3%B3n	SI	
19.Devolución de activos.	8.5.1. Devolución de los Activos	Página 39 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	

20. Directrices de clasificación	8.6. Clasificación de la Información	Página 39 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad., existe un procedimiento Registro de activos de Información e Índice de Información clasificada y reservada https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-PR-025%20Registro%20de%20Activos%20de%20Informaci%C3%B3n%20e%20%C3%8Dndice%20de%20Informaci%C3%B3n%20Clasificada%20y%20Reservada_V3.pdf y una Guía para el Registro y la Clasificación de Activos de Información https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-GS-001%20Gu%C3%ADA%20para%20el%20Registro%20y%20la%20Clasificaci%C3%B3n%20de%20Activos%20de%20Informaci%C3%B3n_V3.pdf y el acto Administrativo Resolución 30 de 2019 http://www.secretariajuridica.gov.co/sites/default/files/instrumentos_gestion_informacion/030-2019%20RESOLUCION%20Activos%20e%20indice.PDF	SI	
21. Etiquetado y manipulado de la información	8.6.2 Etiquetado y manejo de la información.	Página 39-40 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
22. Manipulación de activos.	En el aplicativo Smart existe un módulo donde se almacena la información de los Activos	http://10.80.50.100/SID/index.php?op=27&sop=27.5.18/la=6&li=1	SI	
23. Gestión de soportes extraíbles.	8.7.1. Gestión de Medios de Soporte - Almacenamiento	Página 41 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
24. Eliminación de soportes.	8.7.2. Borrado Seguro	Página 42 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
25. Soportes físicos en tránsito.	8.7.3 Medios Físicos en Tránsito	Página 42 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
26. Política de control de accesos.	11. Política de Control de Acceso	Página 67 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
27. Control de acceso a las redes y servicios asociados.	11.1.1. Acceso a redes y Servicios de Red	Página 67-69 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, además en el Directorio Activo se encuentra registrados todos los funcionarios y contratista de la entidad con sus respectivos permisos.	SI	
28. Gestión de altas/bajas en el registro de usuarios.	11.1.2 Gestión de Contraseñas para usuarios 11.1.4. Retiro de los derechos de acceso	Página 68-69 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, además en el Directorio Activo se encuentra registrados todos los funcionarios y contratista desde donde se realiza la activación e inactivación de usuarios.	SI	
29. Gestión de los derechos de acceso asignados a usuarios.	11.1.2. Gestión de Contraseñas para usuarios 11.1.2 Revisión de los derechos de acceso a usuarios	Página 68 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la página Institucional de la entidad, para los Sistemas de Información Misionales existe la Resolución 104 de 2018 http://sisjur.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=81226 , para la asignación de acceso a usuarios se implementó el procedimiento de Administración de Usuarios 2310200-PR-091 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-PR-091%20ADMINISTRACION%20DE%20USUARIOS.pdf , Creación de Cuentas de Usuario de Directorio Activo y Correo 2310200-IN-014 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-IN-014%20Creaci%C3%B3n%20de%20Cuentas%20de%20Usuario%20de%20Directorio%20Activo%20y%20Correo.pdf y además en el Directorio Activo se encuentra registrados todos los funcionarios y contratista de la entidad con sus respectivos permisos.	SI	
30. Gestión de los derechos de acceso con privilegios especiales. 9.2.2. Suministro Acceso a Usuarios	11.1.1. Control de Acceso a Redes y Servicios en Red 11.1.3. Revisión de los derechos de acceso de los Usuarios	Página 68 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad y además en el Directorio Activo se encuentra registrados todos los funcionarios y contratista de la entidad con sus respectivos permisos especiales de acceso a la <u>infraestructura</u> .	SI	
