MANUAL DE POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE CULTURA,
RECREACIÓN Y DEPORTE

SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE

2023

TABLA DE CONTENIDO

1. OBJETIVO

Establecer las directrices, lineamientos y medidas organizacionales, técnicas, físicas, legales y culturales para la adecuada gestión de la seguridad y privacidad de la información; enmarcadas en la implementación del MSPI (Modelo de Seguridad y Privacidad de la Información) definido por el MINTIC, identificando, valorando y gestionando los riesgos asociados a la misma y propendiendo por garantizar la confidencialidad, integridad y disponibilidad de la información durante la ejecución de los objetivos misionales y estratégicos de la Secretaría de Cultura, Recreación y Deporte – SCRD.

2. ALCANCE

En el presente manual se establecen las políticas para la gestión de la seguridad y privacidad de la información, que la SCRD recolecta, procesa, almacena y transmite en desarrollo de su objeto misional y que son de obligatorio cumplimiento para todos los funcionarios públicos, contratistas, proveedores y terceras partes que interactúen con los activos de información en los cuales la SCRD sea responsable, custodio o usuario.

3. GLOSARIO

- **Seguridad de la información:** Es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de inversiones y oportunidades de negocio. Adicionalmente, se define la seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad de la información, además otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas (NTC-ISO/IEC 27002:2013).
- **Confidencialidad:** Aseguramiento de que la información es accesible sólo para quienes están autorizados.
- **Integridad:** Salvaguardia de la exactitud y completitud de la información y sus métodos de procesamiento.
- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando se requiera.
- **Dominios de Control:** La norma NTC/IEC ISO 17799 con su actualización NTC/IEC ISO 27001:2013 define los dominios de control, como una guía que permite garantizar la seguridad de la información, mediante el empleo de los 14 dominios de control que conforman la guía.
- **Activos de información:** Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.
- **Información:** La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la Entidad y, en consecuencia, necesita una protección adecuada (ISO/IEC 27002:2013).

- **Clasificación de la Información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados a nivel corporativo. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado. La información debe clasificarse en términos de la sensibilidad y la importancia para la Entidad.
- **Propietario de la Información:** Es una parte designada de la Entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada, y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida.
- **Custodio de la Información:** Es una parte designada de la Entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (Toma de copias de seguridad, asignar privilegios de: Acceso, Modificaciones, Borrado) que el propietario de la información haya definido, con base en los controles de seguridad disponibles en la Entidad.
- **Usuario:** Cualquier persona que genere, obtenga, transforme, conserve o utilice información de la Entidad en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la compañía. Son las personas que utilizan la información para propósitos propios de su labor, adecuados y que tendrán el derecho manifiesto de uso dentro del inventario de información.
- **SGSPI:** Sistema de Gestión de Seguridad y Privacidad de la Información.
- **SCRD:** Secretaría de Cultura Recreación y Deporte.
- **COLCERT:** Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT.
- **CSIRT:** Equipo de respuesta a incidentes informáticos.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.

4. REFERENCIAS INFORMATIVAS.

- Norma ISO/IEC 27001:2013: Sistema de Gestión de Seguridad de la Información (SGSI).
- Norma ISO/IEC 27002:2013: Código de Prácticas para la Gestión de la Seguridad de la Información.
- Norma ISO/IEC 27005:2008: Gestión de Riesgo de Seguridad de la Información.
- Ley 1581 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Ley 1712 de 2014, “Por medio de la cual se crea la Ley 1712 de 2014 - Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- Decreto 1008 de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

5. DEFINICIONES DEL SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1. COMPROMISO DE LA DIRECCIÓN

La Secretaría de Cultura, Recreación y Deporte está comprometida con la protección de la confidencialidad, integridad y disponibilidad de los activos de información como parte fundamental y estratégica orientada a la continuidad de la operación tecnológica de la Entidad, la administración de riesgos y la formación de una cultura en seguridad de la información.

Al ser conscientes de los riesgos de seguridad a los cuales se encuentran expuestos los activos de información, la SCRD ha definido un modelo de gestión para el SGSPI como herramienta de cumplimiento de requerimientos legales, contractuales, regulatorios y de mejora continua.

El proceso de identificación de activos y análisis de riesgos de los activos de información es el soporte fundamental para el desarrollo de las políticas de seguridad y privacidad de la información, los controles y actividades implementadas para la obtención de los niveles de protección esperados al interior de la SCRD, y cuyos procesos son liderados de manera permanente por la Oficina de Tecnologías de la Información.

La Alta Dirección de la Secretaría de Cultura, Recreación y Deporte, apoya de manera activa el establecimiento, mantenimiento y mejora continua del SGSPI, a través de:

- Revisiones periódicas de los temas relacionados con el SGSPI.
- Revisiones periódicas a las políticas de seguridad y privacidad de la información, así como también el cumplimiento de estas.
- Asignación de los recursos necesarios para la definición, establecimiento, implementación, mantenimiento y mejora continua del SGSPI.
- Promoviendo la importancia del SGSPI y la formación de una cultura organizacional en seguridad y privacidad de la información al interior de la SCRD.
- Promoviendo la mejora continua del SGSPI.
- Apoyando el cumplimiento del modelo seguridad y privacidad de la información definido por el MINTIC, y las normas y estándares que lo complementen.

5.2. RESPONSABILIDAD

Es responsabilidad de las Subsecretarias, Direcciones, Subdirecciones y Jefes de Oficina de la Secretaría de Cultura, Recreación y Deporte dar cumplimiento a las políticas de seguridad y privacidad de la información, estándares, normativa vigente y procedimientos como parte de sus herramientas de gobierno y gestión, que garanticen el cumplimiento y mejora del SGSPI.

5.3. CUMPLIMIENTO Y VIOLACIONES

El cumplimiento de las Políticas de Seguridad y Privacidad de la Información es obligatorio y aplica para todos los funcionarios públicos, contratistas, proveedores y terceras partes que interactúen con los activos de información de propiedad de la entidad o en calidad de propietario, custodio o usuario. Si los parámetros aquí descritos se infringen, la Secretaría de Cultura, Recreación y Deporte se

reservará el derecho de tomar las medidas correctivas pertinentes, las cuales pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

5.4. EXCEPCIONES

Las excepciones a cualquier cumplimiento de las Políticas de Seguridad y Privacidad de la Información deberán ser pre-aprobadas por la Oficina de Tecnologías de la Información y contar con la autorización del Comité Institucional de Gestión y Desempeño. Por lo tanto, toda excepción deberá ser formalmente documentada, registrada y revisada por las partes aquí indicadas.

5.5. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Toda política de seguridad y privacidad de la información nueva, actualizada, y/o eliminada, será propuesta por la Oficina de Tecnologías de la Información y será aprobada por la jefe de la Oficina de Tecnología de la Información, los roles y responsabilidades serán revisados y concertados con las partes interesadas, esta política será revisada por la OTI para garantizar que siga siendo idónea y pertinente, dicha actividad se realizará como mínimo una vez al año y/o si surten cambios sustanciales que ameriten su actualización.

5.6. VIGENCIA DEL DOCUMENTO

Las Políticas contenidas en el presente documento estarán vigentes desde la fecha de su aprobación. La versión oficial de este documento para funcionarios públicos, contratistas y terceros, será la que se encuentre aprobada y publicada en la intranet en el micrositio MIPG/ Sistema de Gestión.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1. ORGANIZACIÓN INTERNA

6.1.1. Roles y responsabilidades para la seguridad de la información

Todos los funcionarios públicos, contratistas y terceros de la SCRD, deben conocer y dar cumplimiento al modelo de seguridad y privacidad de la información establecido en la Entidad, así mismo la gestión de la seguridad y privacidad de la información es un proceso incluyente de todos los niveles organizacionales de la entidad (Estratégico, Táctico, Operacional y Comunidad), por tal motivo la SCRD, define y asigna los roles y responsabilidades para el cumplimiento del SGSPI (sistema de gestión de seguridad y privacidad de la información).

I. Nivel Estratégico

Rol Comité Institucional de Gestión y Desempeño – Seguridad de la Información

Responsable de la aprobación, divulgación de las políticas de seguridad de la información y comunicación de los roles y autoridades en seguridad de la información a las partes interesadas.

Rol Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información:

Asume la responsabilidad en torno a la planeación, ejecución, cumplimiento y mejora continua de los temas asociados al SGSPI de la SCRD. Este equipo se encuentra conformado por:

- Jefe de la Oficina de Tecnologías de la Información – Secretaria Técnica del Comité

Participantes:

- Director de Gestión Corporativa – Líder Equipo Técnico del Comité
- Jefe Oficina Asesora de Planeación
- Coordinador de Grupo Interno de trabajo de Servicios Tecnológicos (apoya seguridad de la información cuando se requiera.
- Coordinador de Grupo Interno de trabajo de Gestión de Servicios Administrativos
- Coordinador de Grupo Interno de trabajo de Gestión del Talento Humano
- Jefe de Control Interno (tiene voz pero no voto)

Dentro de los roles y responsabilidades del Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información se encuentran:

- Establecer las estrategias, metas, indicadores, acciones y cronograma de trabajo para lograr la implementación de las normas requeridas.
- Definir, diseñar e implementar acciones, lineamientos, herramientas e instrumentos para la implementación y mantenimiento de las políticas de Gobierno y seguridad digital.
- Revisar los resultados de las auditorías internas, que les corresponden, con el fin de establecer, ejecutar, hacer seguimiento a las acciones de mejora.
- Presentar al Comité Institucional de Gestión y Desempeño los avances y requerimientos para la implementación y mejoramiento del sistema -MIPG.

II. Nivel Táctico

Rol Director(a) de Gestión Corporativa:

Su función como Líder de Gestión Corporativa es hacer cumplir los compromisos establecidos en el Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información y proponer mejoras en el SGSPI con el apoyo de las dependencias que se encuentran bajo su cargo, sus responsabilidades son:

- Coordinar, velar por el cumplimiento de los compromisos establecidos en el Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información.
- Validar la implementación y correcto funcionamiento de los requisitos de seguridad aprobados por el Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información.

- Asesorar al Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información en la definición de requisitos y medidas de seguridad de acceso físico que se deben adoptar.
- Validar y proponer al Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información el alcance y límites del SGSI en términos del negocio, límites físicos, activos de información y TIC.

Rol Jefe de la Oficina de Tecnologías de la Información:

Su función como Líder de la Oficina de Tecnologías de la Información es coordinar y controlar las medidas y buenas prácticas de seguridad informática aplicables en la SCRD, sus responsabilidades son:

- Coordinar y velar por el cumplimiento de los compromisos establecidos en el Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información.
    - Gestión para la implementación de políticas, lineamientos, normas, estándares y procedimientos sobre seguridad informática.
- Gestión para la adquisición y administración de las herramientas de seguridad informática necesarias para el aseguramiento y/o monitoreo de la infraestructura tecnológica de la Entidad.
- Participación en la identificación y mitigación de riesgos y vulnerabilidades de seguridad y privacidad de la Información.
- Gestión de proyectos de seguridad y privacidad de la información.
- Gestión de incidentes en seguridad y privacidad de la Información.
- Realizar revisiones periódicas a los sistemas de información y establecer los controles, medidas técnicas y organizativas al interior de la entidad.
- Informar al Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información acerca del desempeño del SGSPI.
- Elaborar y enviar las actas de reunión y someterlas a aprobación por los miembros que conforman el Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información.
- Convocar las reuniones del Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información, por solicitud del líder del Comité.

Rol Oficial de Seguridad y Privacidad de la Información:

Su función como Oficial de Seguridad y Privacidad de la Información en la entidad, es mantener, revisar, gestionar y mejorar el SGSPI al interior de la SCRD, sus responsabilidades son:

- Identificación, análisis y gestión de riesgos, de seguridad y privacidad de la Información, así como también la coordinación en la gestión e implementación de controles alineados a la ISO 27001 y buenas prácticas vigentes.
- Definición de políticas, lineamientos, normas, estándares y procedimientos sobre seguridad y privacidad de la información.

- Definir e implementar indicadores de Seguridad y privacidad de la información.
- Monitoreo y medición del cumplimiento de políticas, lineamientos, normas, estándares y procedimientos en Seguridad y privacidad de la Información.
- Realizar análisis y reporte de vulnerabilidades de seguridad y privacidad de la información, así como también gestión en el desarrollo de los respectivos planes de remediación.
- Realizar y gestionar capacitaciones, sensibilizaciones y entrenamientos en los temas relacionados con seguridad y privacidad de la información.
- Gestionar Incidentes de seguridad y privacidad de la información con el apoyo de los grupos involucrados.
- Implementación de proyectos de cumplimiento normativo en relación con la seguridad y privacidad de la información.
- Apoyar al Jefe de la Oficina de Tecnologías de la Información con la gestión y análisis de incidentes de seguridad y mantener informado al Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información acerca de los incidentes presentados.
- Apoyar y promover la formación y cultura de seguridad privacidad de la información en la Entidad.

