SECRETARIA JURIDICA DISTRITAL						
OFICINA CONTROL INTERNO						
TEMA DE SEGUIMIENTO AL MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES: Proteger la información generada procesada y resguardada por los procesos de la entidad, que generan soluciones jurídicas integrales formulan políticas en materia jurídica, lideran el quehacer de la gestión jurídica y disciplinaria, establecen						
No.	NUMÉRALES DEL MANUAL	ACTIVIDAD	DESCRIPCIÓN DE EVIDENCIA	FECHA DE ENTREGA DE EVIDENCIA	CUMPLE	OBSERVACIONES
1	10.15. Área responsable de la implementación y observancia de esta política y de la atención de peticiones, consultas y reclamos en relación con el tratamiento de datos	La Secretaria Jurídica Distrital tiene a su cargo la labor de desarrollo, implementación, capacitación y observancia de esta Política, para lo cual se coordinará por parte del área designada por la Secretaria(o) Jurídica(o), lo pertinente; inicialmente a través de los responsables de las que se designen de las áreas misionales y de apoyo. Para el efecto, todos los funcionarios que realizan el Tratamiento de Datos Personales en las diferentes áreas, están obligados a dar traslado al área responsable de la implementación y observancia de esta política -de manera inmediata- todas las peticiones, quejas o reclamos que reciban por parte de los Titulares de Datos Personales. Particularmente, la oficina que designe la Secretaria(o) Jurídica (o), será la dependencia responsable de atender las peticiones, consultas y reclamos, donde el titular de la información podrá ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.	No se ha definido el responsable del tratamiento de Datos Personales, se hará una reunión con la Dirección de Gestión Corporativa para que la persona de Atención al Ciudadano maneje esta información. De todas formas, las solicitudes que llegan por radicación SIGA, sobre tratamiento de datos personales son direccionadas por Gestión Documental a las diferentes dependencias para ser atendidas.	6/05/2019	NO	
2	10.16. Derechos del Titular de Datos Personales	El titular de los datos personales tiene los siguientes derechos: a. Conocer, actualizar y rectificar sus datos personales frente a la Secretaria Jurídica Distrital. Este derecho se podrá ejercer, entre otros, frente a los datos personales parciales, inexactos, incompletos, fraccionados, que induzcan a error o aquellos cuyo tratamiento este expresamente prohibido o no haya sido autorizado. b. Solicitar prueba de la autorización otorgada a la Secretaria Jurídica Distrital, salvo la Ley indique que dicha Autorización no es necesaria o que la misma haya sido validada con arreglo a lo establecido en el artículo 10 del Decreto 1377. c. Presentar solicitudes ante la Secretaria Jurídica Distrital respecto al uso que le ha dado a sus datos personales, y que estas le entreguen tal información. d. Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. e. El suministro de datos personales de niños, niñas y adolescentes es de carácter facultativo, tanto para ellos, como para quienes actúan a su nombre. f. Cuando los datos del titular ya se encuentren registrados con anterioridad en la Secretaria Jurídica Distrital, se dará aplicación a lo establecido en el artículo 12 del Decreto 1377 de 2013. g. Solicitar acceso y acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento. h. El suministro de datos personales de los titulares, que hubiesen sido registrados en la entidad, no serán cedidos a terceros, sin su consentimiento expreso. Sin perjuicio de lo anterior, el titular autoriza que se cedan sus datos personales cuando lo requieran las autoridades administrativas competentes o por mandato judicial. i. Los datos consignados por el titular harán parte de una base de datos de la entidad, por tal razón la entidad podrá hacer uso de ellos, para efectos de un determinado proceso. j. El titular de datos personales cuando haya registrado sus datos en una base de datos deberá tener un usuario y claveque solo conocerá el titular y la entidad se compromete a no ceder ni pretender conocer dicha clave, con la excepción de que la transmisión por internet no es segura. k. La Secretaria Jurídica Distrital no se hace responsable por el acceso indebido de terceros a la base de datos por alguna falla técnica en el funcionamiento y/o conservación de datos en los sistemas de información. l. La Secretaria Jurídica Distrital ha adoptado los niveles de seguridad de protección de datos personales legalmente requeridos, instalando los controles técnicos y administrativos necesarios para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de la información facilitada	La Oficina de TIC en el portal de la entidad, creará un espacio para la comunicación de los derechos de los titulares de datos personales y se colocara el link del manual, para conocimiento del ciudadano en un lugar visible.	6/05/2019	NO	