31. Gestión de información confidencial de autenticación de usuarios.	14.3. Política de paso de ambientes de desarrollo, pruebas y producción 16.1.1. Requisitos de seguridad de los sistemas de información	Página 75-76 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad además en el Directorio Activo se encuentra registrados todos los funcionarios y contratista de la entidad con sus respectivos permisos y claves. Página 81-82 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad además en el Directorio Activo se encuentra registrados todos los funcionarios y contratista de la entidad con sus respectivos permisos y claves.	SI	

32. Revisión de los derechos de acceso de los usuarios.	11.1.2 Revisión de los derechos de acceso a usuarios	Página 68 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
33. Retirada o adaptación de los derechos de acceso.	11.1.4. Retiro de los derechos de acceso	Página 69 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, para los Sistemas de Información Misionales existe la Resolución 104 de 2018 http://sisjur.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=81226 , para la asignación de acceso asignados a usuarios se implementó el procedimiento de Administración de Usuarios 2310200-PR-091 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-PR-091%20ADMINISTRACION%20DE%20USUARIOS.pdf , Creación de Cuentas de Usuario de Directorio Activo y Correo 2310200-IN-014 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-IN-014%20Creacion%20de%20Cuentas%20de%20Usuario%20de%20Directorio%20Activo%20y%20Correo.pdf y además en el Directorio Activo se encuentra registrados todos los funcionarios y contratista de la entidad con sus respectivos permisos.	SI	
34. Uso de información confidencial para la autenticación.	9.3.1. Uso de información Secreta.	Se encuentra definido en el manual página 38	SI	
35. Restricción del acceso a la información.	11.1.4. Retiro de los derechos de acceso	Página 68 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, además se le asignan roles y perfiles a los funcionarios de acuerdo con sus actividades que vaya a desempeñar en los Sistemas de Información de acuerdo con la Resolución 104 de 2018 http://sisjur.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=81226 , para la asignación de acceso asignados a usuarios se implementó el procedimiento de Administración de Usuarios 2310200-PR-091	SI	
36. Procedimientos seguros de inicio de sesión.	9.4. Control de Acceso y Aplicaciones.	Se encuentra definido en el manual página 39 Control de acceso y aplicaciones. Este control esta inmerso dentro de la restricción de acceso a la información tal como lo dice la norma, se controla al dar el ingreso a los sistemas y las aplicaciones con el ID definido por la Oficina de Tecnología de la Información y las Comunicaciones.	SI	
37. Gestión de contraseñas de usuarios.	11.1.2. Gestión de Contraseñas para usuarios	Página 68-69 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, para los Sistemas de Información Misionales existe la Resolución 104 de 2018 http://sisjur.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=81226 , para la asignación de acceso asignados a usuarios se implementó el procedimiento de Administración de Usuarios 2310200-PR-091 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-PR-091%20ADMINISTRACION%20DE%20USUARIOS.pdf , Creación de Cuentas de Usuario de Directorio Activo y Correo 2310200-IN-014 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-IN-014%20Creacion%20de%20Cuentas%20de%20Usuario%20de%20Directorio%20Activo%20y%20Correo.pdf y además en el Directorio Activo se encuentra registrados todos los funcionarios y contratista de la entidad con sus respectivos permisos.	SI	
38. Uso de herramientas de administración de sistemas.	8.5 Política de Recursos Tecnológicos	Página 38 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, además se cuenta con herramientas que permite medir la disponibilidad de servidores, bases de datos y servicios tecnológicos el cual se puede evidenciar con Métricas de Disponibilidad de Servicios de TI 2310200-GS-008 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-GS-008%20M%C3%A9tricas%20de%20Disponibilidad%20de%20Servicios%20de%20TI.pdf	SI	
39. Control de acceso al código fuente de los programas.	11.1.1 Controles de Acceso a Redes	Página 68 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
40. Política de uso de los controles criptográficos.	12.1 Controles Criptográficos	Página 69 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