Rol Oficina de Control Interno:

- Realizar las auditorías al MSPI a partir de la identificación de los criterios establecidos para la priorización de las unidades auditables y la incorporación y aprobación del plan anual de auditoría interna, por parte del Comité Institucional de Coordinación de Control Interno.

Rol Oficina Control Interno Disciplinario:

- Determinación de la pertinencia de abrir procesos disciplinarios y/o sanciones por el incumplimiento de políticas y lineamientos de seguridad y privacidad de la información y/u ocurrencia de incidentes que involucren a funcionarios públicos de la SCRD, acorde con lo estipulado en el Código Único Disciplinario (Ley 734 de 2002), o las normas que lo modifiquen o complementen.

Rol Jefe Oficina Asesora de Planeación:

Su función como Líder de Planeación es mantener armonizados los Sistemas de Gestión al interior de la entidad, sus responsabilidades son:

- Dar lineamientos en la documentación del Sistema de Gestión- MIPG frente a la Seguridad de la Información, de acuerdo con lo establecido en el presente manual.
- Verificar y monitorear la implementación de los compromisos que se definan por el Equipo Técnico de Gestión Desempeño Institucional de Seguridad de la Información.
- Verificar que la documentación cumpla con los lineamientos del Sistema de Gestión- MIPG, frente a la Seguridad de la Información, de acuerdo con las solicitudes de elaboración y actualización de los documentos.
- Integrar los riesgos de Seguridad de la información en la metodología y herramientas de los riesgos de gestión y corrupción de la entidad con el acompañamiento de la OTI.

III. Nivel Operacional

Rol Asesor de Seguridad y Privacidad de la Información:

Su función como Asesor de seguridad y privacidad de la Información es la asignada por el SGSPI y por el equipo de Seguridad de la Información de la entidad para ejecutar y gestionar actividades relacionadas en el diseño, definición, implementación, mantenimiento y mejora continua del SGSPI, dentro de sus responsabilidades se encuentran:

- Asistir, apoyar y participar en las mesas de trabajo establecidas por el Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información para la definición, implementación, mantenimiento y mejora del SGSPI al interior de la SCRD, e informar el estado de avance de estas.
- Asesorar al Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información en la definición de requisitos y medidas necesarias que se deben adoptar.
- Apoyar e impulsar la cultura de seguridad y privacidad de la información en la SCRD.
- Apoyar en la gestión de proyectos de seguridad y privacidad de la información.
- Apoyar en la definición y gestión de riesgos de seguridad y privacidad de la información.

Rol Líderes de procesos:

Son los encargados de liderar los diferentes procesos en la SCRD.

- Proponer políticas, lineamientos, normas, estándares y procedimientos sobre la seguridad física, digital y las relacionadas con la gestión documental.
- Proponer e implementar controles de seguridad física y digital, así como realizar seguimiento a la efectividad de los mismos.
- Incluir controles y mecanismos de seguridad de la información en todos los proyectos, procesos contractuales e iniciativas de TI que adelanten al interior de sus procesos y dependencias y a la operación en general.
- Definir e implementar políticas, lineamientos, normas, estándares de seguridad de la información en los procedimientos relacionados con Talento humano de la SCRD.
- Apoyar la identificación y clasificación de activos de información y la identificación y análisis de riesgos de seguridad de la información y sus respectivos planes de tratamiento.
- Definir e implementar políticas, lineamientos, normas, estándares, cláusulas y demás relacionados con seguridad de la información en los procesos de contratación.

IV. Nivel Colaboradores

Rol Colaboradores de la SCRD:

Los colaboradores son todos los funcionarios públicos, contratistas y proveedores que hacen parte de la Secretaría de Cultura, Recreación y Deporte, dentro de sus responsabilidades frente al SGSPI se encuentran:

- Conocer y cumplir con las políticas, estándares, lineamientos y procedimientos de seguridad de la información establecidos por el Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información y que se encuentran en el presente documento.
- Salvaguardar los principios de seguridad de los activos de información.
- Asistir a las capacitaciones y sensibilizaciones que programe la Entidad en temas de Seguridad de la Información
- Reportar de eventos e incidentes de Seguridad de la Información y apoyo en la atención e investigación del mismos.
- Apoyar respuesta a requerimientos internos y externos en materia de Seguridad y Privacidad de la Información.
- Apoyar la identificación y clasificación de activos de información y la identificación y análisis de riesgos de seguridad de la información y sus respectivos planes de tratamiento.
- Aplicar y cumplir los controles para la protección de la información.

6.1.2. Segregación de Funciones

La SCRD cuenta con una estructura organizacional de 19 dependencias y 16, con el fin de evidenciar la relación existente entre los diferentes colaboradores de la entidad y la cual permite identificar la segregación de funciones en los cargos, además de evidenciar las responsabilidades y autoridades específicas para cada uno de los mismos.

La Dirección de la SCRD se asegura de la comprensión de las responsabilidades y autoridades de cada cargo, mediante la comunicación del decreto 340 del 30 de diciembre de 2020, “Por el cual se modifica la estructura organizacional de la Secretaría Distrital de Cultura, Recreación y Deporte y se dictan otras disposiciones.” y la Resolución 327 del 31 de mayo de 2022 “Por medio de la cual se actualiza y modifica el Comité Institucional de Gestión y Desempeño de la Secretaría Distrital de Cultura, Recreación y Deporte”.

6.1.3. Contacto con las autoridades

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de Seguridad y privacidad de la Información, se mantendrán contactos con las entidades competentes en caso de que se presentara un incidente de cualquier índole que pueda colocar en riesgo la confidencialidad, integridad y disponibilidad y de la información de la SCRD, en caso de requerirse el llamado a las autoridades mencionadas, sólo podrán hacerlo los funcionarios públicos encargados en cuyo caso es el Jefe de la Oficina de Tecnologías de la Información y el Oficial de Seguridad y Privacidad de Información. En la Guía de Contacto con las autoridades y grupos de interés especial se encuentra el listado actualizado. Sin embargo, se listan a continuación algunas entidades:

- COLCERT Grupo de Respuesta a Emergencias Cibernéticas
- Centro Cibernético de la Policía Nacional
- CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia Unidad de delitos informáticos de la DIJIN.
- CAI virtual

6.1.4. Contacto con Grupos de Interés Especial

A efecto de intercambiar experiencias y aumentar la red de apoyo en los temas relacionados con seguridad y privacidad de la información de la SCRD. El Jefe de La Oficina de Tecnologías de la Información y el Oficial de Seguridad y Privacidad de la Información, serán los encargados de coordinar los acercamientos con los contactos permanentes de diferentes sectores del distrito, de orden nacional o internacional, instituciones académicas, proveedores o entidades privadas, a fin de obtener conceptos y elevar las capacidades técnicas y administrativas del equipo de Seguridad, además de poder brindar apoyo en la toma de decisiones en materia de seguridad y privacidad de la información de la SCRD. En la Guía de Contacto con las autoridades y grupos de interés especial, se determina el detalle y el listado de contactos.

6.1.5. Seguridad de la información en la gestión de proyectos

Todos los proyectos que se desarrollen en el marco del cumplimiento de los objetivos de los procesos de la SCRD deben considerar los riesgos de seguridad y privacidad de la información.

Por lo anterior y con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información en todas las etapas de los proyectos, la SCRD gestionará la seguridad y privacidad de la información desde el diseño de todos aquellos productos y servicios que se requieran adquirir, implementar y/o desarrollar. Para este fin la SCRD tendrá en cuenta los siguientes aspectos:

- Se debe determinar la criticidad de la información que se utilizará en el proyecto. Esto se hará con base en la clasificación de los activos de información.
- Se debe evaluar la necesidad de uso de los datos recogidos teniendo en cuenta lo establecido en el principio de proporcionalidad.
- Se debe realizar un análisis de riesgos para revisar y confirmar los controles de seguridad, de acuerdo con las obligaciones regulatorias, legales y contractuales en cada uno de los proyectos que se tengan.
- Se debe definir el tiempo que la información será utilizada, los periodos de conservación y el acceso a ésta.
- Se debe incluir controles para proteger la privacidad de la información, en especial de los datos personales en el análisis de riesgos previo al proyecto.
- Teniendo en cuenta los datos personales administrados en el proyecto, se deben gestionar las autorizaciones a que haya de tratamiento de estos datos, e informar de manera clara y oportuna a los titulares de dichos datos, la finalidad del uso de los datos.
- Evaluar si en el proyecto van a participar terceros, en cuyo caso se deben gestionar las cláusulas respectivas de cumplimiento de las normas exigidas por los diferentes entes de control, la autorización de tratamiento de datos, cláusulas de confidencialidad de la información y de aceptación de las políticas de seguridad. Lo anterior incluye acuerdos de intercambio de información física y/o electrónica.

- Verificar, en cada fase del proyecto, el cumplimiento de la Ley de Protección de Datos Personales, las políticas de seguridad de la información de la SCRD y las normas que se consideren relacionadas al proyecto en materia de seguridad de la información a todos los actores del proyecto, incluyendo los terceros involucrados.

- Si el proyecto incluye el desarrollo de sistemas de información, se deben llevar a cabo buenas prácticas de desarrollo seguro y pruebas de penetración para gestionar desde el inicio las debilidades de seguridad que se puedan presentar.

- Al finalizar el proyecto, o bien al finalizar la participación de uno o más actores del proyecto, cada actor en mención debe hacer entrega de toda la información a la que haya tenido acceso en el marco de su participación.

6.2. DISPOSITIVOS MOVILES Y TELETRABAJO

6.2.1. Políticas para dispositivos móviles

La SCRD reconoce como dispositivos móviles los equipos portátiles, teléfonos móviles, tabletas y cualquier otro que permita la portabilidad y visualización de la información, ya que en estos dispositivos se almacena información usada para el cumplimiento de los objetivos misionales y estratégicos de la Entidad.

La SCRD debe controlar la seguridad de la información cuando se utiliza medios de computación móvil, por tal motivo este documento establece los siguientes controles necesarios y pertinentes para salvaguardar la información:

- El uso de dispositivos móviles en interacción con la infraestructura para el procesamiento de la información de la SCRD, estará autorizado para aquellos colaboradores cuyo perfil del cargo y funciones lo requiera de mutuo acuerdo entre todas las dependencias y la Oficina de Tecnologías de la Información. Así mismo, a quien se le haya autorizado el uso de alguno de los dispositivos enunciados, se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de la Entidad.

- Cualquier funcionario o tercero autorizado para el uso de dispositivos móviles en la entidad y que requiera tener acceso a la información desde redes externas, podrá acceder remotamente mediante un proceso de autenticación, a través del uso de conexiones seguras y asegurando el cumplimiento de requisitos de seguridad de los equipos desde los que se accede. Estos recursos tecnológicos y de seguridad para las conexiones externas deben ser provistos por La Oficina de Tecnologías de la Información.

- La SCRD se propone con la presente política, concientizar a los funcionarios públicos, contratistas y colaboradores sobre los riesgos asociados con el uso de los dispositivos móviles, tanto para los sistemas de información como para la infraestructura tecnológica de la Entidad, asegurar el correcto manejo de la información digital que reposa en la SCRD.

- La SCRD se reserva el derecho de monitorear el uso de dispositivos móviles siempre y cuando hagan uso de la infraestructura tecnológica de la Entidad, siempre respetando y preservando el derecho a la intimidad.

- El colaborador que utilice dispositivos móviles de su propiedad es responsable de su seguridad física, por tal motivo se recomienda el uso de guayas, así mismo, deben ser guardados bajo llave en el caso de estar desatendidos.

6.2.2. Teletrabajo y/o Trabajo en casa

Por medio de la resolución 354 del 25 de mayo de 2021 se implementó la modalidad de Teletrabajo para los funcionarios públicos de la Secretaría Distrital de Cultura, Recreación y Deporte Para aquellos cargos cuyas funciones establecidas en el respectivo manual específico de funciones y de competencias laborales puedan ser desarrolladas sin requerir la presencia física del servidor (a) público (a) que las ejerce en un sitio específico de trabajo, que sean identificadas como teletrabajables, se suscribirá un acuerdo previo y legalizado a través del "Acuerdo de voluntariedad de teletrabajo", el cual será firmado por el servidor(ra), el jefe inmediato y el Director(ra) de Gestión Corporativa, en el que se establecerán las condiciones de aplicación, los deberes y derechos del Teletrabajador y los deberes de la Secretaría.

