SECRETARIA JURIDICA DISTRITAL

OFICINA DE CONTROL INTERNO

TEMA: SEGUIMIENTO A LA POLITICA DE SEGURIDAD DE LA INFORMACION. Política General de Seguridad de la Información. La Secretaría Jurídica Distrital mediante la implementación del Sistema de Gestión de Seguridad de la Información como parte del Modelo de Seguridad y Privacidad de la Información protege, preserva y administra la integridad, confidencialidad, disponibilidad y autenticidad de la información, así como la seguridad digital y la gestión de la continuidad de la operación, conforme al mapa de procesos

No	TEMA A EVALUAR	ACTIVIDAD	DESCRIPCION DE LA EVIDENCIA	FECHA DE ENTREGA DE LA EVIDENCIA	CUMPLE	OBSERVACIONES
1	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 6.1.2. Contacto con las Autoridades	Contacto con las autoridades. Se ha realizado contacto con las entidades que representan autoridad en temas de seguridad de la información con el fin de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad de la información.	La SJD tiene los números de contacto de la Alta Consejería de TIC, Colcert Gobierno, CAI Virtual en caso de apoyo a temas de incidentes de seguridad de la información. Durante el año 2020 no ha sido necesario contactar a estas entidades.	10/12/2020.	SI	No se han realizado contactos para asesoramiento
2	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 6.1.3.	Contacto con grupos de interés especial. Se han realizado los contactos apropiados con grupos de interés especiales, con foros especializados y asociaciones de profesionales en seguridad de la información, con el fin de estar actualizado en temas de seguridad de la información.	Desde la Alta Consejería de las TIC se realizan invitaciones a foros, conferencias, talleres y otras actividades en referencia a seguridad de la información. Esta información se divulga a través de un grupo de WhatsApp en donde se encuentran todos los oficiales de seguridad de la información de las entidades del Distrito	10/12/2020.	SI	Se adjuntan evidencias de los eventos, foros, talleres enviados por la Alta Consejería de TIC
3	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN- 7.3.1.- Contacto con grupos de interés especial	Terminación o cambio de responsabilidades del empleo. La Dirección de Gestión Corporativa ha enviado los reportes de desvinculación o cambio de labores y ha solicitado la modificación o inhabilitación de usuarios a la Oficina de Tecnologías de la Información y las Comunicaciones.	La Dirección Corporativa reporta los usuarios que se retiran o cambian de área a la Oficina de Tecnologías de la Información y las Comunicaciones para su correspondiente bloqueo	14/12/2020.	SI	Se soporta con las evidencias de las solicitudes de Dirección Corporativa y bloqueos de usuarios por parte de la OTIC
4	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN - 7.3.2.-Política de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios y personal provisto por terceros	Los supervisores de contratos han solicitado a la Ofician de Tecnologías de la Información y Comunicaciones la cancelación de las cuentas de usuario de los recursos tecnológicos que fueron asignados al ingresar a la entidad.	Los supervisores de los contratos reportan los usuarios que se retiran o cambian de área a la Oficina de Tecnologías de la Información y las Comunicaciones para su correspondiente bloqueo	14/12/2020.	SI	Se anexan las evidencias de las solicitudes de los supervisores de contratos y bloqueos de usuarios por parte de la OTIC
5	MANUAL DE POL ÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.8.1.1. - Inventario de activos.	Inventario de activos. Con el fin de contribuir a la protección de los activos de la Entidad, se elaboró y actualizo el Registro de Activos de Información liderada por la Oficina de TIC.	La Oficina de Tecnologías de la Información y Comunicaciones actualizó la matriz del registro de activos de información en el año 2020. Esta matriz está publicada en la página web de la entidad	10/12/2020.	SI	Se adjunta evidencia de la matriz de activos de información actualizada