41. Gestión de claves.	11.1.1 Controles de Acceso a Redes	Página 68 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
42. Perímetro de seguridad física. Seguridad física y ambiental	13.1.1. Seguridad física y del entorno	Página 70 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad y se cuenta con un Plan Ambiental 2019 https://secretariajuridica.gov.co/intranet/planeacion/subsistema-gest%C3%B3n-ambiental/plan-acc%C3%B3n-riega-2019	SI	

43. Controles físicos de entrada.	13.1.2 Controles de Acceso Físico	Página 71 del manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
44. Seguridad de oficinas, despachos y recursos.	13.1.2 Controles de Acceso Físico	Página 71 -73 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
45. Protección contra las amenazas externas y ambientales.	11.1.3 Protección Contra Amenazas Ambientales.	Se encuentra definido en el manual numeral 11.1.3 pagina 42	SI	
46. El trabajo en áreas seguras.	13.1.3. Ubicación y Protección	Página 71 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
47. Áreas de acceso público, carga y descarga.	13.1.2 Controles de Acceso Físico	Página 71 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
48. Emplazamiento y protección de equipos.	11.2 Ubicación y Protección de Equipos.	Se encuentra definido en el manual numeral 11.2 pagina 43	SI	
49. Instalaciones de suministro.	NO SE DEFINIO			NO
50. Seguridad del cableado.	11.1.1. Control de Acceso a Redes y Servicios en Red 15.1. Política de Gestión de Seguridad de las Redes	Página 67, 71, 81 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
51. Mantenimiento de los equipos.	8.5. Política de uso de Recursos Tecnológicos	Página 38 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
52. Salida de activos fuera de las dependencias de la empresa.	13.1.4. Seguridad de los equipos fuera de las instalaciones	Página 71 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
53. Seguridad de los equipos y activos fuera de las instalaciones.	13.1.4. Seguridad de los equipos fuera de las instalaciones	Página 71 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
54. Reutilización o retirada segura de dispositivos de almacenamiento.	8.7.1. Gestión de medios removibles 13.1.6 Retiro de Activos	Página 41,70 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
55. Equipo informático de usuario desatendido.	11.2.6. Política de escritorio y Pantalla limpia.	Se encuentra definido en el manual pagina 46. Esta Inmerso en la política de escritorio y pantalla limpia en horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar la información confidencial protegida bajo llave. Esto incluye: Documentos impresos, CD, dispositivos de almacenamiento USB y medios removibles en general.	SI	
56. Política de puesto de trabajo despejado y bloqueo de pantalla.	13.2 Política de escritorio despejado y pantalla despejada	Página 72 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
57. Documentación de procedimientos de operación.	22.1. Procedimientos de Operación Documentados	Se encuentra definido en el manual pagina 46	SI	
58. Gestión de cambios.	14.1. Gestión de Cambios	Página 73 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
59. Gestión de capacidades.	14.2. Gestión de Capacidad	Página 74 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
60. Separación de entornos de desarrollo, prueba y producción.	14.3. Paso de ambiente de Desarrollo, Ensayo y Operación.	Página 75 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
61. Controles contra código malicioso.	14.4 Protección contra Código Malicioso	Página 76 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
62. Copias de seguridad de la información.	14.5 política de Backups	Página 78 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, además se tiene un procedimiento de Administración de Backups y Restore 2310200-PR-046 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-PR-046%20ADMINISTRACION%20DE%20BACKUPS%20Y%20RESTORE%20V4.pdf y el Manual de Política de Copias de Seguridad y Recuperación 2310200-MA-002 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-MA-002%20Manual%20de%20Pol%C3%ADtica%20de%20Copias%20de%20Seguridad%20y%20Recuperaci%C3%B3n_V2.pdf	SI	
63. Registro y gestión de eventos de actividad.	14.6. Política de Auditoria 14.6.1 Registro de Eventos y Generar evidencia	Página 78-80 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	