El teletrabajo está implementado teniendo en cuenta lo establecido en:

- La Ley 1221 de 2008 en el artículo 2, establece normas para promover y regular el Teletrabajo.
- El Decreto 884 de 2012 reglamentó la Ley 1221 de 2008, cuyo fin es establecer las condiciones laborales especiales del Teletrabajo que regirán las relaciones entre empleadores y teletrabajadores.
- En el Decreto Distrital 806 del 24 de diciembre de 2019, se dictan disposiciones para la implementación, apropiación, adopción, fomento y sostenibilidad del Teletrabajo en organismos y entidades Distritales.
- El proceso de Talento Humano se encargará de llevar el registro de los Teletrabajadores al servicio de la SCRD; en dicho registro se incluirá la información correspondiente a la identificación de cada uno, la ubicación de su puesto de trabajo, los teléfonos de contacto, las fechas de vigencia del mismo, la modalidad aplicable (identificando plenamente los días que deberá realizar sus labores desde su domicilio y los días que lo hará en la Entidad), la identificación de los equipos de cómputo que le fueron asignados, entre otros.
- La Oficina de Tecnologías de la Información será el encargado de implementar los controles de seguridad físicos y tecnológicos necesarios para proteger la confidencialidad, integridad y disponibilidad de la información en la modalidad de Teletrabajo.
- Las herramientas oficiales de chat y reuniones aprobadas por la SCRD, son las de GOOGLE, las cuales todos los funcionarios públicos deben mantener activas durante su horario laboral y responder con la debida diligencia, tal como si estuviesen realizando sus funciones y actividades en las instalaciones físicas de la entidad.
- El acceso remoto se puede realizar desde equipos propiedad de la Entidad y equipos de propiedad de los funcionarios públicos, contratistas y terceros debidamente autorizados y configurados por la Oficina de Tecnologías de la Información.
- Los funcionarios públicos bajo la modalidad de teletrabajo en la SCRD, que tengan conexión remota, no deben instalar ningún software, programa o aplicativo en los equipos designados para su labor en la entidad.
- La Oficina de Tecnologías de la Información, o a quien designe, debe establecer y verificar los criterios tecnológicos establecidos para los Teletrabajadores y los parámetros de seguridad de la información necesarios.

- La Oficina de Tecnologías de la Información o a quien designe, debe verificar periódicamente la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la SCRD.
- El Oficial de Seguridad de la Información será el encargado de socializar las medidas de seguridad y privacidad, las buenas prácticas para proteger la información en la modalidad de teletrabajo.
- Los equipos de cómputo que se usen para teletrabajo deben tener instalada la misma línea base de software que los equipos que se usan en la SCRD.
- Los equipos en los que se realice teletrabajo deben contar con protección contra software malicioso debidamente actualizado.
- Es responsabilidad de los usuarios realizar copias de respaldo de la información de forma mensual y organizarla en su repositorio de Drive, para asegurar la continuidad de las funciones realizadas.
- En caso de pérdida, suplantación de identidad o robo de un equipo, dispositivo móvil o cualquier medio de almacenamiento que contenga información de la SCRD, debe ser reportada inmediatamente a la mesa de ayuda y realizar la respectiva denuncia ante las autoridades competentes.

7. SEGURIDAD EN EL RECURSO HUMANO

7.1. ANTES DE ASUMIR EL EMPLEO

7.1.1. Selección

En el proceso de selección el Grupo Interno de trabajo de Gestión del Talento Humano debe establecer los siguientes controles:

- Solicitar autorización para el tratamiento de los datos personales de los aspirantes para llevar a cabo el proceso de selección.
- Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

7.1.2. Términos y condiciones del empleo

Se deben hacer acuerdos contractuales con los funcionarios públicos, contratistas y terceros, para establecer sus responsabilidades y las de la SCRD en cuanto a la seguridad y privacidad de la información y los datos personales a los que va a tener acceso en virtud del vínculo contractual, por tal motivo es indispensable el cumplimiento de los siguientes controles:

- Todos los funcionarios públicos, contratistas y terceros de la SCRD deben aceptar y firmar los términos y condiciones de su nombramiento y/o contrato, en el cual se establecen sus responsabilidades y las de la entidad para la seguridad y privacidad de la información, así como también las cláusulas de confidencialidad, buen uso de credenciales de acceso, propiedad y autorización de tratamiento de datos personales definidas por la Entidad, antes

de asumir su contratación y/o cualquier prestación de servicios, dichas cláusulas harán parte integral en cada uno de los contratos; de la misma forma las acciones a tomar si no se cumple con los términos y condiciones laborales.

7.2. DURANTE LA EJECUCIÓN DEL EMPLEO

7.2.1. Responsabilidades de la Alta Dirección

- Es responsabilidad de la dirección de la SCRD, la exigencia del cumplimiento normativo interno y externo de la entidad, así como también la adopción del presente documento como parte integral del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI.

7.2.2. Toma de conciencia, educación y formación en la seguridad de la información

- Todos los funcionarios públicos, contratistas y terceros, deben asistir a las inducciones que se realicen del SGSPI o sensibilizaciones en seguridad de la información, cuyo objetivo es fortalecer las capacidades en el buen tratamiento de la información de la SCRD.
- En los procesos de inducción, sensibilización y entrenamiento que se efectúen, se debe informar a los colaboradores sobre los riesgos comunes de seguridad de la información a los que la SCRD se encuentra expuesta, los requerimientos y lineamientos de seguridad establecidos, las buenas prácticas, sus deberes y derechos en la materia y sus responsabilidades frente al incumplimiento. Así mismo, se debe brindar información relacionada con el uso seguro de los activos de información.
- Cuando los lineamientos de seguridad de la información aplique a usuarios externos, proveedores y otros terceros por la naturaleza de su relación con la SCRD o por disposición contractual, dichos lineamientos deben ser puestos en su conocimiento.
- Todos los funcionarios públicos, contratistas y terceros antiguos deben participar en las sensibilizaciones y/o capacitaciones en temas de Seguridad y Privacidad de la Información, una vez al año y/o conforme al plan institucional de capacitación para funcionarios públicos, o a nivel de transferencia de conocimiento para los contratistas y terceros.

7.2.3. Proceso disciplinario

- Se debe contar con un proceso formal y comunicado, para emprender acciones contra funcionarios que hayan cometido una violación a las políticas de seguridad de la información.
- Si las políticas aquí descritas se infringen, la Secretaría de Cultura, Recreación y Deporte se reservará el derecho de tomar las medidas correctivas que estime pertinentes, las cuales pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario u otras que apliquen.

7.3. TERMINACIÓN Y CAMBIO DE EMPLEO

7.3.1. Responsabilidades en la terminación o cambio de empleo

- El Grupo Interno de trabajo de Gestión del Talento Humano, la Oficina de Tecnologías de la Información, el Grupo Interno de trabajo de Gestión de Servicios Administrativos y el Jefe Inmediato del funcionario y/o supervisor del contratista, serán los encargados del proceso de terminación de labores y asegurarán que todos los activos propios de la Entidad sean

devueltos, los accesos físicos y lógicos sean eliminados, y la información pertinente sea transferida, de acuerdo con los procedimientos que se encuentran establecidos en el Sistema Integrado de Gestión.

- En caso de que un funcionario y/o contratista tenga un cambio de funciones, se deben seguir los mismos procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, la transferencia de información y la posterior entrega de los mismos de acuerdo a su nuevo rol.
- Es responsabilidad del Grupo Interno de trabajo de Gestión del Talento Humano y del Grupo Interno de trabajo de Contratación, notificar a las diferentes dependencias, mediante un informe o reporte por mesa de ayuda que se entregue a más tardar los 5 primeros días hábiles del mes, frente a la terminación de las relaciones laborales de funcionarios públicos y/o de los contratos de prestación de servicios, para que se realicen los procesos verificación de deshabilitación de acceso a los servicios tecnológicos y físicos, así como la verificación de la devolución de activos.
- La Oficina de Tecnologías de la Información realizará el monitoreo sobre la gestión de roles y perfiles de acceso a la plataforma tecnológica de la SCRD en la terminación contractual o desvinculación de la Entidad.

8. GESTIÓN DE ACTIVOS.

La Secretaría de Cultura, Recreación y Deporte cuenta con una metodología, procedimiento y formato para identificar, clasificar y valorar los activos de información de todos los procesos al interior de la Entidad.

8.1. RESPONSABILIDAD POR LOS ACTIVOS DE INFORMACIÓN

8.1.1. Inventario de Activos de Información

El inventario de los activos de información se hace con el fin de identificar cuáles son los más importantes o críticos para la SCRD, para darle el tratamiento de seguridad adecuado en el cumplimiento de los objetivos misionales y estratégicos de la Entidad.

- Toda la información producida, gestionada y transmitida, haciendo uso de los recursos físicos y tecnológicos de la SCRD es de propiedad de la Entidad, a menos que se especifique lo contrario a través de un contrato u otro medio legal suscrito por el Representante legal de la Entidad. Por ello, el tratamiento de la información institucional está sujeto a lo establecido en las cláusulas de propiedad intelectual y confidencialidad incluidas en los contratos establecidos con los colaboradores y en los contenidos de este manual, con el objeto de garantizar que no se realice uso de ésta, con propósitos personales comerciales o de otra índole.
- Todos los funcionarios públicos, contratistas y terceros deben hacer entrega de los activos de información que se encuentran bajo su custodia al terminar su contrato y/o cada vez que el mismo haga cambio de dependencia o responsabilidades al interior de la SCRD.

- Para la disposición final de los activos de información de tipo “información” se deberá seguir lo dispuesto por Gestión Documental.

8.1.2. Propiedad de los activos

La propiedad del activo se le debe asignar a un cargo, un proceso o grupo de trabajo que tendrá la responsabilidad de garantizar que la información y los activos asociados con los procesos se gestione de manera adecuada. Por tal razón el propietario del activo de información en la SCRD deberá:

- Cada activo de información de la Entidad debe tener un propietario y un custodio, deben clasificarlos de acuerdo con la metodología de identificación y clasificación definida por la Oficina TIC
- Asegurarse de que el activo asignado se encuentra en el inventario de la SCRD.
- Asegurar que los activos estén clasificados y protegidos apropiadamente.
- Definir y revisar periódicamente las restricciones de acceso y las clasificaciones.

8.1.3. Uso aceptable de activos

Todos los colaboradores a los que se la haya asignado activos de información para el desarrollo de sus funciones contractuales o laborales, deben cumplir los siguientes lineamientos:

- **Uso aceptable de la información**

- Toda actividad de administración y operación que se realice con los activos de información de propiedad de la SCRD, deben estar orientadas única y exclusivamente a cumplir con los objetivos misionales y estratégicos de la Entidad.
- Todos los colaboradores deben aplicar los controles de seguridad definidos en el presente manual, para reducir riesgos que afecten la integridad, confidencialidad y disponibilidad de los activos de información.
- Los activos de información que almacenen o usen datos personales “privados, sensibles y de niños niñas y adolescentes”, tendrán acceso controlado que será garantizado por el propietario y el responsable de la custodia de la información.
- Ningún colaborador puede compartir sus credenciales de autenticación para acceder a los activos de información.
- Cualquier modificación que se le deba hacer a los activos de información, debe ser autorizada y verificada por su propietario.
- Todos los colaboradores deben reportar a la Oficina de Tecnologías de la Información mediante la mesa de ayuda, cualquier evento que pueda afectar la integridad, disponibilidad y confidencialidad de cualquier activo de información.
- Todos los funcionarios públicos y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Es responsabilidad de todos los funcionarios públicos y contratistas o colaboradores de la Secretaría Distrital de Cultura, Recreación y Deporte reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los activos de información.

- No está permitido el uso de los recursos tecnológicos para difundir o participar en actividades de partidos y movimientos políticos.

- **Uso aceptable equipos de computo**

- A los colaboradores de la SCRD que para el cumplimiento de sus obligaciones requieran del uso de un equipo de cómputo, se les podrá asignar y entregar uno de escritorio o portátil de acuerdo a la disponibilidad, una vez legalizado su contrato o vinculación con la Entidad. Una vez efectiva la entrega, los colaboradores son responsables por todos los elementos que se encuentren incorporados o hacen parte del equipo asignado (CPU, Teclado, Mouse, Pantalla, entre otros). Dicha responsabilidad se debe confirmar a través de la firma de un registro o acta de entrega en la cual se relacionan los activos asignados.

- La configuración, instalación, desinstalación y mantenimiento de hardware y software operativo, base, de aplicación y utilitario de los equipos de cómputo y de los dispositivos periféricos como impresoras o escáner, así como equipos de comunicaciones como Router, Switch y Access Point, son responsabilidad única de la Oficina de Tecnologías de la Información de la SCRD.

- Los colaboradores tienen prohibido instalar software no autorizado en los equipos de cómputo de la SCRD.

- **Uso aceptable del correo corporativo**

- Los colaboradores de la SCRD no deben emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos de la Entidad, en especial, cuentas de correo personal.

- La responsabilidad del contenido de los mensajes de correo electrónico es del usuario remitente. En los procesos de reenvío de estos, no se deben alterar los datos originales.

- No está permitido crear, enviar o retransmitir mensajes de correo electrónico que contengan contenido textual y/o gráfico que constituya acoso, que puedan contribuir a un ambiente de convivencia hostil, o que sean considerados difamatorios, explícitamente sexuales o que puedan ofender a alguien con base en su raza, género, nacionalidad, orientación sexual, religiosa o política, apariencia física, estrato social o discapacidad.

- Está prohibida la generación, reproducción y envío de mensajes en cadenas o similares, debido a que esto puede habilitar la propagación de código malicioso (virus, troyanos, entre otros), saturar el tráfico de correo causando indisponibilidad del servicio o provocar fuga de información a través de mecanismos como spam, phishing, entre otros.