6	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN .9.2.6. Cancelación o ajuste a los derechos de usuario	Cancelación o ajuste a los derechos de usuarios. Como se realiza la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de Correo electrónico corporativo, existe un procedimiento ?.	Existe el procedimiento 2310200-PR-091 ADMINISTRACIÓN DE USUARIOS en donde se establecen las actividades para la gestión de usuarios de red y correo corporativo. Las solicitudes de gestión de red y correo corporativo se realizan a través de GLPI o el formulario de gestión de usuarios	10/12/2020.	SI	Se cuenta con la evidencia del formato de gestión de usuarios diligenciados durante el año 2020
7	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN .9.4.2. Sistema de Gestión de Contraseñas.	Sistema de Gestión de Contraseñas. Se esta verificando por la oficina de TIC que el usuario tiene autorización del propietario de la información para el uso del sistema, base de datos o servicios de información. Como se realiza. ?	Se realiza de acuerdo a las solicitudes que se reciben de los diferentes procesos. Durante el año 2020 se han recibido solicitud de revisiones de roles y privilegios de sistemas de información tales como PERNO, SAE, SAI	10/12/2020.	SI	Anexan la evidencia de la verificación de roles y perfiles de los sistemas de información PERNO, SAE Y SAI.
8	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 11.2.4. Seguridad del Cableado	Seguridad del Cableado Se tienen separadas las rutas de cableado de energía y comunicaciones con el fin de evitar interferencias.	Los centros de cableado son administrados por la Secretaria General de la Alcaldía Mayor, aún así en los RACK se cuenta con unas unidades donde se encuentran ubicados nuestros Switch de Borde, los puntos de red de usuarios ya se encontraban instalados, estos fueron conectados a los SW de la SJD. En cuanto al tema de Corriente AC y regulada dependemos directamente de la Secretaria General ya que ellos administran estos temas.	14/12/2020.	SI	Se adjunta diagrama de conexión de la red WAN de la SJD.
9	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 11.2.5. Seguridad del Cableado	Mantenimiento a los Equipos Se esta efectuando el mantenimiento preventivo y correctivo a los equipos por personal autorizado. En caso afirmativo anexar los soportes del mantenimiento ejecutado este año.	Se tiene un cronograma establecido para las actividades de mantenimiento preventivo y correctivo de los equipos de cómputo por parte de la OTIC	14/12/20920.	SI	Se cuenta con el cronograma de actividades de los mantenimientos por áreas de la SJD y acta de seguimiento de los mantenimientos.
10	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 12.2.6. Política de Escritorio y Pantalla Limpia.	Política de Escritorio y Pantalla Limpia Todos los equipos de cómputo y dispositivos portátiles tienen aplicado el cierre de sesión por inactividad, definido por la Oficina de TIC.	En el Directorio Activo se tiene parametrizada una política de bloqueo automático de estaciones de trabajo por inactividad	10/12/2020.	SI	Se adjunta evidencia de la política configurada en el Directorio Activo

11	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 12.2.	Protección Contra Código Malicioso. Que controles se han implementado para la detección, prevención, y recuperación, combinados con la toma de conciencia apropiada de los usuarios, para la protección contra código malicioso.	La Oficina de Tecnologías de la Información y Comunicaciones adquirió la herramienta de Ciberseguridad ESCAN para proteger la red de virus y ataques internos y externos que puedan afectar la información de la entidad y se encuentra en proceso de instalación y configuración de dicha herramienta. En el mes de septiembre se realizó una charla de sensibilización de las políticas de seguridad de la información en la entidad	10/12/2020.	SI	Lo soporta la evidencia de la citación, presentación y asistencia a la charla de seguridad de la información realizada en septiembre
12	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 16.2.	Responsabilidades y Procedimientos Se ha revisado el procedimiento para la gestión de los incidentes en forma periódica por el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones con el fin de identificar cambios o ajustes necesarios.	En el año 2020 se realizó la actualización del documento, 2310200-MA-015 Manual de Gestión de Incidentes de seguridad de la Información el cual se encuentra publicado en el sistema SMART	10/12/2020.	SI	Se adjunta la evidencia de la fecha de creación, aprobación y publicación del Manual de Incidentes de Seguridad de la Información
13	MSPI. MODELO DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION.	Se ha aplicado el formato de autodiagnóstico que identifica el estado de avance del MSPI. numeral 4.2. y numeral 5.1.2 de la Política de Seguridad Se tienen definidos los indicadores de seguimiento para medir el avance del plan de Privacidad y seguridad de la información como lo exige MINTIC en Gobierno en Línea. numeral 4.2.	En el mes de marzo se realizó el autodiagnóstico del MSPI y del cual se generó el mapa de ruta para establecer el Plan Estratégico de Seguridad de la Información. Los indicadores del MSPI se encuentran en proceso de formalización por parte de la Oficina Asesora de Planeación	10/12/2020.	SI	Se adjunta evidencia del autodiagnóstico realizado en el mes de marzo y los indicadores de gestión del MSPI
14	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 16.1.5. Respuesta a incidentes de seguridad	Respuesta a incidentes de seguridad de la información Se ha realizado un análisis posterior a cada incidente de seguridad de la información materializado, para identificar su origen.	En el documento 2310200-MA-015 Manual de Incidentes de seguridad de la información en el capitulo llamado FASE 2. Detección, se establecen las actividades de identificación de la fuente origen de los incidentes de seguridad. Hay que señalar que durante el año 2020 no se han presentado incidentes de seguridad de la información en la SJD.	14/12/2020.	SI	Se adjunta el documento 2310200-MA-015 Manual de Incidentes de seguridad de la información. En el capitulo llamado FASE 2. Detección, se establecen las actividades de identificación de la fuente origen de los incidentes de seguridad.
15	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 13.1.2. Seguridad de los servicios de red	Seguridad de los servicios de red La secretaria cuenta con acuerdos de niveles de servicio para los proveedores de servicio de red.	La Oficina de Tecnologías de la Información y Comunicaciones tiene establecido Acuerdos de Niveles de Servicio con los proveedores de servicio de red donde mensualmente se monitorea la gestión y cumplimiento de los ANS	10/12/2020.	SI	la evidencia del reporte de cumplimiento de ANS de red del mes de noviembre
16	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓNA. 13.1.1. Controles de redes	Controles de redes Se tiene definido responsabilidades y procedimientos para la gestión de equipos de redes.	Se cuenta con las responsabilidades definidas para la gestión de acceso a redes la cual está a cargo del área de infraestructura y un contratista	14/12/2020.	SI	Evidencias de la gestión de acceso a redes WIFI para funcionarios y visitantes