3	10.17. Procedimiento para el tratamiento de Datos personales (ejercer los derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización)	Los titulares, o sus causahabientes, o sus representantes, previa acreditación de su identidad, podrán solicitar a través del correo electrónico que sea designado por la entidad, personalmente en la Carrera. 8 No. 10 - 65 de la ciudad de Bogotá, o a los teléfonos: 3813000, la información personal del Titular que repose en cualquier base de datos y archivos de la Secretaria Jurídica Distrital. El término para ser atendidas las consultas será de diez (10) días hábiles, contados desde la fecha de su recibo. En caso de no poder dar respuesta durante este tiempo, se deberá informar los motivos de la demora señalando la fecha en que se dará la contestación, sin que esta supere cinco días hábiles, después de vencido el primer plazo. Así mismo, a través del correo electrónico antes mencionado, los titulares, sus causahabientes, o sus representantes, podrán solicitar rectificación, actualización o supresión de sus datos personales. Las solicitudes, deben contener la siguiente información: a. Nombre y domicilio del titular para enviar la respuesta b. Documentación que acredite la identidad o personalidad de su causahabiente o representante. c. Descripción clara y precisa de los datos personales respecto de los cuales se desea ejercer los derechos. En cualquier momento y de manera gratuita el titular o su representante podrán solicitar a personal de la Secretaria Jurídica Distrital, la rectificación, actualización o supresión de sus datos personales, previa acreditación de su identidad. Los derechos de rectificación, actualización o supresión únicamente se podrán ejercer por: a. El titular o sus causahabientes, previa acreditación de su identidad, o a través de instrumentos electrónicos que le permitan identificarse. b. Su representante, previa acreditación de la representación. Cuando la solicitud sea formulada por persona distinta del titular, deberá acreditarse en debida forma la personería o mandato para actuar; y en caso de no acreditar tal calidad, la solicitud se tendrá por no presentada. La solicitud de rectificación, actualización o supresión debe ser presentada a través de los medios habilitados por la secretaria jurídica distrital señalados en el aviso de privacidad y contener, como mínimo, la siguiente información: a. El nombre y domicilio del titular o cualquier otro medio para recibir la respuesta. b. Los documentos que acrediten la identidad o la personalidad de su representante. c. La descripción clara y precisa de los datos personales respecto de los cuales el titular busca ejercer alguno de los derechos. d. En caso dado otros elementos o documentos que faciliten la localización de los datos personales.	Una vez se realice la reunión con la Dirección de Gestión Corporativa, se creará el correo para que los usuarios pueden remitir sus solicitudes de tratamiento de datos, el cual será responsabilidad de Atención al Usuario.	6/05/2019	NO	

4	11.1.4. Retiro de los derechos de acceso	Cada uno de los Directores, Jefes de Oficina de la entidad serán los encargados de comunicar a la Dirección Corporativa, el cambio de cargo, funciones/actividades o la terminación contractual de los funcionarios pertenecientes al proceso. La Dirección Corporativa será la encargada de comunicar a la Oficina de Tecnologías de la Información y las Comunicaciones sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.	La Oficina de TIC está trabajando en la elaboración del procedimiento de Administración de usuarios, en el cual se incluirá el formato denominado Acuerdo de Confidencialidad.	6/05/2019	PARCIALMENTE	
5	12.1. Políticas de Uso de Controles Criptográficos	La Secretaría Jurídica Distrital debe proteger la confidencialidad, integridad y disponibilidad de la información por medio de técnicas criptográficas apropiadas. Se contemplará la evaluación e implementación de controles criptográficos en la medida que un determinado servicio de procesamiento de información o acceso lo requiera. Se verificarán los medios y herramientas criptográficas que mejor se acoplen a las necesidades de la entidad. Antes de la implementación del tipo de control criptográfico seleccionado, se debe definir y comunicar el procedimiento para la gestión de las llaves públicas o privadas, según el caso, entre las partes interesadas. Las características de los controles