- En caso de requerirse enviar un correo masivo para informar algo fuera del contexto institucional, como eventos sociales, clasificados, publicidad y ubicación de objetos perdidos, entre otros, debe solicitarse la publicación a través del proceso de comunicaciones para dirigir la información a quién corresponda. Igualmente, es posible solicitar la publicación de dicha información en el portal corporativo de la SCRD.

- El envío de mensajes a grupos de usuarios múltiples como “funcionarios públicos y contratistas” cuyo tamaño pueda ocasionar saturación en el tráfico de la red, pone en riesgo la disponibilidad de los servicios informáticos de la Entidad al exceder su capacidad, por lo que este servicio debe habilitarse exclusivamente para las dependencias que lo soliciten a través de la mesa de ayuda, con su respectiva justificación.

- Los mensajes de procedencia dudosa o desconocida no deben ser respondidos y deben ser clasificados por el usuario en su cliente de Gmail como correo no deseado. Lo anterior con el objeto de mitigar los riesgos relacionados con eventos de phishing, spam, Scamming, entre otros.
- A pesar de que las herramientas tecnológicas institucionales como el antivirus, realizan un análisis de los archivos adjuntos de correo, para determinar si éstos contienen código malicioso, no se deben descargar archivos adjuntos de destinatarios desconocidos o sospechosos.
- La Oficina de Tecnologías de la Información debe configurar para todos los mensajes que se dirigen a destinatarios externos, una advertencia de seguridad estándar que se adjunte a la firma y que especifique como mínimo que: el mensaje puede contener información confidencial, es para el uso de los destinatarios nombrados, su indebida retención, difusión, distribución o copia está prohibida y es sancionada por la ley, y representa opiniones y puntos de vista personales del autor, los cuales no necesariamente reflejan los de la SCRD.
- Los mensajes enviados a través del correo corporativo deberán contener el siguiente disclaimer.

- **“AVISO DE CONFIDENCIALIDAD:**

Este correo electrónico, incluyendo sus archivos adjuntos, pueden contener información de carácter confidencial, sensible y/o privilegiada, la cual está dirigida única y exclusivamente a la persona y/o entidad destinataria. Si usted no es a quien se dirige el presente correo, por favor contactar al remitente respondiéndolo y eliminar todas las copias del mensaje original, incluyendo sus archivos. Mediante la recepción del presente correo usted reconoce y acepta que en caso de incumplimiento de su parte y/o de sus representantes a los términos antes mencionados, la Secretaría Distrital de Cultura, Recreación y Deporte tendrá derecho a la reparación de los daños y perjuicios causados. La copia, revisión, uso, revelación y/o distribución de dicha información confidencial sin la autorización por escrito de la Secretaría Distrital de Cultura, Recreación y Deporte SCRD está prohibida.”

- **Uso aceptable de internet**

- La SCRD, con el objetivo de apoyar el desarrollo de las actividades institucionales, brinda acceso a Internet a sus colaboradores, con base en unos perfiles de navegación definidos. Teniendo en cuenta que los recursos de la Entidad deben ser optimizados, los usuarios deben dar un uso racional al servicio de Internet y acoger los lineamientos de este manual.
- La SCRD se reserva el derecho de realizar revisiones periódicas al cumplimiento de los lineamientos definidos sobre el uso de Internet. y podrá aplicar restricciones o medidas en caso de que se encuentren excesos o la utilización indebida de ese recurso
- La Oficina de Tecnologías de la Información debe realizar la propuesta de perfiles y reglas de control de contenido en la navegación de Internet de la SCRD, en donde estos se ajusten acorde a las necesidades de los grupos, evaluando que no involucren el acceso a sitios catalogados de alto consumo de recursos de ancho de banda, juegos y el acceso a páginas especiales.
- No está permitido el acceso a sitios pornográficos, con especial énfasis en los que involucran pornografía infantil, de contenido erótico, obsceno y sitios terroristas.

- La utilización de chat o mensajería instantánea, la descarga de música, radio o video en vivo es discrecional y está sujeta a la definición de perfiles de navegación que realice la Oficina de Tecnologías de la Información, y el acceso a sitios web que no se encuentren dentro de las mencionadas categorías, pero que requieran ser accedidas por los colaboradores para cumplir con sus obligaciones, podrán someterse a consideración de eso grupo, previa justificación por el solicitante.
- Dado que la SCRD tiene la obligación legal de utilización de software licenciado, y que está comprometida con la protección de los derechos de propiedad intelectual y con la optimización del recurso de ancho de banda de las redes, los usuarios no deben descargar desde Internet, almacenar en la plataforma tecnológica de la SCRD y/o usar software, música, libros, publicaciones, video, entre otro material protegido por derechos de autor, sobre el cual la Entidad no haya realizado el pago de los derechos patrimoniales que corresponda.
- Los usuarios que utilicen Internet institucional para la realización de transacciones comerciales de carácter personal como pago de facturas, transacciones bancarias, entre otras, deben asumir los riesgos que dichas transacciones implican. La SCRD no se hace responsable de la seguridad de las mismas, incluyendo la información que se transmita y que pueda ser objeto del monitoreo que se realiza al uso de Internet.
- La SCRD, con el objeto de dar cumplimiento a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Estrategia de Gobierno en Digital, que incluye dentro de sus objetivos facilitar los mecanismos de participación ciudadana, dispone de cuentas en redes sociales, que se encuentran formalmente asignadas a unos responsables, por parte del Grupo de comunicaciones y que deben ser utilizadas bajo los protocolos de uso institucional, definidos para tal fin.
- No está permitido el uso e ingreso a paginas relacionas con pornografía, drogas, terrorismo, segregación racial, hacking, chat, redes sociales, música, videos, TV, juegos y similares que promuevan y atenten contra los principios de seguridad de la información sobre los activos de información, salvo que dicha información se requiera para el ejercicio de las funciones al cargo y no exista otro medio para verla o consultarla.
- El uso de Internet está permitido exclusivamente para actividades institucionales, los colaboradores utilizarán únicamente los servicios para los cuales están autorizados.
- No está permitido utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o no autorizados por la Oficina de Tecnologías de la Información.
- No es debido compartir en sitios web diferentes al Institucional, información propia de la SCRD calificada como información reservada o clasificada.
- Cargar, descargar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de derecho de autor.
- No está permitido utilizar el servicio de Internet/Intranet para propósitos comerciales ajenos a la SCRD.
- No está permitido publicar o enviar opiniones, declaraciones políticas y asuntos no propios de la SCRD, dirigidos a funcionarios públicos, contratistas y público en general, del sector oficial, de otras instituciones y organizaciones, a través de este servicio.

- Descargar, instalar y configurar navegadores distintos a los permitidos e instalados por la Oficina de Tecnologías de la Información.

8.1.4. Devolución de activos

- Todo activo de propiedad de la Entidad, asignado a un colaborador o a un tercero, deberá ser entregado al finalizar su vínculo laboral o contractual, por cambio de cargo o finalización de tareas específicas (terceros). Esto incluye los documentos institucionales, equipos de cómputo (Hardware y Software), dispositivos móviles, periféricos, manuales y la información que tenga almacenada en dispositivos móviles o removibles.
- Adicionalmente, si algún colaborador utiliza su equipo personal, debe transferir toda la información que haya producido durante la vigencia del contrato a la SCRD y eliminarla de manera segura como consecuencia de su desvinculación con la Entidad.

8.2. Clasificación de la información

8.2.1. Clasificación de la información Pública, Clasificada (Sensible) y Reservada

- **Información Pública**: información que puede ser accedida sin restricciones por personal interno o externo a la entidad y su publicación no representa ninguna consecuencia para la población, ministerio público, entes de control y para la entidad.
- **Información pública clasificada**: corresponde a la información que solo puede ser accedida por personal autorizado y cuya divulgación no autorizada podría generar daños y perjuicios a la población víctima, a la entidad y a sus funcionarios, contratistas y colaboradores y bajo el cumplimiento de los requisitos consagrados en el artículo 18 de la ley 1712 de 2014 - Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- **Información Pública Reservada**: corresponde a la información con restricción de acceso a la ciudadanía por daño a intereses públicos y bajo el cumplimiento de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014 - Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- La Oficina de Tecnologías de la Información – OTI, debe definir la metodología de Activos de Información alineada con la Ley 1712 de 2014, generando directrices frente a la clasificación de la información. La aplicabilidad de la metodología, será liderada por la OTI, realizando acompañamiento a los responsables de inventariar y clasificar la información de cada proceso y dependencia de la Entidad o sus delegados.
- Toda la información existente y/o generada en la SCRD debe ser identificada y clasificada por el responsable de la información, con el objetivo de determinar el nivel de acceso y criticidad de la información y de esta manera definir controles específicos para su adecuada protección.
- La SCRD debe gestionar el inventario de activos de información, en el cual se identifican los activos incluyendo el nivel de clasificación de la información como: información pública, información clasificada e información reservada y se actualiza de forma manual una vez al año, de acuerdo a lo establecido en la Ley 1712 de 2014 - Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

- La información física y digital de la SCRD debe tener un tiempo de retención que puede ser dictaminado por las Tablas de Retención Documental o por requerimientos legales o misionales, este periodo deberá ser indicado en las tablas de retención documental (TRD) y cuando se cumpla este tiempo, toda la información deberá ser eliminada adecuadamente.

8.2.2. Etiquetado de la información

- Es responsabilidad de cada una de las dependencias y procesos, llevar a cabo la implementación de la etiqueta correspondiente a la clasificación determinada en el inventario de Activos de Información, el cual se encuentra alineado con la Ley 1712 de 2014 - Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Se debe hacer la rotulación y el etiquetado de la información que esté en medios físicos, digitales o electrónicos teniendo como insumo principal el esquema de clasificación definido.
- Las Tablas de Retención Documental (TRD) deberán contener el tipo de clasificación de las series, subseries y documentos en ella contenidas para facilitar el trabajo de etiquetado.
- Los propietarios y custodios de la información deben supervisar que el etiquetado de los activos se esté haciendo según los criterios establecidos por la SCRD.

8.2.3. Manejo de Activos

- Es responsabilidad de cada una de las dependencias llevar a cabo el desarrollo y la implementación de procedimientos para la adecuada gestión y acceso a los activos de información, de acuerdo con el esquema de clasificación de información adoptado por la Entidad.

8.2.4. Manejo de información clasificada (sensible) y reservada

Aplica a toda la información institucional que contenga datos personales considerados como sensibles, privados, especialmente protegidos, información clasificada y reservada o de índole confidencial, independiente de si es generada en la Entidad, proviene de un tercero y del medio de tratamiento ya sea físico o digital. En razón a lo anterior se definen los siguientes controles para salvaguardar y mitigar riesgos de seguridad de la información contra uso no autorizado, divulgación o revelación, modificación, daño o pérdida y para asegurar el cumplimiento de las regulaciones y leyes aplicables. Aplica a todo el personal de la SCRD incluyendo, pero no limitado a funcionarios, contratistas, terceros, y demás.

- Es responsabilidad de cada una de las dependencias identificar y clasificar su información, de acuerdo con el contenido de la misma aplicando la metodología de Activos de Información, teniendo en cuenta la debida identificación de datos personales públicos, privados, semiprivados, sensibles y especialmente protegidos (de niños, niñas y adolescentes).
- Cada proceso y dependencia de la Entidad debe contar con el inventario de sus activos de información actualizado, a través del instrumento dispuesto para ello y reportarlos a la Oficina de Tecnologías de la Información.
- En caso de que alguna Entidad, proveedor, tercero o personal externo requiera acceso a información **sensible o crítica**, el responsable(s) de la misma debe implementar los controles pertinentes, entre los cuales se considera como mínimo, suscribir acuerdos de confidencialidad y de no divulgación, para salvaguardar la información y cumplir con la normatividad vigente asociada.

- Es responsabilidad de todos, tomar las medidas para la protección de la información sensible que se encuentre en medios de almacenamiento removibles bajo su custodia (Discos Duros Externos, Memorias USB, MicroSD, SD, entre otros) para evitar accesos no autorizados, daños, perdida o fugas de información.
- La información sensible (información pública clasificada o reservada) que deba ser eliminada de medios de almacenamiento removibles, por reúso o eliminación de éste, deberá emplear métodos de borrado seguro, definidos por la Oficina de Tecnologías de la Información.
- Está prohibido el uso de medios de almacenamiento removibles que contengan información sensible, información pública clasificada o reservada en los dispositivos que tenga acceso el público. De igual manera, se prohíbe el préstamo o uso de los medios que contengan información sensible a personal no autorizado o externo de la Entidad.
- La información sensible que se encuentre en medios físicos documentos en papel y medios de almacenamiento removibles, se debe almacenar en el archivo centralizado o bajo llave en gabinetes, archivadores u otro tipo de mobiliario que genere un nivel de seguridad adecuado.
- La información sensible que se recolecta, almacena, gestiona por medio de sistemas de información y aplicativos de la SCRD, debe ser identificada para realizar la respectiva anonimización de la información, de preferencia por medio de algoritmos de cifrado.
- La Oficina de Tecnologías de la Información debe velar por el uso apropiado y eficaz de la criptografía, para proteger la confidencialidad, integridad, disponibilidad y el no repudio de la información **sensible o crítica**. Por lo cual requiere implementar técnicas criptográficas para cifrado de la información, certificados digitales en los aplicativos y sistemas de información web, e implementar protocolos seguros para comunicaciones cuando se requiera trasferir, recibir o almacenar información de carácter sensible.