64. Protección de los registros de información	14.6.2 Registro del administrador y del Operador	Página 80 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
65. Registros de actividad del administrador y operador del sistema.	14.6.2 Registro del administrador y del Operador	Página 80 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, además cada mes los responsables de la redes, bases de datos y servidores presentan informe del estado de las actividades y configuraciones realizadas en la infraestructura y sistemas.	SI	
66. Sincronización de relojes.	14.6.3 Sincronización de Relojes	Página 78 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
67. Instalación del software en sistemas de producción.	14.3. Política de paso de ambientes de desarrollo, pruebas y producción	Página 75-76 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
68. Gestión de las vulnerabilidades técnicas.	14.7. Política de Gestión de vulnerabilidades técnicas. En el aplicativo Smart existe un módulo en donde se registran los eventos	Página 80 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad. Módulo de Incidencias o vulnerabilidades en el SMART http://10.80.50.100/SJD/index.php?op=27&sop=27.4.1&la=5&li=1	SI	
69. Restricciones en la instalación de software.	8.5. Política de uso de Recursos Tecnológicos	Página 38 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
70. Controles de auditoría de los sistemas de información.	14.6. Política de Auditoría	Página 38 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
71. Controles de red.	11.1.1 Controles de Acceso a Redes	Página 65 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
72. Mecanismos de seguridad asociados a servicios en red.	15.1. Política de Gestión de Seguridad de las Redes	Página 78 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
73. Segregación de redes.	15.2 Separación de las Redes	Página 79 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
74. Políticas y procedimientos de intercambio de información.	Cumplimiento de los lineamientos de MINTIC y Alta Consejería Distrital de Tecnologías de la Información y las Comunicaciones - Secretaría General Alcaldía Mayor de Bogotá	Circular 32, 38 y 53 de 2018 Proceso de actualización del Sistema Distrital de Quejas y Soluciones Bogotá Te Escucha e interoperabilidad con Govimentum desde nuestro portal institucional estamos interoperando con Bogotá Te Escucha http://www.secretariajuridica.gov.co/ , además se realizó interoperabilidad entre SIGA y Bogotá Te Escucha la cual fue Notificada con Cumplimiento Nivel 3 por cumplir con los lineamientos de Lenguaje del Min TIC.	SI	
75. Acuerdos de intercambio.	Se construyeron los servicios de intercambio de información con las respectivas controles de acceso solo a la información requerida por SIGA.	Se desarrollaron servicios de intercambio de información entre la Secretaría Jurídica Distrital y la Secretaría General Mayor de Bogotá	SI	
76. Mensajería electrónica.	8.1. Política de uso de correo electrónico.	Página 25 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, una evidencia de este son los correos institucionales de los funcionarios de la entidad, entre estos el correo de notificacionesjudiciales@secretariajuridica.gov.co y contactenos@secretariajuridica.gov.co	SI	
77. acuerdos de confidencialidad y secreto.	Se envió el acuerdo de confidencialidad a Corporativa, para que se incorpore en el procedimiento de Contratación de Personal	Para la asignación de acceso a usuarios se implementó el procedimiento de Administración de Usuarios 2310200-PR-091, donde se estableció el formato Compromiso de Confidencialidad de Información 2310200-FT-268 para ser firmado por los funcionarios y contratistas al iniciar la vinculación o el contrato con la entidad http://smart.bogota.gov.co/SJD/portal/resultados_busqueda.php?proceso=3&opcion_regreso=0 , https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-PR-091%20ADMINISTRACION%20DE%20USUARIOS.pdf ,	SI	
78. Análisis y especificación de los requisitos de seguridad.	14.1.1. Análisis y Especificaciones de Requisitos de Seguridad de la Información.	Se encuentra definido en el manual pagina 58.	SI	