criptográficos, incluyendo el tipo, fortaleza y calidad, al igual que las herramientas y mecanismos a emplear para implementar los controles, serán definidos por la Oficina de Tecnologías de la Información y las Comunicaciones en función de la clasificación de la información. Se debe garantizar que el uso de controles criptográscentes es de carácter facultativo, tanto para ellos, como para quienes actúan a su nombre. f. Cuando los datos del titular ya se encuentren registrados con anterioridad en la Secretaría Jurídica Distrital, se dará aplicación a lo establecido en el artículo 12 del Decreto 1377 de 2013. g. Solicitar acceso y acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento. h. El suministro de datos personales de los titulares, que hubiesen sido registrados en la entidad, no serán cedidos a terceros, sin su consentimiento expreso. Sin perjuicio de lo anterior, el titular autoriza que se cedan sus datos personale	No se ha realizado, se debe ejecutar en el segundo semestre, sin embargo, las claves de usuarios de los Sistemas de Información y bases de Datos se encuentran cifradas.	6/05/2019	PARCIALMENTE	
6	13.1.1. Perímetro de Seguridad Física	La Secretaría Jurídica Distrital debe evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que generen afectaciones a la confidencialidad, integridad o disponibilidad de la información.	En razón a que la Oficina de TIC de La Secretaría Jurídica Distrital debe evitar accesos físicos no autorizados a las instalaciones de procesamiento de la información, ya que se pueden generar afectaciones a la confidencialidad, integridad o disponibilidad de la información. El acceso al Data Center se encuentra restringido con un control biométrico de acceso, al cual solo pueden ingresar personas que estén autorizadas. A causa de esto existe un formato denominado Bitácora de Acceso a Centro de Computo 2310200-FT-087, con el propósito que se registre: Nombre del visitante, empresa, fecha, hora de ingreso, hora de salida, observaciones, elementos ingresados, firma del visitante y nombre del servidor responsable de la actividad. Agregado a lo anterior los servidores y contratistas cuentan con una tarjeta de proximidad la cual se encuentra habilitada para que ingresen solo a los lugares autorizados.	6/05/2019	SI	Ver fotos de evidencia  C:\Users\oelopez\Desktop\Informe 7-05-2019 v fotos
7	13.1.3. Ubicación y Protección de los equipos	La infraestructura tecnológica (hardware, software y comunicaciones) deberá contar con medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados. Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.	La infraestructura tecnológica de la Secretaría Jurídica cuenta con medidas de protección tanto física como electrónica, con el fin de evitar daños e interceptaciones a la información o accesos no autorizados. Se tiene instalado un tablero totalizador electrónico dentro del centro de cómputo, de tal manera que se pueda interrumpir el suministro de energía manualmente en caso de que ocurra alguna emergencia. De la misma forma, la Oficina de TIC protege la infraestructura de procesamiento de la información mediante contratos de mantenimientos preventivos y correctivos.	6/05/2019	SI	
8	13.1.6. Retiro de Activos	Los equipos de cómputo, la información o el software no deben ser retirados de la entidad sin una autorización formal. Periódicamente se deben llevar a cabo por parte de la Dirección de Corporativa, comprobaciones puntuales para detectar el retiro no autorizado de activos de la entidad.	Se realizará una reunión con la Dirección de Gestión Corporativa para tratar el tema.	6/05/2019	NO	

9	14.1. Política de Gestión de Cambios	La Secretaría Jurídica Distrital debe asegurar que los cambios de alto impacto realizados sobre la organización, los procesos de negocio, las instalaciones o los sistemas de procesamiento de información se realicen de forma controlada. Toda solicitud de cambio en los servicios de procesamiento de información, se deben realizar siguiendo el Procedimiento de Análisis, Diseño, Desarrollo e Implementación de Soluciones, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información, e igualmente tener una trazabilidad de este tipo de solicitudes. El procedimiento de gestión de cambios especifica los siguientes canales autorizados para la recepción de solicitudes de cambios: Mesa de Ayuda (Recepción de documentación Software), correo electrónico o memorando dirigido al Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones Se debe establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, bien sea porque se trate de actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad del aplicativo o a los componentes que soportan el sistema de información, tales como el sistema operativo o cambios en hardware. Existe sin embargo una situación especial para cambios de emergencia en la cual se debe garantizar que los cambios se apliquen de forma rápida y controlada. (Ver Procedimiento Análisis, Diseño, Desarrollo e Implementación de Soluciones) Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los funcionarios que por sus actividades tienen relación con el sistema de información. Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información. Estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto. Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantienen las condiciones de operatividad del sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema, y que el propósito del cambio se cumplió satisfactoriamente. Se debe disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.	La oficina de TIC de la Secretaría Jurídica Distrital comunica, que el control de cambios es realizado en los aplicativos; los cuales se trabajan mediante manuales técnicos y de usuarios, donde se documentan los cambios realizados en cada uno de los sistemas con su respectivo versión año tras año, y se encuentran publicados en el portal de la entidad y en la biblioteca virtual, como también en cada uno de los respectivos aplicativos. De igual modo, la Oficina de Tecnología de la Información y Comunicación mediante el aplicativo de soporte GLPI, lleva el control de los cambios realizados a todo el Software Misional de la Entidad y a los Sistemas Administrativos y Financieros. Como también, lleva el control de los computadores a los que se les presta soporte técnico.	6/05/2019	SI	
10	14.2. Política de Gestión de la capacidad	La Secretaría Jurídica Distrital debe asegurar la disponibilidad de los recursos necesarios para la operatividad de los sistemas de información contemplando necesidades actuales y futuras. La Oficina de Tecnologías de la Información y las Comunicaciones definirá las actividades específicas para monitorear, proyectar y asegurar la capacidad de la infraestructura de procesamiento de información, con el objeto de garantizar el buen desempeño de los recursos tecnológicos necesarios para la ejecución de los procesos. La capacidad de los recursos debe ser ajustada periódicamente para garantizar la disponibilidad y eficiencia requerida de acuerdo a las necesidades actuales y futuras de la Secretaría Jurídica Distrital. El monitoreo y gestión de la capacidad debe hacerse considerando la criticidad de la información y los sistemas que soportan, para lo cual se utilizará la criticidad determinada durante el levantamiento del inventario de activos de información. Aquellos componentes que soporten activos con criticidad alta siempre deben estar sujetos a monitoreo y gestión de capacidad. Se debe tomar las acciones adecuadas para minimizar o evitar la dependencia de elementos o personas claves para la prestación de un servicio. Dentro de las acciones se deben contemplar: redundancia de elementos, arquitecturas de contingencia o de alta disponibilidad, técnicas de gestión de conocimiento sobre la operatividad de la infraestructura, etc. Los umbrales de óptimos de capacidad se pueden obtener incrementando la capacidad o reduciendo la demanda, lo cual incluye las siguientes posibles acciones que deberán ser llevadas a cabo por la Oficina de Tecnologías de la Información y las Comunicaciones: □ Eliminación de información obsoleta. □ Supresión de aplicaciones. □ Bases de datos o ambientes en desuso. □ Optimización de procesos o tareas automáticas. □ Afinamiento de consultas a bases de datos o lógica de aplicaciones. □ Restricción de ancho de banda para servicios con alto consumo de capacidad que no sean misionales.	Para la ampliación de la capacidad de cómputo y comunicaciones del Data Center, La Oficina de Tecnologías de la Información y las Comunicaciones realizará con los recursos que están dispuestos para la vigencia 2019. El proyecto del Sistema Integrado de Información de acuerdo con las especificaciones técnicas y de software que defina la Unión Temporal que está a cargo del proyecto.	6/05/2019	NO	