8.3. MANEJO DE MEDIOS

8.3.1. Gestión de medios de almacenamiento removibles

- La SCRD es consciente que este tipo de medios como lo son (CD, DVD, USB, Discos duros internos y Externos, memorias flash, smartphones, reproductores portátiles MP3/MP4, cámaras, SD cards, mini SD cards, micro SD cards, entre otros) son útiles para el almacenamiento y transporte de información pero igualmente son elementos que permiten extraer información sin dejar huella física ni registro de dicha acción, por esta razón la SCRD define los compromisos frente al uso de dispositivos de almacenamiento externo para asegurarse de que la información propietaria, adquirida o puesta en custodia en la SCRD no está exenta de fuga, uso no autorizado, modificación, divulgación o pérdida y que ésta debe ser protegida adecuadamente según su valor, y nivel de clasificación.
- El uso de dispositivos de almacenamiento externo está permitido en la SCRD para los funcionarios públicos y contratistas; con el fin de facilitar el compartir y transportar información que no sea de carácter clasificado ni reservado de la SCRD dentro de las normas y responsabilidades del manejo de información.
- Los funcionarios públicos, contratistas y terceros autorizados, se comprometen a asegurar física y lógicamente el dispositivo a fin de no poner bajo ningún riesgo, la información de la SCRD y los demás activos de información bajo su custodia.

- Todo medio de almacenamiento removible debe ser sometido a análisis con la herramienta antivirus – antimalware, instalada en los equipos de la SCRD.
- La Oficina de Tecnologías de la Información es responsable de implementar los controles necesarios para asegurar que únicamente los funcionarios públicos y contratistas autorizados, hagan uso de los medios de almacenamiento removibles.
- Los medios de almacenamiento removibles que se conecten a los equipos de cómputo de la SCRD o que estén bajo su custodia, pueden estar sujetos a monitoreo por parte de la Oficina de Tecnologías de la Información, cuando en los medios de almacenamiento removibles se alojen datos de especial protección (privados, sensibles y de menores de edad) o información clasificada o reservada de la SCRD, por lo cual, se deben usar técnicas de cifrado para proteger dicha información.
- No está permitido la ejecución de programas no autorizados desde algún medio extraíble identificado anteriormente.
- No está permitido trasladar información clasificada o reservada dentro y fuera de la SCRD en los medios extraíbles sin cifrar dicha Información.

8.3.2. Disposición de medios

Se deben establecer procedimientos formales para la disposición segura de medios, para minimizar el riesgo de fugas de información y datos personales sensibles. Para esto se deben tener en cuenta las siguientes consideraciones:

- El proceso de eliminación lógica debe ser realizado por medio de aplicaciones que estén diseñadas para un proceso eficaz de borrado seguro. La Oficina de Tecnologías de la Información apoyará en la evaluación del desempeño de dicha aplicación y deberá considerar nuevas aplicaciones en caso de detectar incompatibilidad con los resultados esperados y las necesidades de la SCRD.
- El proceso de eliminación lógica debe ser revisado y validado y se llevará un registro de resultados del proceso para un control y seguimiento posterior.
- Se deben realizar pruebas de recuperación de información aleatorias para verificar que los datos se hayan eliminado totalmente o que hayan quedado inutilizables e irrecuperables.
- Realizar las pruebas con herramientas específicas para cada medio de almacenamiento.
- Para los discos duros, se debe realizar un proceso de eliminación lógica que puede ser por desmagnetización y sobreescritura segura, antes de hacerle eliminación física.
- La destrucción física debe llevarse a cabo por cualquiera de los siguientes métodos: desintegración, pulverización, fundición, incineración o trituración.
- El proceso de eliminación físico debe dejar inutilizable el dispositivo antes de ser desechado completamente.
- Generar registro de la destrucción de los medios.
- Todo medio óptico de almacenamiento debe ser destruido físicamente por pulverización, trituración de corte transversal o incineración. Este proceso de eliminación puede llevarse a cabo por el colaborador que tenga a su cargo el dispositivo. Se debe generar registro de este procedimiento.

- La destrucción debe ser inmediata y hacer imposible la reconstrucción de los documentos o la información contenida en ellos.
- No entregar ni vender los documentos destruidos como papel usado para reciclaje, sin destruirlos previamente.
- Los documentos con información clasificada o reservada no deben depositarse al descubierto en cajas o paquetes, ni depositarse en contenedores junto con el resto de la basura o reciclaje. Esto debido a que siguen siendo legibles y permanecen expuestos al alcance de cualquier persona en vía pública.
- El método más recomendado es la trituración mediante corte en tiras cuyo tamaño se debe elegir dependiendo de la criticidad de la información que esté contenida en los documentos a destruir
- Generar registro de los documentos destruidos.

8.3.3. Transferencia de medios físicos

Con el fin de proteger la información almacenada en medios físicos que requieren transferencia de un lugar a otro, se deben adoptar los siguientes lineamientos:

- La información calificada como CLASIFICADA o RESERVADA que esté almacenada en medios de almacenamiento removibles y estos requieran ser transportados fuera de las instalaciones de la SCRD, deben cumplir con las disposiciones de seguridad indicadas por La Oficina de Tecnologías de la Información, específicamente aquellas referentes al empleo de técnicas de cifrado. Adicionalmente, deben ser transportados en medios especialmente acondicionados, que protejan frente a golpes o caídas, teniendo en cuenta las recomendaciones del fabricante.
- Para el transporte de medios de almacenamiento y/o documentos físicos, se debe usar un proveedor de mensajería de confianza e incluir cláusulas de seguridad en el transporte, datos personales y acuerdos de confidencialidad dentro de los contratos.
- Se debe tener un registro de entradas y salidas de medios de almacenamiento y documentos que contengan información de interés para la SCRD. Adicional a esto, el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte y el recibido.

9. CONTROL DE ACCESO.

9.1. REQUISITOS DE LA SCRD PARA CONTROL DE ACCESO

9.1.1. Política de control de acceso lógico

- Todos los colaboradores y terceros de la SCRD tendrán acceso sólo a la información que necesitan para el desarrollo de sus funciones y actividades dentro de la SCRD. La asignación de permisos y acceso a los activos de información se basa en la necesidad de uso de los procesos internos y deben ser autorizados por el propietario de los activos de información. Estas necesidades deben ser definidas y autorizadas por cada dependencia y/o supervisores de contrato, en función de los roles y responsabilidades de cada colaborador y/o tercero.

- La SCRD mediante la Oficina de Tecnologías de la Información, tiene las facultades de bloquear o eliminar los accesos a cualquier usuario que represente riesgo en la integridad, disponibilidad y confidencialidad de la información personal y de la operación de la entidad.
- Se deben identificar los privilegios asociados a sistemas operativos, sistemas de administración de bases de datos, aplicaciones, servicios de red y cualquier otro componente tecnológico, contando con una matriz de roles y privilegios documentada y aprobada por el responsable primario de la información allí gestionada.
- La Oficina de Tecnologías de la Información debe habilitar el almacenamiento y garantizar los respaldos (Logs) de la información relacionada con usuarios y privilegios.
- La SCRD suministra a los colaboradores y terceros, las credenciales de acceso respectivas para acceder a los recursos de la plataforma tecnológica a los que hayan sido autorizados, estas credenciales son de uso personal e intransferible. Es responsabilidad del usuario el manejo de la información de autenticación.

9.1.2. Acceso a redes y servicios de red

Internet

- La Oficina de Tecnologías de la Información es la única dependencia encargada de proveer el servicio de acceso a internet, así como de vigilar su correcto uso y funcionamiento.
- La Oficina de Tecnologías de la Información asignará los permisos de acceso conforme a la necesidad de acceso que se requiera para la ejecución de las labores de los funcionarios públicos y contratistas, a través de listas blancas y negras.
- La Oficina de Tecnologías de la Información, cuenta con la facultad para bloquear o restringir todos aquellos sitios de Internet que considere que no son compatibles con las labores de los funcionarios públicos y contratistas, o que repercutan en un riesgo de seguridad para la SCRD.
- No está permitido el uso y conexión de dispositivos alternos, que provean servicio a internet y/o configurar los dispositivos de la entidad para el acceso a estos medios alternos.
- No está permitido el uso de cuentas de usuario de otros funcionarios públicos para el ingreso a páginas de internet a las cuales no tiene permisos con el usuario asignado.
- Los colaboradores de la SCRD tendrán acceso restringido para redes sociales en los horarios previamente establecidos por la Oficina de Tecnologías de la Información.
- Realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.
- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los navegadores instalados por la Oficina de Tecnologías de la Información.
- Acceder a sitios de contenido multimedia (videos, música, emisoras online, etc.) debido al alto consumo de canal de comunicaciones. Únicamente se autorizará el acceso a aquellos funcionarios públicos, contratistas que por sus actividades requieran monitorear estos sitios externos y tengan previa aprobación del Jefe Inmediato y la autorización ante la Oficina de Tecnologías de la Información.
- Las cuentas de correo y acceso a la red de funcionarios públicos de la SCRD serán desactivadas una vez sea notificado a la Oficina de Tecnologías de la Información mediante

resolución expedida por talento humano. Para los contratistas se realizará a la firma del paz y salvo de terminación contractual o discreción del supervisor.

Acceso Remoto

- Dentro de la Secretaría Distrital de Cultura, Recreación y Deporte únicamente se encuentra autorizado el acceso y uso de VPN para conexiones remotas, asignada únicamente a los funcionarios públicos autorizados por la Oficina de Tecnologías de la Información y los jefes de las dependencias.
- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la Secretaría Distrital de Cultura, Recreación y Deporte, las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Oficina de Tecnologías de la Información.
- No está permitido el uso de aplicaciones y servicios interactivos como: Team Viewer, TightVNC, RemoteVNC, Chrome Remote Desktop, Join.me, Ammy Admin, Putty, WinSCP, Screen Leap, Vyew, Croos Loop, Skype, Google+ y similares que permitan realizar conexiones con cualquier dispositivo y atente contra la seguridad de los activos de información de la Secretaría Distrital de Cultura, Recreación y Deporte.

Carpetas compartidas

- Para las carpetas compartidas en red, se deben asignar permisos de acceso al usuario únicamente a la información que este se encuentre autorizado, dichos permisos deben asignarse a través de grupos de usuarios para su acceso.
- Es responsabilidad de cada una de las dependencias solicitar la creación de su recurso compartido, al igual que sus necesidades en seguridad y es responsabilidad de La Oficina de Tecnologías de la Información establecer los parámetros adecuados de seguridad para estos recursos.

Impresoras

- Únicamente se deben asignar permisos a los colaboradores que por sus funciones requiera este servicio, su acceso debe realizarse por medio de usuario y contraseña.

Sistemas de Información

- Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.
- La identificación del equipo en la red en lo posible debe indicar claramente a cuál red está autorizado a conectarse el equipo, si existe más de una red y particularmente si estas redes tienen diferentes grados de confidencialidad. En caso de ser necesario, es importante considerar la protección física del equipo para mantener la seguridad del identificador del equipo.
- Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
- Implementar un procedimiento para los puertos de configuración y diagnóstico remoto en donde se enuncian los controles adoptados. Dentro de los controles para los puertos de diagnóstico remoto, se encuentran:

- Garantizar que los puertos de diagnóstico y configuración sólo sean accesibles mediante acuerdo entre el Administrador de Red y/o el personal de soporte de hardware o software que requiere el acceso.
- Los puertos, servicios y prestaciones similares instaladas en un servicio de computador o de red, que no se requieren específicamente para la funcionalidad de la entidad se deben inhabilitar o retirar.

9.2. GESTIÓN DE ACCESO DE USUARIOS

9.2.1. Creación y eliminación de cuentas de usuarios

- La Oficina de Tecnologías de la Información debe definir e implementar un procedimiento para la creación y eliminación de derechos de acceso de usuarios.
- Los procesos de Grupo Interno de trabajo de Gestión del Talento Humano y Grupo Interno de Trabajo de Contratación deben informar de forma oportuna y por los medios establecidos, las solicitudes de creación y eliminación de cuentas de usuario, para su respectivo trámite y seguimiento por parte de la Oficina de Tecnologías de la Información.

9.2.2. Gestión de acceso a los usuarios

- Los propietarios de la información, sistemas de información y aplicativos deben autorizar formalmente el acceso y permisos que se otorgará a los usuarios e informarlo a la Oficina de Tecnologías de la Información para su respectiva gestión.