79. Seguridad de las comunicaciones en servicios accesibles por redes públicas.	8.2. Política de uso de Internet	Página 31 - 38 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
80. Protección de las transacciones por redes telemáticas.	14.1.3. Protección de Transacciones de Servicios de Aplicaciones.	Se encuentra definido en el manual pagina 58.	SI	
81. Política de desarrollo seguro software.	14.3. Política de paso de ambientes de desarrollo, pruebas y producción 16. Adquisición, Desarrollo y Mantenimiento de Sistemas	Página 75, 81 - 83 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
82. Procedimientos de control de cambios en los sistemas.	16.1.2. Procedimiento de Control de Cambios	Página 82 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, además se cuenta con el procedimiento Análisis, Diseño, Desarrollo e Implementación de Soluciones 2310200-PR-045%20An%C3%A1lisis%20Dis%20Desarrollo%20Implementaci%C3%B3n%20de%20Soluciones%20V3.pdf	SI	
83. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	14.1. Política gestión de cambios	Página 73 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
84. Restricciones a los cambios en los paquetes de software.	14.1. Política gestión de cambios 15.1.3. Desarrollo de Software contratado externamente	Página 73, 82 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
85. Uso de principios de ingeniería en protección de sistemas.	16.1. Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información 16.1.1. Requisitos de seguridad de los sistemas de información	Página 81-83 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
86. Seguridad en entornos de desarrollo.	14.3. Política de paso de ambientes de desarrollo, pruebas y producción 16. Adquisición, Desarrollo y Mantenimiento de Sistemas	Página 75, 81 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
87. Externalización del desarrollo de software.	16.1.3. Desarrollo de Software contratado externamente	Página 82 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
88. Pruebas de funcionalidad durante el desarrollo de los sistemas.	14.3. Política de paso de ambientes de desarrollo, pruebas y producción. Se elaboró un procedimiento de análisis, diseño e implementación de soluciones nuevas y existentes en la entidad.	Página 75 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad. Se cuenta con el procedimiento Análisis, Diseño, Desarrollo e Implementación de Soluciones 2310200-PR-045%20An%C3%A1lisis%20Dis%20Desarrollo%20Implementaci%C3%B3n%20de%20Soluciones%20V3.pdf	SI	

89. Pruebas de aceptación.	Se elaboró un procedimiento de análisis, diseño e implementación de soluciones nuevas y existentes en la entidad.	Página 75 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad. Se cuenta con el procedimiento Análisis, Diseño, Desarrollo e Implementación de Soluciones 2310200-PR-045 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-PR-045%20An%C3%A1lisis%20Dise%C3%B1o%20Desarrollo%20e%20Implementaci%C3%B3n%20de%20Soluciones%20V3.pdf	SI	
90. Protección de los datos en pruebas.		Este control esta inmerso en el control definido en pruebas de seguridad en los sistemas de información. - Pruebas de compatibilidad, se debe garantizar el funcionamiento adecuado y continuo del software desarrollado en diferentes plataformas hardware, sistemas operativos y redes. - Pruebas de integración: Se deben comprobar las conexiones y comunicaciones.	SI	
92. Política de seguridad de la información para suministradores.	17.1. Política de Seguridad de la Información con Proveedores	Página 83 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
92. Tratamiento del riesgo dentro de acuerdos de suministradores.	17.1.1. Consideraciones de seguridad en los acuerdos con terceras partes.	Página 83 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
93. Cadena de suministro en tecnologías de la información y comunicaciones.	NO SE DEFINIO			ND
94. supervisión y revisión de los servicios prestados por terceros.	Se realiza un seguimiento a los servicios prestados por terceros	Se realiza supervisión a los servicios prestados por terceros y se lleva un control y registro de incidencias en la prestación de servicios con cada proveedor, cada mes se reciben informes de las actividades realizadas por los proveedores y contratistas, además se lleva un control de las obligaciones de los contratistas. Para hacer seguimiento y medición de los servicios contamos con unas Métricas de Disponibilidad de Servicios de TI https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-GS-008%20M%C3%A9tricas%20de%20Disponibilidad%20de%20Servicios%20de%20TI.pdf	SI	
