11	ANEXO A - OBJETIVOS DE CONTROL Y CONTROLES ISO 27001 - A.16.1. Gestión de Incidentes y Mejoras en la Seguridad de la Información:	a) Se establecieron los procedimientos para la gestión de los incidentes de seguridad de la información. b) Es revisado el procedimiento periódicamente por el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones con el fin de identificar cambios o ajustes pertinentes que garanticen la eficiencia y eficacia de las respuestas a los incidentes. c)Se asignó un responsable en la secretaría Jurídica de la gestión de los incidentes de seguridad. d) Se ha capacitado a los servidores públicos en el registro y/o reporte de eventos y debilidades de gestión de la privacidad, seguridad de la información y continuidad del negocio. e) Se tienen definidos los indicadores de gestión y reportes de los tipos de incidentes, cantidad de los mismos e impacto generado sobre servicios y activos de la entidad.	Las revisiones documentales y evidencias presentadas, determinan el estado de los literales: a) Cumple b) Cumple c) Cumple d) Cumple e) Cumple	21/08/2020	SI	Se recomienda revisar y complementar el numeral 7 del Manula de Gestión de Incidentes de seguridad de la información
Elaboro: Oscar Alonso Rodríguez Fontecha			Aprobó: Jefe Oficina Control Interno - DIK MARTINEZ VELASQUEZ			

7	ANEXO A - OBJETIVOS DE CONTROL Y CONTROLES ISO 27001 - A.13.2.1. Políticas y Procedimientos para la Transferencia de la Información	Políticas y procedimientos para transferencia de información: a) Se cuenta con la política, el procedimiento y los controles formales para proteger la transferencia de información.	Revisado los documentos y evidencias presentadas, determina el estado del literal: a) Cumple parcialmente	21/08/2020	PARCIAL	No cumple con el procedimiento y los controles formales para proteger la transferencia de información.
8	ANEXO A - OBJETIVOS DE CONTROL Y CONTROLES ISO 27001 - A.14.2.1. Política de Desarrollo Seguro.	Política de desarrollo seguro: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas de información y a los desarrollos que se dan dentro de la organización en las siguientes directrices: a) Está definida la seguridad del ambiente de desarrollo. b) Se orienta la seguridad en el ciclo de vida de desarrollo del software. 1) Está definida la seguridad en la metodología de desarrollo de software. 2) Se establecieron las directrices de codificación seguras para cada lenguaje de programación usado. c) Están definidos los requisitos de seguridad en la fase diseño. d) Se definieron los puntos de chequeo de seguridad dentro de los hitos del proyecto. e) Se establecieron los depósitos seguros. f) Está definida la seguridad en el control de la versión.	Las revisiones documentales y evidencias presentadas, determinan el estado de los literales: a) Cumple b) Cumple. 1.- No Cumple. 2.- No Cumple c) Cumple d) No cumple e) No cumple f) No cumple.	21/08/2020	PARCIAL	En el procedimiento "Procedimiento de análisis, diseño, desarrollo e implementación de soluciones" no se evidencia la identificación de un depósito seguro de los códigos fuentes que son desarrollados y no se evidencian controles asociados con la seguridad en el control de las versiones de los desarrollos de software. • La secretaría no cuenta con: Directrices de codificación seguras para cada lenguaje de programación usado. Un Plan de emergencia para las aplicaciones que manejan información crítica.
9	ANEXO A - OBJETIVOS DE CONTROL Y CONTROLES ISO 27001 - A.15.1.1. Política de Seguridad de la Información para las Relaciones con Proveedores:	a) Se acordaron los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la secretaría Jurídica. b) Están documentados los requisitos de Seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la secretaría Jurídica. c) Se refleja en la política los acuerdos con cada proveedor de incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnologías de información.	Las revisiones documentales y evidencias presentadas, determinan el estado de los literales: a) No cumple b) No cumple c) No cumple	21/08/2020	NO	La secretaría no cuenta con: Un documento que indique los requisitos de Seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la Secretaría Jurídica. Los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnologías de información, no se han identificado para la secretaría.
10	ANEXO A - OBJETIVOS DE CONTROL Y CONTROLES ISO 27001 - A.12.3. Copias de Respaldo.	Copias de Respaldo (Backup). a).- En qué medio de almacenamiento están respaldadas las copias que respaldan los sistemas de información? b.- En qué fecha se realizó la última copia de respaldo efectuada? c.- Cuáles la frecuencia de respaldo establecida, quien la definió y como se comunicó. d.- Existe un plan de emergencia para las aplicaciones que manejan información crítica y cuando la fue la última vez que se realizó una prueba a este plan.	Las revisiones documentales y evidencias presentadas, determinan el estado de los literales: a) No cumple b) Parcialmente c) No cumple d) No cumple	25/08/2020	PARCIAL	Se evidencia que es requerido articular lo establecido en el Manual de Copias de Seguridad y Recuperación junto con las actividades ejecutadas en la Oficina de Informática y Telecomunicaciones dado que no se están cumpliendo las actividades descritas. El Manual de Copias de Seguridad y Recuperación en la página 10 establece: "Se realizarán las copias de seguridad diarias diferenciales y los sábados son backups Full para las bases de datos", más, sin embargo, en las evidencias allegadas se observa que los backups Full para la base de datos misional fue realizado el día viernes 21 de agosto del 2020. El Manual de Copias de Seguridad y Recuperación en la página 12 establece: "Para la base de datos misional, se genera un Backup Full todos los jueves a la 1:21 a.m., y los backup de archivos (backups diferenciales) todos los días a las 9:20 a.m., 12:20 a.m., 14:20 p.m. y 7:20 p.m.", más sin embargo, en las evidencias allegadas se observa que para el día 21 de agosto solo se ejecutó el de las 7:20 p.m. (19:20 p.m.).