9.2.3. Gestión de derechos de acceso privilegiados

- Los privilegios de acceso privilegiados se deben asignar a los usuarios, con base en las necesidades y eventos, sólo y durante el tiempo requerido y aprobado.
- Toda asignación de permisos de acceso privilegiado debe contar con previa autorización de la Oficina de Tecnologías de la Información, Dependencia responsable del activo de información o aprobación del Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información (cuando sea requiera).

9.2.4. Gestión de la información de autenticación secreta de los usuarios

- La entrega de la información del usuarios y autenticación secreta de los funcionarios públicos nuevos, debe ser asignada después de haber firmado sus funciones u obligaciones contractuales y se debe anexar un documento al contrato donde el funcionario, corrobora la recepción de dicha información, esta información solo puede ser conocida por el funcionario a contratar, el administrador del sistema de administración de usuarios y el profesional responsable de contratación.
- No está permitido divulgar, compartir, distribuir, asignar, permitir, entregar, alquilar, comunicar, intercambiar, vender y/o prestar la contraseña de él(los) usuario(s) administrador(es) de la plataforma tecnología, dispositivos, bases de datos, equipos, servidores, aplicaciones, sistemas de información y similares, sin previa autorización la Oficina de Tecnologías de la Información, Dependencia responsable del activo de información o aprobación del Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información.

9.2.5. Revisión de derechos de acceso de usuario

- El acceso a las plataformas, aplicaciones, servicios y en general a cualquier recurso de información de la Secretaría Distrital de Cultura, Recreación y Deporte, debe contar con las autorizaciones de las dependencias propietarias de la información para su acceso.
- Los propietarios de la información y de las aplicaciones, deben revisar periódicamente los derechos de acceso de usuarios concedidos e informar a La Oficina de Tecnologías de la Información los ajustes pertinentes.

9.2.6. Remoción o ajuste de los derechos de acceso

- Los derechos de acceso de todos los funcionarios públicos, contratistas y terceros de acceso a la información y a los servicios de procesamiento de información se deben retirar al terminar su contratación laboral, contrato o acuerdo y/o se deben ajustar cuando existan cambios de dependencias y/o responsabilidades.

9.3. RESPONSABILIDADES DE LOS USUARIOS

9.3.1. Uso de la información de autenticación secreta

- Todos los funcionarios públicos, contratistas y terceros, cuentan con un usuario y contraseña único, personal e intransferible y asumen su responsabilidad de los eventos e incidentes que puedan ocurrir bajo su autenticación sobre los activos de información a los cuales acceden y procesan dentro del desarrollo de sus funciones.
- Se debe dar uso adecuado a los activos de información y deben ser usados únicamente bajo las condiciones netamente laborales.
- Todos los funcionarios públicos, contratistas y terceros, que requiera tener acceso a los sistemas de información de la Secretaría Distrital de Cultura, Recreación y Deporte deben estar debidamente autorizados y debe acceder a dichos sistemas haciendo uso de un usuario y contraseña y cumplir los siguientes lineamientos:
- No divulgar, compartir, distribuir, asignar, permitir, entregar, alquilar, comunicar, intercambiar, vender y/o prestar la(s) contraseña(s) del o los usuarios por los que accede a la plataforma tecnológica en ninguna circunstancia.
- No se debe intentar acceder de forma no autorizada con otro usuario y clave diferente a cualquier sistema de información o plataforma tecnológica
- Cambiar la contraseña a intervalos regulares.
- Construir contraseñas seguras que incluyan como mínimo:
  - 1 carácter especial.
  - 1 carácter en Mayúscula.
  - 1 carácter en Minúscula.
  - 1 carácter numérico.
  - Debe contener una longitud mínima de 8 Caracteres.

- No utilizar contraseñas maestras.
- La contraseña no pude ser el mismo usuario.
- La contraseña no podrá repetirse durante los siguientes 10 cambios.
- No escribir la contraseña en medios físicos, digitales y/o electrónicos.
- No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento.
- Dar aviso la Oficina de Tecnologías de la Información, a través de los medios establecidos, de cualquier fallo de seguridad, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.

9.4. CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

- La Oficina de Tecnologías de la Información, es la única dependencia que cuenta con la facultad para crear, asignar, bloquear, retirar y modificar, usuarios y permisos de acceso de forma administrada de las plataformas de las cuales son responsables.
- Para las dependencias que cuentan con sistemas de información y su administración, es su responsabilidad de cada una de ellas mantener y garantizar el control de acceso sobre estas plataformas.

9.4.1. Restricción de acceso a información.

- El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

9.4.2. Procedimiento de conexión segura.

- Cuando se requiera acceso seguro a sistemas y aplicaciones, se debe controlar mediante un proceso de conexión segura (VPN).

9.4.3. Sistema de gestión de contraseñas.

- Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar que se cumple con los requerimientos de calidad de las contraseñas.

9.4.4. Uso de programas utilitarios privilegiados.

- Se debe restringir y controlar el uso de programas utilitarios que podrían tener capacidad de anular los controles de los sistemas operativos y las aplicaciones.

9.4.5. Control de acceso a códigos fuente de programas.

- Se debe restringir el acceso a códigos fuente de los sistemas de información y aplicativos.

10. CRIPTOGRAFÍA.

10.1. CONTROLES CRIPTOGRÁFICOS

10.1.1. Política de controles criptográficos

- Para efectos de identificar la necesidad de implementar controles criptográficos para proteger la información de la SCRD que garanticen (confidencialidad, integridad y disponibilidad) de la información se debe realizar un análisis de riesgos, que concluya sobre los activos que requieran estos controles.
- Es responsabilidad del Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información analizar la propuesta de plan para la implementación de controles criptográficos y gestionar los recursos requeridos, sujeto a la capacidad financiera y presupuestal de la SCRD. Se deben utilizar como mínimo controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios.
- Con el fin de proteger la confidencialidad, integridad, autenticidad y no repudio de la información, la SCRD, establecerá el uso de protocolos y controles criptográficos para transferencia de información, enlaces de comunicaciones, protección de medios, acceso remoto, sobres digitales y firmas electrónicas y digitales con Entidades externas.
- Estas herramientas deberán estar incluidas en el listado de software autorizado, y no se permitirá el uso de herramientas o mecanismos de cifrado de información diferentes a los autorizados por la Oficina de Tecnologías de la Información.
- Todo software construido por la Entidad o por un tercero deberá utilizar un algoritmo de cifrado de datos solo cuando dentro de los requerimientos funcionales del sistema de información se haya especificado, o cuando un requisito de ley así lo exija.

10.1.2. Gestión de llaves

- La administración de claves criptográficas y certificados digitales estará a cargo de La Oficina de Tecnologías de la Información.
- Los certificados digitales entregados a funcionarios públicos de la SCRD quedan bajo su responsabilidad y control y deben ser correctamente utilizados.
- Se debe tener en cuenta los recursos técnicos y la capacidad de cómputo de los equipos que hacen parte de los sistemas de información (estaciones de trabajo, servidores, etc.). para poder gestionar debidamente las llaves criptográficas.
- Se debe tener en cuenta la velocidad de cifrado, uso de memoria, el rango de aplicaciones en el que se puede usar el protocolo de cifrado, el costo y la seguridad.
- El algoritmo de cifrado que se va a utilizar y los mecanismos de implementación. Observando que algunos algoritmos han perdido vigencia y han entrado en desuso. Se debe plantear el uso de combinaciones de algoritmos.
- En el caso en el que una autoridad certificadora sea vulnerada o se descifre un algoritmo de cifrado, la SCRD debe estar preparada para reemplazar todos sus certificados y llaves de cifrado en el menor tiempo posible.

- El almacenamiento de las claves debe hacerse de forma segura, cifrándolas y protegiendo el sistema de almacenamiento con contraseña. El único usuario que puede acceder a este sistema es la Oficina de Tecnologías de la Información o quien este delegue.
- Si se hace uso de un sistema de gestión de llaves, se deben seguir las recomendaciones de seguridad que indique el fabricante.
- La destrucción de las llaves de cifrado implica que se debe eliminar el sistema de creación de las llaves, es decir, las aplicaciones de software, las copias de las llaves y el borrado seguro de los dispositivos donde estaban almacenadas o si es necesario la destrucción física de los dispositivos de almacenamiento, la revocación de privilegios a los usuarios mientras se establece el nuevo esquema de llaves de cifrado y la revisión del registro de versiones de las claves.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

11.1. ÁREAS SEGURAS

11.1.1. Perímetro de seguridad física.

- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido y en consecuencia deben contar con controles adecuados para el control de acceso.

11.1.2. Controles físicos de entrada.

- Todos los terceros deberán registrase al ingreso y portar el adhesivo que lo acredita como visitante en un lugar visible, durante su permanencia en la SCRD.
- Todos los colaboradores, deben portar el carnet que los acredita como funcionario de la Secretaría Distrital de Cultura, Recreación y Deporte en un lugar visible y durante su permanencia en la Entidad.

11.1.3. Seguridad de oficinas, salones e instalaciones.

- Las puertas de acceso a cada una de las dependencias, oficinas, centros de cableado, data center, salas de capacitación y similares deben permanecer cerradas bajo ausencias temporales.

11.1.4. Protección contra amenazas externas y ambientales.

- Se deben implementar medidas de protección física para evitar daños causados por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre.

11.1.5. Trabajo en áreas seguras.

- Se debe establecer y asignar permisos de acceso a las dependencias, oficinas, centros de cableado, data center, salas de capacitación y similares únicamente a los funcionarios públicos autorizados para su acceso.

- Los centros de cómputo, cableado y cuartos técnicos de la Secretaría Distrital de Cultura, Recreación y Deporte deben contar con mecanismos adecuados contra las amenazas ambientales (temperatura, humedad, fuego, etc.), especificados por los fabricantes de los equipos que albergan.
- No está permitido albergar, mantener y/o guardar elementos inflamables dentro de las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones.

11.1.6. Áreas de despacho y carga.

- Se deben controlar todos los puntos de acceso físico, tales como áreas de despacho, de carga y otros puntos para evitar el acceso de personas no autorizadas.

11.2. EQUIPOS

11.2.1. Ubicación y protección de los equipos.

- Los equipos que contengan y/o procesen información identificada como clasificada y reservada de la SCRD, se deben instalar en lugares en los cuales se evite que la información pueda ser vista o accedida por personas no autorizadas.
- Es responsabilidad de los funcionarios públicos, contratistas y/o terceros no afectar la disponibilidad de los equipos que componen la infraestructura tecnológica en el momento de fumar, beber y/o consumir cualquier tipo de alimento cerca de ellos.
- No está permitido el almacenamiento de información en los equipos de escritorio, toda la información debe ser almacenada en la carpeta compartida del área.
- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por la Oficina de Tecnologías de la Información.

11.2.2. Equipos de soporte.

- La Secretaría Distrital de Cultura, Recreación y Deporte es responsable de establecer los controles apropiados de acceso y prestación de servicios de suministro energético cuya indisponibilidad pueda atentar contra los activos de información, se deben identificar, clasificar, valorar, analizar sus riesgos y establecer los controles apropiados para garantizar los principios de seguridad.

11.2.3. Seguridad del cableado.

- Toda la infraestructura tecnológica debe contar y mantener estándares de seguridad (hardening), para su funcionamiento.
- El cableado de la energía y las telecomunicaciones que llevan datos o sostienen los servicios de información deben permanecer protegidos a través de canaleta para evitar el deterioro y disponibilidad del servicio.
- Los centros de cómputo, cableado y cuartos técnicos deben permanecer debidamente etiquetados para reducir riesgos por manipulación indebida de estos elementos.

11.2.4. Mantenimiento de equipos.

- Durante las actividades de mantenimiento preventivo o correctivo, es importante mantener la concordancia con los intervalos y especificaciones del proveedor, así mismo, se deben generar los registros a que haya lugar en donde se permita realizar la trazabilidad de las fallas, personas involucradas y actividades desarrolladas.

11.2.5. Retiro de activos.

- No está permitido retirar y/o sacar entre dependencias o fuera de la Secretaría Distrital de Cultura, Recreación y Deporte, activos de información sin previa autorización del responsable y sus registros de ingresos y salidas pertinentes.

11.2.6. Seguridad de equipos y activos fuera de las instalaciones.

- No está permitido retirar equipos que contengan información sensible y/o confidencial de la SCRD en sus medios de almacenamiento.
- Se debe garantizar que los equipos que se encuentran fuera de las instalaciones de la SCRD tengan configuradas contraseñas de ingreso al sistema operativo y servicios, para evitar accesos no autorizados.

11.2.7. Disposición segura o reutilización de equipos.

- La información sensible o confidencial de la SCRD que se imprima debe ser recogida inmediatamente para evitar que sea conocida y/o divulgada a personas no autorizadas.
- Todos los equipos que contengan información sensible y/o confidencial en sus medios de almacenamiento deben pasar por un procedimiento de borrado seguro antes de su reutilización o finalización de su vida útil.