17	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 12.4.4. Sincronización de relojes	Sincronización de relojes Se cuenta con una única fuente de referencia de tiempo para sincronizar los rejoles.	Los servidores se conectan a una página web a través del puerto NTP para realizar la sincronización con la hora legal colombiana	14/12/2020.	SI	Se adjunta pantalla de configuración de los servidores NTP a la página co.pool.ntp.org
18	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 11.1.1. Perímetro de seguridad física	Perímetro de seguridad física Se cuenta con controles de acceso y sistemas de supervisión para acceder a las áreas seguras.	Se cuenta con control de acceso biométrico al Centro de Cómputo. Este acceso lo tienen los administradores de infraestructura, sistemas misionales y el jefe de la OTIC	10/12/2020.	SI	Lo soporta evidencia fotográfica del acceso al Centro de Cómputo
19	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 11.1.2. Controles de acceso físico	Controles de acceso físico La secretaria registra la fecha y la hora de entrada y salida de visitantes.	Se registra la fecha y hora de la entrada y salida de visitantes en la portería principal del edificio Liévano	10/12/2020.	SI	Lo realiza una dependencia diferente a la Secretaria Jurica.
20	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 11.1.3. Seguridad en oficinas, recintos e instalaciones	Seguridad en oficinas, recintos e instalaciones La secretaria mantiene las áreas seguras fuera de la visita del público.	El Centro de Cómputo se ubica en un sitio donde no hay público en general	10/12/2020.	SI	Lo soporta evidencia fotográfica del acceso al Centro de Cómputo
21	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 11.1.4. Protección contra amenazas externas y ambientales	Protección contra amenazas externas y ambientales Se cuenta con controles físicos contra incendios..	Se cuenta con extintores de incendios ubicados en diferentes sitios físicos de la entidad	11/12/2020.	SI	Se adjunta evidencia fotográfica de la ubicación de extintores en diferentes sitios de la SJD
22	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 11.1.5. Trabajo en áreas seguras	Trabajo en áreas seguras La secretaria prohíbe el uso de equipos de fotografía o filmación a personal no autorizado.	Actualmente no se tiene ningún aviso o alerta que informe a los visitantes la prohibición de filmar o fotografiar en la SJD	11/12/2020.	NO	se recomienda dar cumplimento a lo estipulado en la política de seguridad de la in formación numeral 11.1.4 " En las áreas de acceso restringido debe haber una continua supervisión del trabajo realizado, especialmente por terceros, se debe limitar el uso de quipos como cámaras fotográficas, de video, celulares. En caso de ser requerido solo podrá ser autorizado mediante autorización previa".
23	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 11.1.6. Áreas de carga, despacho y acceso público	Áreas de carga, despacho y acceso público La secretaria controla el acceso de personal de carga a otras áreas de la organización.	La Oficina de Tecnologías de la Información y las Comunicaciones informa a través de correo electrónico a la Secretaría General el acceso de elementos y bienes de tecnología hacia las instalaciones de SJD	14/12/2020.	SI	Se adjuntan evidencias de correos electrónicos informando el acceso de equipos de cómputo a la Secretaría General.
24	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 8.1.1. Inventario de activos	Inventario de activos Se realiza periódicamente la identificación de los activos	La Oficina de Tecnologías de la Información y Comunicaciones actualizó la matriz del registro de activos de información en el año 2020. Esta matriz está publicada en la página web de la entidad	10/12/2020.	SI	La evidencia de la matriz de activos de información actualizada