11	14.4. Política de Protección contra Código Malicioso	La Secretaría Jurídica Distrital debe establecer medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos. La infraestructura de procesamiento de información debe contar con un sistema de detección/prevención de intrusos, sistema anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos. Así mismo, se restringirá la ejecución de aplicaciones y se mantendrá instalado y actualizado un sistema de antivirus, en todas las estaciones de trabajo y servidores de la Secretaría Jurídica Distrital. Se restringirá la ejecución de código móvil aplicando políticas en el sistema operacional, en el software de navegación de cada máquina y en el sistema de control de navegación. Los usuarios de los servicios TIC de la Secretaría Jurídica Distrital son responsables de la utilización de programas antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos y/o removibles y/o los archivos y/o el correo electrónico que esté autorizado a emplear. La Secretaría Jurídica Distrital contará permanentemente con los programas antivirus de protección a nivel de red y de estaciones de trabajo, contra virus y/o código malicioso, el servicio será administrado por la Oficina de Tecnologías de la Información y las Comunicaciones.Los programas antivirus deben ser instalados por la Oficina de Tecnologías de la Información y las Comunicaciones en los equipos centralizados de procesamiento y en las estaciones de trabajo de modo residente, para que estén activados durante su uso. Las instalaciones nuevas de estaciones de trabajo o servidores que sirvan al propósito operativo de la Secretaría Jurídica Distrital deben contar con un programa de antivirus previo a la instalación de cualquier otro programa sobre el sistema operativo. Los servicios de TIC que se emplean para servir a una finalidad operativa y administrativa en relación con la entidad y que intercambien información o los sistemas que la procesan, redes y demás infraestructura TIC la Secretaría Jurídica Distrital se consideran bajo el control de la entidad y pueden ser revisados por el administrador de la suite de productos de seguridad. Se debe actualizar periódicamente las versiones de los componentes de los diferentes sistemas de seguridad operativos, incluidos, motores de detección, bases de datos de firmas, software de gestión en el lado cliente y servidor, etc. Se debe validar de forma periódica el uso de software no malicioso en las estaciones de trabajo y servidores. Esta labor se debe programar de forma automática con una periodicidad semanal y su correcta ejecución y revisión estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones. Se deben tener controles para analizar, detectar y restringir el software malicioso que provenga de posibles fuentes de código malicioso, entre ellas: descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc. Se deben generar boletines informativos acerca de las formas de reconocer malware, horas, spyware, etc., los cuales ayuden a generar una cultura de seguridad de la información entre los funcionarios la Secretaría Jurídica Distrital. Los funcionarios de la Secretaría Jurídica Distrital, pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio, que consideren sospechoso de contener software malicioso. En cualquier caso, los funcionarios siempre podrán consultar a la Oficina de Tecnologías de la información y las Comunicaciones sobre el tratamiento que debe darse en caso de sospecha de malware. Los funcionarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus y/o de detección de código malicioso, en los equipos o sistemas en que estén instalados. Cada usuario es responsable por la destrucción de todo archivo o mensaje, que le haya sido enviado por cualquier medio provisto por la Oficina de Tecnologías de la Información y las Comunicaciones, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta mesadeayuda@secretariajuridica.gov.co con la	La Oficina de la Tecnologías de la Información y Comunicaciones tiene instalado en todas las maquinas un antivirus para la prevención de intrusos, lo mismo que tiene restringido a todos los usuarios el acceso a páginas que no sean permitidas y a instalar software en los equipos de la entidad. En cuanto al desarrollo de nuevas funcionalidades en los sistemas de información, no se realizan pruebas instalaciones o desarrollos de software, directamente sobre el entorno de producción, para ello existe el ambiente de pruebas y evitar el fraude o inserción de código malicioso.	6/05/2019	SI	