11.2.8. Equipos sin supervisión de los usuarios.

- Todas las estaciones de trabajo deberán bloquear la sesión del usuario de forma automática después de cinco (5) minutos de inactividad.
- Los funcionarios públicos, contratistas y/o terceros son responsables de bloquear la sesión de su equipo durante su ausencia y/o ausencias temporales, se considerará sesión desatendida en el momento que el usuario, pierda el control de su equipo.
- Los funcionarios públicos, contratistas y/o terceros son responsables de mantener la información sensible (activos de información de clasificación Restringida y/o clasificada) bajo llave, durante su ausencia y/o ausencias temporales, esto incluye documentos impresos, CDs, dispositivos de almacenamiento, medios de almacenamiento removibles en general y similares.

11.2.9. Política de escritorio limpio y pantalla limpia.

- Todas las estaciones de trabajo deberán usar el papel tapiz corporativo establecido automáticamente por la Oficina de Tecnologías de la Información.
- Los funcionarios públicos, contratistas y/o terceros son responsables de mantener el escritorio del equipo libre de información sensible, confidencial y de uso diario (Carpetas, archivos de uso diario, accesos directos y similares), para evitar el fácil acceso a la información por personal no autorizado.

12. SEGURIDAD DE LAS OPERACIONES

12.1. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

12.1.1. Procedimientos de operación documentadas.

- Se deben documentar los procedimientos de operación de TI, tales como instalación y configuración de sistemas operativos, aplicativos, infraestructura tecnológica, procedimientos de monitoreo entre otros que se estimen pertinentes.

12.1.2. Gestión de cambios.

- Es responsabilidad de la Secretaría Distrital de Cultura, Recreación y Deporte llevar a cabo revisiones periódicas, aprobaciones y evaluación de errores de los cambios programados antes, durante y después de su ejecución y debe existir una aprobación previa de las dependencias interesadas para la ejecución del cambio.

12.1.3. Gestión de capacidad

- Es responsabilidad de la Oficina de Tecnologías de la Información monitorear, revisar, proyectar y gestionar adecuadamente la capacidad de la infraestructura tecnológica de la SCRD.

12.1.4. Separación de los ambientes de desarrollo, pruebas y operación.

- Es responsabilidad de la Oficina de Tecnologías de la Información separar los ambientes de desarrollo, pruebas y producción de los desarrollos internos y externos si aplica.
- El mantenimiento y el copiado de las librerías fuente de programas deben estar sujetos a un procedimiento estricto de control de cambios.

12.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

12.2.1. Controles contra códigos maliciosos

- Es responsabilidad de la Oficina de Tecnologías de la Información que todos los activos de información tipo Hardware cuenten con un sistema de antivirus y antispyware instalado y actualizado regularmente, para la protección contra códigos maliciosos.
- Únicamente el administrador de la plataforma de antivirus tendrá los permisos necesarios para deshabilitar, remover, eliminar y/o desinstalar el software de antivirus, estas actividades pueden llevarse a cabo bajo autorización previa del jefe de La Oficina de Tecnologías de la Información.
- Se deben realizar escaneos a intervalos regulares, como control del estado de la infraestructura tecnológica.

12.3. COPIAS DE RESPALDO

12.3.1. Copias de respaldo de la información

- Es responsabilidad de la Oficina de Tecnologías de la Información realizar las copias de respaldo correspondientes a los activos de información de la SCRD que lo requieran y realizar pruebas aleatorias de restauración para garantizar que son accesibles y funcionales.

12.4. REGISTRO Y SEGUIMIENTO

12.4.1. Registro de eventos.

- Se deben activar los log de eventos de auditoría, excepciones, eventos, fallas y se deben conservar por un periodo de tiempo establecido por la Oficina de Tecnologías de la Información.

12.4.2. Protección de la información de registro.

- Se debe conservar un respaldo de los log de eventos de aplicativos y sistemas con el fin de facilitar las labores de auditoría y preservarlos de accesos no autorizados.

12.4.3. Registros del administrador y del operador.

- Se deben revisar periódicamente los log de eventos de aplicativos y sistemas con el fin de verificar el adecuado funcionamiento y detectar posibles fallas de los mismos.

12.4.4. Sincronización de relojes.

- Todos los relojes de los sistemas de procesamiento de información de la Secretaría Distrital de Cultura, Recreación y Deporte deben estar sincronizados con una fuente de tiempo única.

12.5. CONTROL DE SOFTWARE OPERACIONAL

12.5.1. Instalación de software en sistemas operativos

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la Secretaría Distrital de Cultura, Recreación y Deporte es responsabilidad de La Oficina de Tecnologías de la Información, y por tanto son los únicos autorizados para llevar a cabo esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la Secretaría Distrital de Cultura, Recreación y Deporte a través de esta oficina.
- La Oficina de Tecnologías de la Información debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y/o cualquier aplicación instalada.

12.6. GESTIÓN DE VULNERABILIDA TÉCNICA

12.6.1. Gestión de las vulnerabilidades técnicas

- Se deben realizar análisis de vulnerabilidades a los activos de información de la Entidad antes de su salida a producción.

- Se deben realizar análisis de vulnerabilidades periódicamente, a la infraestructura tecnológica, para identificar los riesgos a los cuales se encuentra expuesta y tomar medidas correctivas para evitar su materialización.
- No está permitido que los funcionarios públicos, contratistas y terceros realicen pruebas y/o aprovechen las debilidades de seguridad en la infraestructura tecnológica.

12.6.2. Restricciones sobre la instalación de software.

- Se debe restringir la práctica de instalación de software no autorizado a través de políticas de dominio y otorgar los permisos únicamente a los funcionarios públicos autorizados.

12.7. CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN

12.7.1. Controles sobre auditorías de sistemas de información.

- Se deben realizar revisiones internas periódicas frente al aseguramiento de los sistemas operativos para verificar el cumplimiento de los controles de acceso establecidos en la presente política.
- Ejecutar auditorías según lo establecido en el Plan Anual de Auditorias definido por la Entidad y en caso de ser necesario se pueden programar revisiones parciales o totales sobre una o varias líneas de acción o trabajo.

13. SEGURIDAD DE LAS COMUNICACIONES

13.1. GESTIÓN DE LA SEGURIDAD DE LAS REDES

13.1.1. Controles de redes.

- Únicamente los funcionarios públicos y terceros autorizados por la Oficina de Tecnologías de la Información, previa solicitud por parte de la dependencia que lo requiera, pueden conectarse a la red inalámbrica de la Secretaría Distrital de Cultura, Recreación y Deporte.
- La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de la Secretaría Distrital de Cultura, Recreación y Deporte, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por la Oficina de Tecnologías de la Información.
- Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
- Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso.
- Se deben implementar controles de redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso.

- Llevar un registro de todo el mantenimiento y reparaciones del hardware de la red, incluyendo la instalación o el retiro de los equipos activos y de sus dispositivos, así como un registro de todos los visitantes autorizados y un registro de los chequeos de seguridad realizados y el comienzo y cierre de cada día de trabajo.
- Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
- Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
- Realizar monitoreo de los canales de comunicación, con el fin de establecer el desempeño mensual de los mismos y generar los mecanismos de control a que haya lugar.
- Se debe establecer controles para la detección de intrusos con el fin de detectar cualquier tipo de actividad contra los sistemas presentes.

13.1.2. Separación en las redes.

- Distribuir la red conforme a los roles y responsabilidades de los funcionarios públicos de la Entidad haciendo uso de VLANs, y restringir el acceso remoto de las plataformas por medio del uso de VPN previamente autorizadas.
- La comunicación entre entidades internas y externas a través de accesos dedicados, conmutados y/o públicos, debe permanecer en todo momento cifrado.
- Se deben configurar reglas específicas en el Firewall, teniendo en cuenta únicamente los servicios, puertos, origen y destino necesarios y expresamente autorizados.

13.2. TRANSFERENCIA DE INFORMACIÓN

13.2.1. Políticas y procedimientos de transferencia de información.

- Se deben establecer procedimientos y controles formales que protejan el intercambio de información mediante el uso de los recursos de TI de la SCRD y las partes interesadas.

13.2.2. Acuerdos sobre transferencia de información.

- Se deben establecer y hacer firmar por las partes interesadas acuerdos para la transferencia y/o intercambio seguro de información.
- Se deben definir las características técnicas para la transferencia y/o intercambio seguro de información.
- Se deben definir los controles de acceso pertinentes para la transferencia y/o intercambio seguro de información.

13.2.3. Mensajes electrónicos.

- La Oficina de Tecnologías de la Información es la dependencia encargada de proporcionar el servicio de correo institucional, así como vigilar su correcto uso y funcionamiento.

- Los funcionarios públicos y contratistas de la Entidad contaran con una cuenta de correo institucional, al igual que las dependencias, los proyectos y los eventos oficiales de la Secretaría Distrital de Cultura, Recreación y Deporte.
- Cada buzón de correo tendrá un espacio máximo de almacenamiento, por lo tanto, los funcionarios públicos deben depurar continuamente su buzón de correo, con el fin de mantener siempre espacio disponible para enviar y recibir nuevos mensajes.
- Los usuarios no deben abrir correos de remitentes desconocidos o sospechosos y no activar ningún tipo de enlace ni ejecutar archivos adjuntos.
- Los colaboradores de la Secretaría Distrital de Cultura, Recreación y Deporte no pueden emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos de la Entidad.
- La información contenida en el buzón de correo se considera privada, por lo tanto, debe ser manejada como una comunicación directa entre el remitente y su destinatario.
- Cada usuario es responsable de la información enviada y/o remitida desde su cuenta de correo.

13.2.4. Acuerdos de confidencialidad o de no divulgación.

- Se deben establecer y hacer firmar acuerdos de confidencialidad o no divulgación de información con las partes interesadas (funcionarios, contratistas y terceros).

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

14.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

14.1.1. Análisis y especificación de requisitos de seguridad de la información

- Los enunciados de los requerimientos para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.
- La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en la Secretaría Distrital de Cultura, Recreación y Deporte, deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad de la Oficina de Tecnologías de la Información y las dependencias propietarias del sistema en cuestión.
- Si los productos son comprados, se debe realizar un proceso de prueba y adquisición formal, identificando dentro de los contratos con el proveedor los requerimientos de seguridad identificados anteriormente. Cuando la funcionalidad de seguridad de un producto propuesto no satisface el requerimiento especificado entonces se debieran reconsiderar el riesgo introducido y los controles asociados antes de comprar el producto.
- Dentro de las actividades a desarrollar durante la validación de los datos, se debe encontrar:
- Se deben verificar las entradas duales u otras entradas, tales como verificación de fronteras o campos limitantes para especificar los rangos de los datos de entrada, con el fin de detectar

errores (valores fuera de rango, caracteres no válidos en los campos de datos, datos incompletos o ausentes, exceso en los límites superiores e inferiores del volumen de datos, datos de control inconsistentes o no autorizados) durante la validación de datos en el desarrollo.

- Se deben ejecutar revisiones periódicas del contenido de los campos clave y de los archivos de datos para confirmar su validez e integridad.
- Se deben inspeccionar los documentos de entrada para determinar cambios no autorizados (todos los cambios en los datos de entrada deben estar autorizados).
- Durante la validación de datos en el ciclo de desarrollo se deben diseñar y documentar los procedimientos de respuesta ante errores de validación y procedimientos para probar la credibilidad de los datos de entrada.
- Se deben establecer los roles y responsabilidades para todo el personal que participa en el proceso de entrada de datos y se debe crear un registro de las actividades implicadas en el proceso de entrada de datos, en el ciclo de desarrollo.
- Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
- Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.
- Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
- Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.
- Durante la validación de datos de salida se deben validar los suministros de información para que un lector o un sistema de procesamiento posterior, puedan determinar la exactitud, totalidad, precisión y clasificación de la información.
- Se deben definir las responsabilidades de todo el personal que participa en el proceso de la salida de datos.
- Dentro de los términos de referencia de las aplicaciones se debe tener en cuenta el control de acceso, autenticación y mecanismos de autorización, en las medias de seguridad a tener en cuenta durante el análisis y especificaciones de seguridad.
- El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.

14.1.2. Seguridad de servicios de las aplicaciones en redes públicas.

- Se deben utilizar controles criptográficos en las aplicaciones para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Se debe establecer el nivel de protección adecuado para mantener la confidencialidad e integridad de la información.

- Se debe evitar la pérdida o duplicación de información en las transacciones que se realizan en los aplicativos.
- Se deben aplicar protocolos y puertos seguros para la comunicación con las aplicaciones.

14.1.3. Protección de transacciones de servicios de aplicaciones.

- Se debe aplicar protocolos y puertos seguros para la comunicación con las aplicaciones.
- Se debe aplicar rutas de comunicación cifradas entre todas las partes involucradas.
- Se debe aplicar la implementación de autoridades de confianza en los aplicativos.

14.2. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE

14.2.1. Política de desarrollo seguro.

- Se deben establecer y aplicar lineamientos para el desarrollo de software y de sistemas a los desarrollos de la SCRD.

14.2.2. Procedimiento de control de cambios en sistemas.

- Los cambios a los sistemas de información y aplicativos dentro del ciclo de vida de desarrollo se deben controlar mediante un procedimiento formal de control de cambios.