25	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 8.1.2. Propiedad de los activos	Propiedad de los activos El propietario conoce los activos que están bajo su responsabilidad.	La Dirección de Gestión Corporativa diligencia el formato 2311500-FT-223 y lo entrega a cada funcionario para su correspondiente firma. El formato original reposa en la carpeta de hoja de vida de cada funcionario. Los bienes con los responsables a su cargo son incluidos en el sistema SAI	11/12/2020.	SI	Se adjunta evidencia del formato 2311500-FT-223 y reporte de los bienes a cargo de un funcionario generado desde el sistema SAI
26	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.8.1.3. Uso aceptable de los activos	Uso aceptable de los activos En la secretaria los funcionarios y contratistas son consientes del uso aceptable de los activos de información a su cargo.	La Dirección de Gestión Corporativa establece en el procedimiento 2311500-PR-075 Seguimiento y Control de Bienes la responsabilidad que tienen los funcionarios sobre los bienes que tienen bajo su custodia	11/12/2020.	SI	Lo soporta con la pantalla del marco operacional del procedimiento 2311500-PR-075 Seguimiento y Control de Bienes
27	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 8.1.4. Devolución de los activos	Devolución de los activos La secretaria a través de la oficina de TIC cuenta con un procedimiento para la devolución de información física.	La Dirección de Gestión Corporativa cuenta con el procedimiento 2311520-PR-087 Préstamo y Consulta de Expedientes en donde se establecen las actividades para el préstamo, consulta y devolución de carpetas físicas. La actividad No 6 de este procedimiento define la solicitud de devolución de carpetas físicas	11/12/2020.	SI	Se cuenta con el procedimiento 2311520-PR-087 Préstamo y Consulta de Expedientes. En la actividad No 6 de este procedimiento se define la solicitud de devolución de carpetas físicas.
28	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 8.2.1. Clasificación de la información	Clasificación de la información En la secretaria a través de la oficina de TIC se ha validado que se tiene la información física clasificada.	La Oficina de Tecnologías de la Información y Comunicaciones actualizó la matriz del registro de activos de información en el año 2020 y en la cual se encuentra la clasificación de los activos de información. Esta matriz está publicada en la página web de la entidad	10/12/2020.	SI	Se adjunta evidencia de la matriz de activos de información actualizada
29	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 8.2.2. Manejo de activos	Manejo de activos La secretaria a través de la oficina de TIC aplica los procedimientos establecidos para el manejo de las carpetas e información física.	La Dirección de Gestión Corporativa cuenta con el procedimiento 2311520-PR-087 Préstamo y Consulta de Expedientes en donde se establecen las actividades para el préstamo, consulta y devolución de carpetas físicas. En el capitulo de marco operacional se establecen los protocolos para el adecuado manejo y protección de la información en cuanto a integridad y disponibilidad de las carpetas físicas	11/12/2020.	SI	El procedimiento 2311520-PR-087 Préstamo y Consulta de Expedientes. En el capitulo de marco operacional se establecen los protocolos para el adecuado manejo y protección de la información en cuanto a integridad y disponibilidad de las carpetas físicas
30	MSPI. MODELO DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION.	Se tienen definidos los indicadores de seguimiento para medir el avance del plan de Privacidad y seguridad de la información como lo exige MINTIC en Gobierno en Línea. numeral 4.2.	Se definieron y aprobaron los indicadores de gestión del MSPI. Se encuentran en proceso de formalización por parte de la Oficina Asesora de Planeación	10/12/2020.	NO	No se ha dado cumplimiento a lo estipulado por MINTIC EN EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION en lo relacionado con definir los indicadores de seguimiento para medir el avance del plan de privacidad y seguridad de la informacion. Se recomienda dar cumplimiento a los plazos estipulados en el Numeral 12.2. del Modelo. "Sujetos Obligados del Orden Territorial. A. Gobernaciones de categoría Especial y Primera; alcaldías de categoría Especial, y demás sujetos obligados de la administración publica en el mismo nivel. Para las entidades agrupadas en A, B y C los plazos serán los siguientes:" Año/ (%) 2015 70% 2016 90% 2017 100%. 2018 mantener 100% 2019 mantener 100%. 2020 mantener 100%

31	MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 18.2.1. Revisión independiente.	Revisión independiente. Se están revisando en forma independiente , los controles, las políticas, los procesos y los procedimientos de la seguridad de la información a intervalos planificados o cuando ocurran cambios significativos, adjuntar la evidencia, plan o soporte.	En el año 2020 se han realizado dos auditorías enfocadas al cumplimiento de la seguridad de la información para los sistemas LEGALBOG, SAE, SAI, PERNO y SMART	10/12/2020.	SI	Se soporta con los dos informes de auditoría realizados por la Oficina de Control Interno
Elaboro: Oscar Alonso Rodriguez Fontecha			Aprobó: Jefe Oficina Control Interno DIK MARTINEZ VELASQUEZ			