12	14.5. Política de Backus	La Secretaría Jurídica Distrital debe proporcionar medios de respaldo adecuados para asegurar que la información esencial y el software asociado se puedan recuperar después de una falla. La información de cada sistema de información debe ser respaldada regularmente sobre un medio de almacenamiento como cinta, CD, DVD, Disco Externo, de acuerdo a su nivel de criticidad identificada en el inventario de activos de información. La información con criticidad mayor debe estar sujeta a una mayor frecuencia de tareas de respaldo. Los medios se almacenarán en una custodia externa que cuente con los mecanismos de protección ambiental como detección de humo, incendio, humedad, y mecanismos de control de acceso físico (Ver Procedimiento de Administración de Backus y Restore). Se deben realizar pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad. Estos aspectos técnicos se deben registrar en el formato de Control de Restauraciónalta siempre deben estar sujetos a monitoreo y gestión de capacidad. Se debe tomar las acciones adecuadas para minimizar o evitar la dependencia de elementos o personas claves para la prestación de un servicio. Dentro de las acciones se deben contemplar: redundancia de elementos, arquitecturas de contingencia o de alta disponibilidad, técnicas de gestión de conocimiento sobre la operatividad de la infraestructura, etc. Los umbrales de óptimos de capacidad se pueden obtener incrementando la capacidad o reduciendo la demanda, lo cual incluye las siguientes posibles acciones que deberán ser llevadas a cabo por la Oficina de Tecnologías de la Información y las Comunicaciones: Eliminación de información obsoleta.	La Oficina de TIC de la Secretaría Jurídica Distrital proporciona medios de respaldo adecuados, para asegurar que la información esencial y el software asociado se puedan recuperar después de una falla. Como también tiene definido donde guarda las copias de seguridad que realiza, y con qué frecuencia se ejecutan. Existe un formato de control de Backup.	6/05/2019	SI	C:\Users\oelopez\Desktop\Informe 7-05-
13	16.1.2. Procedimientos de control de cambios	Cualquier tipo de cambio sobre los sistemas de información deberá seguir lo establecido en el Procedimiento de Análisis, Diseño, Desarrollo e Implementación de Soluciones para la Secretaría Jurídica Distrital y tener en cuenta la aceptación de las pruebas técnicas y funcionales dictaminadas por cada uno de los responsables a quienes afectaran los cambios que se realicen.	La Oficina de TIC hace la aclaración que el control de cambios en los aplicativos, se trabajan mediante manuales técnicos y de usuario. Donde se documentan los cambios realizados en cada sistema con su respectivo versión año tras año, los cuales se encuentran publicados en el Portal de la entidad y la Biblioteca Virtual y en cada uno de los aplicativos.	6/05/2019	SI	
14	19.1. Política de Gestión de la Continuidad del Negocio	La Secretaría Jurídica Distrital debe garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información de la entidad.	La oficina de TIC de la Secretaría Jurídica Distrital cuenta con un Plan de Contingencia 2310200-PL-003, el cual permitirá mantener la continuidad de los sistemas de información frente a eventos críticos, de la entidad y minimizará el impacto negativo sobre la misma, sus recursos y usuarios. Este plan es parte integral de las políticas informáticas de la entidad que servirá para evitar interrupciones, para estar preparado contra fallas potenciales y para guiar hacia una solución oportuna en la restauración del servicio y se encuentra publicado en la Intranet.	6/05/2019	SI	
15	19.1.1. Seguridad de la información en la continuidad del negocio	Ante la ocurrencia de eventos no previstos en cuanto a la indisponibilidad del Centro de Datos principal, de la Secretaría Jurídica Distrital debe contar y asegurar la implementación de un Plan de Recuperación de Desastres que asegure la continuidad de las operaciones tecnológicas de sus procesos críticos. Para la Secretaría Jurídica Distrital su recurso más importante es el Recurso Humano y por lo tanto será su prioridad y objetivo principal protegerlo adecuadamente en cualquier situación. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, deben estar incorporados y definidos en un "Plan de contingencias".	Ante la ocurrencia de eventos no previstos en cuanto a la indisponibilidad del Centro de Datos principal, la Oficina de TIC de la Secretaría Jurídica Distrital, se encuentra trabajando en el documento de métricas, el cual hará parte del Plan de Contingencia y estará publicado en la Intranet para el mes de junio de la vigencia 2019.	6/05/2019	PARCIALMENTE	
16	19.1.2. Pruebas y mantenimiento del plan de continuidad del negocio	La Secretaría Jurídica Distrital debe establecer un plan de pruebas periódico del plan de Contingencia de la Plataforma Tecnológica.	La Oficina de TIC de la Secretaría Jurídica Distrital dentro de la actualización del Plan de Contingencias, incluirá el tema de métricas pruebas de servicios y el plan de continuidad; con el sitio alterno que cuenta la Secretaría Jurídica en las instalaciones de la Secretaría General.	6/05/2019	NO	

Elaboró - Oscar Ernesto López Acuña

Aprobó - Jefe Oficina de Control Interno: Dik Martínez Velásquez