95. Gestión de cambios en los servicios prestados por terceros.	14.1. Política de Gestión de Cambios	Página 73 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
96. Responsabilidades y procedimientos.	6.1.2. Roles y responsabilidades 8. GESTIÓN DE ACTIVOS 8.1.4. Responsabilidades, 8.2. Política de uso de Internet 8.2.4. Responsabilidades 8.4. Política de uso de la Intranet 8.4.4. Responsabilidades De acuerdo con el Sistema Integrado de Gestión, en el ítem de Gestión de procesos la entidad cuenta con procedimientos los cuales cuentan con actividades, tareas, registros y puntos de control.	El Decreto 323 de 2016 establece la estructura organizacional de la Secretaría Jurídica Distrital y sus funciones http://sisjur.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=66674 , así como la Resolución 039 de 2019 que establece el manual de funciones de la entidad https://secretariajuridica.gov.co/sites/default/files/intranet_documentos_talento_humano/039-2019%20RESOLUCION%20SECRETARIA%20JURIDICA.PDF , Página 81 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad. En el sistema de información de SMART se pueden consultar los procedimientos y evidenciar que estos cuentan con controles http://smart.bogotajuridica.gov.co/SID/portal/resultados_busqueda.php , además se puede consultar el Manual del Sistema Integrado de Gestión http://www.secretariajuridica.gov.co/sites/default/files/planeacion/2310100-MA-001manual%20de%20SIG.pdf	SI	
97. Notificación de los eventos de seguridad de la información.	18.1. Gestión de Incidentes de Seguridad de la Información	Página 83 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, además se cuenta con una Guía de Gestión de Incidentes de Seguridad de la Información 2310200-GS-004 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-GS-004%20GU%C3%8DA%20GESTI%C3%93N%20DE%20INCIDENTES%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N_0.pdf	SI	

98. Notificación de puntos débiles de la seguridad	18.1.2. Gestión incidentes y mejoras	Página 83 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, además se cuenta con una Guía de Gestión de Incidentes de Seguridad de la Información 2310200-GS-004 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-GS-004%20GU%C3%8DA%20GESTI%C3%93N%20DE%20INCIDENTES%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N_0.pdf	SI	
99. Valorización de eventos de seguridad de la información y toma de decisiones.	14.6.1. Registro de eventos 18.1.1. Reporte sobre los eventos 19.1.1. Seguridad de la información en la continuidad del negocio	Página 80, 83, 84 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad, además se cuenta con un Plan de Contingencia 2310200-PL-03 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-PL-003%20Plan%20de%20Contingencia_V2.pdf	SI	
100. Respuestas a los incidentes de seguridad.	En el Sistema de SMART se cuenta con un módulo para el registro, tratamiento, seguimiento y evidencias de los incidentes de seguridad que se presenten en la entidad.	http://10.80.50.100/SJD/index.php?op=27&sop=27.4.1&la=5&li=1	SI	
101. Aprendizaje de los incidentes de seguridad de la información.	En el Sistema de SMART se cuenta con un módulo para el registro, tratamiento, seguimiento y evidencias de los incidentes de seguridad que se presenten en la entidad.	http://10.80.50.100/SJD/index.php?op=27&sop=27.4.1&la=5&li=1	SI	
102. Recopilación de evidencias.	En el Sistema de SMART se cuenta con un módulo para el registro, tratamiento, seguimiento y evidencias de los incidentes de seguridad que se presenten en la entidad.	http://10.80.50.100/SJD/index.php?op=27&sop=27.4.1&la=5&li=1	SI	
103. Planificación de la continuidad de la seguridad de la información.	19.1.1. Seguridad de la información en la continuidad del negocio	Se cuenta con un Plan de Contingencia 2310200-PL-03 https://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-PL-003%20Plan%20de%20Contingencia_V2.pdf	SI	