SECRETARIA JURIDICA DISTRITAL

OFICINA DE CONTROL INTERNO

TEMA: SEGUIMIENTO A LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. **CORTE: 31 de agosto del 2020**

No	TEMA A EVALUAR	ACTIVIDAD	DESCRIPCION DE LA EVIDENCIA	FECHA DE ENTREGA DE LA EVIDENCIA	CUMPLE	OBSERVACIONES
1	ISO 27001 - NUMERAL 5.2 POLÍTICA. Revisión de las políticas para la seguridad de la información	La política de la seguridad de la información: e) Está disponible como información documentada. f) Se ha comunicado y/o socializado dentro de la secretaría Jurídica Distrital (Anexar asistencia de la socialización) g) Está disponible para las partes interesadas	Las revisiones documentales y evidencias presentadas, determina el estado de los literales: e) Cumple f) Cumple g) Cumple	21/08/2020	SI	
2	ANEXO A - OBJETIVOS DE CONTROL Y CONTROLES ISO 27001 - A.6.2.1. Política para dispositivos móviles	a) Se adoptó una política y unas medidas de seguridad de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles	Las revisiones documentales y evidencias presentadas, determina el estado del literal: a) Cumple parcialmente	21/08/2020	PARCIAL	En proceso: "La Oficina de Informática y Telecomunicaciones indica que se "encuentra en proceso de adquirir una herramienta tecnológica para protección de la información a través de dispositivos móviles".
3	ANEXO A - OBJETIVOS DE CONTROL Y CONTROLES ISO 27001 - A.6.2.2. Teletrabajo.	a) Se implementó una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso y que es procesada o almacenada en los lugares en los que se realiza teletrabajo	Las revisiones documentales y evidencias presentadas, determina el estado del literal: a) Cumple El teletrabajo en la secretaría es desarrollado a través del uso de VPN dando cumplimiento a lo establecido en el documento: "Manual de Políticas de Seguridad de la Información".	24/08/2020	SI	
4	ANEXO A - OBJETIVOS DE CONTROL Y CONTROLES ISO 27001 - A.9.1.1. Política de Control de Acceso.	Política de control de acceso: a) Se estableció el documento que contempla la política y se revisó la política de control de acceso con base en los propósitos de la secretaría Jurídica Distrital para la seguridad de la información.	Las revisiones documentales y evidencias presentadas, determina el estado del literal: a) Cumple El control de acceso a la infraestructura de TI es gestionado por la Oficina de Informática y Telecomunicaciones a través del diligenciamiento de un formulario de Google.	21/08/2020	SI	
5	ANEXO A - OBJETIVOS DE CONTROL Y CONTROLES ISO 27001 - A.10.1.1. Política sobre el Uso de Controles Criptográficos	Se desarrolló una política sobre el uso de controles Criptográficos para la protección de la información que incluya: a) El enfoque de la dirección con relación al uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se deben proteger la información; b) Se realizó una valoración de los riesgos, que identifican el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido; c) Se utiliza la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación; d) Se Gestionaron las llaves y los métodos para la protección de llaves criptográficas y la recuperación de información encriptada, en el caso de llaves perdidas y llaves cuya seguridad está comprometida; e) Se establecieron los roles y responsabilidades; f) Quién es responsable por: 1) la implementación de la política de controles criptográficos. 2) la gestión de llaves, incluida la generación de llaves.	Las revisiones documentales y evidencias presentadas, determinan el estado de los literales: a) Cumple b) No cumple c) Cumple d) No cumple e) No cumple f) 1.- Cumple 2.- No cumple.	26/08/2020	PARCIAL	Los riesgos que identifican el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido por la secretaría, no han sido identificados. La Oficina de Informática y Telecomunicaciones indica que: "La SJD cuenta con certificados digitales en las páginas web, intranet y los sistemas misionales de acceso a web. Estos certificados digitales son adquiridos y administrados por la Oficina de TIC". Esta es una solución muy provisional. (Va hasta el mes de octubre)
6	ANEXO A - OBJETIVOS DE CONTROL Y CONTROLES ISO 27001 - A.11.2.9 Política de escritorio limpio y pantalla limpia	a) Se creó la política de escritorio limpio y de pantalla para prevenir la perdida, daño, robo o compromiso de la información durante y fuera de las horas laborales, en los equipos de cómputo de los funcionarios de la Secretaría	Revisado los documentos y evidencias presentadas, determina el estado del literal: a) Cumple	21/08/2020	SI	