104. Implantación de la continuidad de la seguridad de la información.	19.1.1. Seguridad de la información en la continuidad del negocio	Se cuenta con un Plan de Contingencia 2310200-PL-03 http://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-PL-003%20Plan%20de%20Contingencia_V2.pdf	SI	
105. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	19.1.1. Seguridad de la información en la continuidad del negocio	Se cuenta con un Plan de Contingencia 2310200-PL-03 http://secretariajuridica.gov.co/sites/default/files/intranet_formatos/2310200-PL-003%20Plan%20de%20Contingencia_V2.pdf	SI	
106. Disponibilidad de instalaciones para el procesamiento de la información.	Las instalaciones de procesamiento de información de la entidad están implementadas con redundancia	La infraestructura del Data Center donde se realiza el procesamiento de información fue configurado en redundancia suficiente para cumplir con los requisitos de disponibilidad.	SI	
107. Identificación de la legislación aplicable.	20. Cumplimiento de los Requisitos Legales	Página 84 - 85 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
108. Derechos de propiedad intelectual (DPI)	20.1.2. Derechos de propiedad Intelectual.	Página 85 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
109. Protección de registros de la organización	20.1.3. Protección de los Registros de la Organización	Página 85 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
110. Protección de datos y privacidad de la información personal.	9. Principios Rectores para la Protección de Datos Personales	Página 43 - 67 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	

111. Regulación de los controles criptográficos.	12. Criptografía	Página 69 del Manual de Políticas de Seguridad de la Información y Protección de Datos Personales publicado en la Sección de Transparencia de la página Institucional de la entidad.	SI	
112. revisión independiente de la seguridad de la información.	Las revisiones se deberían realizar según las políticas de seguridad apropiadas y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados. Alinee los procesos de auto-evaluación de controles de seguridad con las auto-evaluaciones de gobierno corporativo, cumplimiento legal y regulador, etc., complementados por revisiones de la dirección y verificaciones externas de buen funcionamiento.	La Secretaría Jurídica Distrital encabeza de la Oficina de TIC se encuentra actualizando e implementando las actividades que hacen parte de la Política de Seguridad Digital, realizando la revisión y actualización de objetivos de control, controles, políticas, procedimientos, registros, así mismo la Oficina de Control Interno ha realizado revisiones sobre los riesgos digitales y diagnósticos sobre las actividades que se realiza sobre el Modelo de Seguridad de la informaciones la entidad.	SI	
113. Cumplimiento de las políticas y normas de seguridad.	Política de Seguridad y Manual de Políticas de Seguridad de la Información y Protección de Datos Personales	Se están realizando la actualización de la política y manual de seguridad de la información y protección de datos personales, revisando temas como el plan de seguridad y tratamiento de riesgos, así como los riesgos digitales, los controles y su implementación, capacitaciones sobre seguridad de la información a los funcionarios y contratistas de la entidad, además se remiten mensualmente tipos de seguridad a los correos de los funcionarios y contratistas.	SI	
114. Comprobación del cumplimiento.	Implementación de riesgos, controles, políticas y planes.	Se evidencia en las actividades que se han desarrollado durante el transcurso del año en el tema de Seguridad de la Información y Datos personales, con la actualización de la política y el manual, los controles y los riesgos digitales que se han establecido, además se esta implementando las actividades que tiene que ver con los datos personales como han sido el formato de compromiso de confidencialidad, el mensaje de dilatabilidad de confidencialidad en los correos y el mensaje de tratamiento de datos personales en los formularios que reciben datos personales.	SI	

Elaboró: Oscar Ernesto López Acuña - Profesional Universitario
 Revisó: Dik Martínez Velásquez - Jefe OCI
 Aprobó: Dik Martínez Velásquez - Jefe OCI

DESCRIPCIÓN	CANTIDAD	%
CONTROLES IMPLEMENTADOS	112	98,25%
CONTROLES NO IMPLEMENTADOS	2	1,75%
TOTAL CONTROLES	114	100,00%