14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

- Cuando se cambien los sistemas operativos o componentes de operación, se deben revisar las aplicaciones críticas de la entidad y realizar pruebas, para asegurarse que no existen fallas en la operación o problemas de seguridad de la información.
- Se deben revisar los procedimientos de control y de integridad de las aplicaciones para asegurarse de que no han sido comprometidos por los cambios en los sistemas operativos.

14.2.4. Restricciones sobre los cambios en los paquetes de software

- Se deben verificar las modificaciones en los paquetes y componentes de software, limitándose a los cambios necesarios, y todos los cambios que se realicen deben ser objeto de un control y pruebas para garantizar su correcto funcionamiento.

14.2.5. Principios de construcción de sistemas de seguros

- Se deben aplicar lineamientos y directrices para la construcción de sistemas de información y aplicativos seguros. La seguridad en el desarrollo de software se debe contemplar en todas las fases del ciclo de vida de los aplicativos.
- Se deben verificar los medios y las comunicaciones de salida para evitar la fuga de información por programas maliciosos.

14.2.6. Ambiente de desarrollo seguro

- Se deben implementar ambientes para el desarrollo de software seguro.

- Se debe controlar y limitar el acceso de los desarrolladores a los demás ambientes, con el fin de proteger la información y la funcionalidad de los aplicativos y sistemas de información.
- Se debe restringir el acceso al código fuente y las librerías de los aplicativos desarrollados para la Entidad, así como el software para su servicio.
- Se deben conservar las versiones anteriores del software de aplicación como medida de contingencia.

14.2.7. Desarrollo contratado externamente

- Se debe supervisar y monitorear el desarrollo de software que sea contratado de forma externa, para que cumpla los lineamientos establecidos por la SCRD para el desarrollo de sistemas de información y aplicaciones.
- Se deben aclarar y especificar acuerdos sobre: las licencias, propiedad de los códigos y derechos y cesión de propiedad intelectual, convenios de fideicomiso en caso de falla de la tercera parte, derechos de acceso para auditar la calidad y exactitud del trabajo realizado, requisitos contractuales para la calidad y la funcionalidad de la seguridad del código, ejecución de pruebas antes de la instalación para detectar códigos troyanos o maliciosos y/o el empleo de funciones que afecten la seguridad de la información en los aplicativos.
- Ningún software debe estar en producción sin soporte y se debe prever que en la contratación quede establecida la transferencia tecnológica.
- Dentro de los acuerdos o contratos con los entes externos, es importante la definición de una metodología de desarrollo, el periodo de mantenimiento de software, los acuerdos de confidencialidad con el fin de resguardar adecuadamente la información.

14.2.8. Pruebas de seguridad de sistemas

- Se deben realizar pruebas de seguridad tanto a los desarrollos internos como externos, en cada una de las fases del ciclo de vida del desarrollo de los sistemas de información y aplicativos.

14.2.9. Pruebas de aceptación de sistemas

- Para los sistemas de información y aplicativos nuevos, actualizaciones y/o nuevas versiones, se debe realizar pruebas y establecer los criterios de aceptación para el paso a producción.

14.3. DATOS DE PRUEBA

- Se debe seleccionar cuidadosamente, proteger, generar y controlar la data de prueba.
- No está permitido el uso y copia de información operacional como datos de pruebas, salvo autorización previa de la Oficina de Tecnologías de la Información y el Responsable del activo, esta autorización sede ser solicitada cada vez que se requiere realizar la copia información operacional en un sistema de aplicación de prueba; de igual forma, la información operacional debe ser borrada de los sistemas de aplicación de prueba inmediatamente después de haber completado la prueba; registrar el copiado y uso de la información operacional para proporcionar un rastro de auditoría.

15. RELACIONES CON LOS PROVEEDORES

15.1. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

- Antes del inicio de cualquier actividad con terceros, se debe realizar un análisis de riesgos para establecer los requisitos de seguridad y controles adicionales, estos deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.
- Los requerimientos de seguridad de la información identificados, las obligaciones derivadas de las leyes de propiedad intelectual y los derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre la Secretaría Distrital de Cultura, Recreación y Deporte y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información.
- Es responsabilidad de la Oficina de Tecnologías de la Información garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con el Grupo Interno de Trabajo de Contratación establecer estos aspectos con las obligaciones contractuales específicas.

15.2. GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES

- Las partes interesadas, proveedores, clientes y otros asociados a la Entidad deben tener conocimiento de sus responsabilidades relacionadas con la seguridad de la información y esta responsabilidad se debe ver reflejada en los contratos con la Secretaría Distrital de Cultura, Recreación y Deporte.
- Cualquier acceso por parte de un tercero a los recursos tecnológicos o a la información de la Entidad, debe haber cumplido con las autorizaciones respectivas y además contar los acuerdos de confidencialidad respectivos debidamente firmados.
- Al momento de terminar relaciones con un tercero el cual maneje información de la Entidad, el tercero debe destruir de una manera adecuada la información o en su debido defecto devolver la información, proceso que deberá estar incluido en el contrato con el tercero.
- Dentro de los acuerdos de servicios con terceras partes se debe incluir una cláusula, la cual autorice a la Secretaría Distrital de Cultura, Recreación y Deporte a realizar auditoria para validar los controles utilizados por los terceros para el manejo de la información.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1. GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

- Se debe establecer un punto de contacto para el reporte formal de eventos e incidentes de seguridad de la Información, este debe ser conocido a través de toda la entidad, debe estar disponible y debe proporcionar una respuesta adecuada y oportuna a los usuarios.

- Se requiere que todos los empleados, contratistas y terceros Todos los funcionarios públicos de la entidad deben tener conciencia sobre los procedimientos de reporte de los diferentes tipos de eventos e incidentes de seguridad que puedan tener impacto sobre los activos de información.
- Deben tomarse acciones correctivas oportunas, ante los eventos e incidentes de seguridad reportados, con base en el aprendizaje obtenido en la gestión de incidentes de seguridad.
- Es deber de todos los funcionarios públicos, contratistas y terceros usuarios de los sistemas y servicios de información reporten cualquier evento o incidentes que atente contra la seguridad de los activos de información.
- Se deben mantener las evidencias necesarias para establecer el reporte del incidente de seguridad para toda acción de seguimiento contra una persona u entidad. Así mismo contar con los soportes que sean exigidos por una acción legal (sea civil o criminal).
- Se deben establecer categorías de los eventos e incidentes de seguridad y conforme a la criticidad, se establecen los mecanismos de atención adecuados para su solución. Así mismo, se lleva un registro de cada uno de los incidentes reportados, con su respectiva estadística.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

17.1.1. Planificación de la continuidad de la seguridad de la información

- La SCRD debe planificar, implementar, verificar revisar y evaluar el plan de continuidad tecnológica y seguridad de la información de la entidad y los planes de contingencia basados en el análisis y la valoración de los riegos a los cuales se encuentra expuesta la entidad.
- La Oficina de Tecnologías de la Información debe establecer un conjunto de tareas con sus respectivos responsables para gestionar la continuidad de la operación tecnológica y de la seguridad de la Información reduciendo, a niveles aceptables, la interrupción causada por desastres naturales, fallos funcionales o de seguridad en la infraestructura tecnológica mediante la implementación de controles preventivos, de recuperación y correctivos.
- Implementación de la continuidad de la seguridad de la Información
- Se debe realizar una identificación de los procesos críticos de la entidad y realizar un análisis de impacto para determinar los aspectos y responsabilidades más importantes que puedan afectar en la prestación de servicio y continuidad tecnológica y de seguridad de la información de la SCRD.
- Teniendo en cuenta el tiempo que puede tomar la implementación del plan de continuidad tecnológica y de seguridad de la información de la SCRD, cada una de las dependencias de la entidad debe desarrollar e implementar planes de contingencia sencillos, tales como tareas manuales temporales y copias de respaldo, para asegurar que sus procesos y las operaciones más importantes pueden restaurarse de manera oportuna. Para estos planes de contingencia se deben analizar las consecuencias de posibles desastres, fallas en el

funcionamiento y la seguridad de los dispositivos de la infraestructura tecnológica, pérdidas de disponibilidad de datos, servicios y sistemas de información críticos identificados en el BIA.

17.1.2. Verificación revisión y evaluación de la continuidad de la Seguridad de la Información

- Todos los funcionarios públicos de la SCRD deben participar proactivamente en las actividades que sean designadas por la Alta Dirección, para las pruebas del plan de continuidad de la seguridad de la información y deben cumplir con los lineamientos establecidos por el SGSPI.
- La Alta Dirección es responsable de asignar el recurso necesario para la ejecución de las pruebas de continuidad del negocio.
- Los planes de continuidad tecnológica de la entidad deben ser objeto de pruebas y revisiones periódicas, las cuales garanticen su actualización, eficiencia y desempeño en su ejecución; además de servir como parte del entrenamiento respectivo, por todos los actores involucrados en el evento de interrupción de las operaciones tecnológicas normales de la SCRD.

17.2. REDUNDANCIAS

17.2.1. Disponibilidad de instalaciones de procesamiento de Información

- La Oficina de Tecnologías de la Información es la responsable de implementar las redundancias suficientes y garantizar la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica, así como también debe implementar configuraciones en alta disponibilidad para minimizar la probabilidad de la interrupción del acceso a la información. Estas configuraciones deben ser probadas y documentadas por los responsables de administrar los componentes tecnológicos de la SCRD.

18. CUMPLIMIENTO

18.1. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

18.1.1. Identificación de la Legislación Aplicables y de los Requisitos Contractuales

- La SCRD se compromete a asegurar el cumplimiento de las leyes y normas reglamentarias y regulatorias establecidas en el país (y países donde se encuentre y tenga relaciones comerciales), así como de velar por el cumplimiento de la normatividad interna desarrollada para la protección de la información en la entidad, para ello, se deben definir y documentar todos los requisitos normativos y contractuales pertinentes para cada sistema de información.
- Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la entidad relevante para cada sistema de información y la entidad una vez al año y/o cada vez que estos sean requeridos.

18.1.2. Derechos de Propiedad Intelectual

- Las aplicaciones desarrolladas por los colaboradores de la SCRD para uso interno deben ser desarrolladas usando software de propiedad, licenciado o autorizado por la entidad en el caso de software libre.
- Todo el software utilizado por la entidad, para trabajar o desarrollar debe estar licenciado y debe ser usado únicamente bajo los términos y condiciones definidos en las licencias.
- Todo colaborador de la SCRD y terceras partes es responsable de garantizar que todo material utilizado con propósito laboral cumpla con la legislación de derechos de propiedad intelectual.
- Los responsables de las aplicaciones deben asegurar que el número máximo de usuarios permitidos por las licencias no sea excedido, para tal efecto se deben realizar monitoreos periódicos de la utilización de software que se encuentren en la línea base de la SCRD.
- Los funcionarios públicos, contratistas y terceras partes, no pueden por ningún motivo descargar o almacenar archivos de música, fotos, videos, o material sujeto a propiedad intelectual en los equipos de la SCRD.
- La SCRD debe identificar y garantizar el cumplimiento adecuado a la legislación vigente y/o requisitos legales aplicables (derechos de propiedad intelectual, protección de registros, privacidad y protección de la información de datos personales, Reglamentación de controles criptográficos) de seguridad de la información.
- El propietario del material con derechos de autor tiene derechos exclusivos para la reproducción y distribución de dicho material. Es ilegal duplicar o distribuir software o su documentación sin permiso del propietario de los derechos de autor. Los colaboradores de la SCRD deben cumplir con las leyes de derechos de autor y acuerdos de licencia, la reproducción no autorizada de software con derechos de autor es una violación de la ley.
- Los nombres de dominios registrados por la SCRD, no pueden ser usados por otras organizaciones; deben ser protegidos y asegurados de manera similar a cualquier otro activo de valor de la Entidad.

18.1.3. Privacidad y Protección de Datos Personales

- LA SCRD cuenta una política de protección de datos personales, así como también gestiona los controles, e instrumentos de la misma de acuerdo a la Ley 1581 del 2012 y sus decretos reglamentarios.

18.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

18.2.1. Revisión Independiente de la Seguridad de la Información

- La SCRD debe establecer controles periódicos para revisar y garantizar el cumplimiento de los controles de seguridad de seguridad frente al marco regulatorio y los objetivos de la entidad, a través de programas de auditorías internas y externas en los intervalos planificados.
- Cada grupo o dependencia debe asegurarse de que las revisiones periódicas del cumplimiento de conformidad al SGSPI se lleven a cabo con la cooperación del personal encargado de las auditorías internas.

- La frecuencia de las revisiones se debe basar en el riesgo y criticidad del ambiente de proceso, de los principales cambios, o de las nuevas regulaciones o leyes.
- La SCRD debería realizar auditorías independientes con personal interno y/o externo a la entidad a intervalos planificados o siempre que se produzcan cambios significativos al sistema de gestión de seguridad y privacidad de la información. Estas también pueden ser desarrolladas por la Oficina de Control Interno, o por organizaciones externas como ACDTIC u otras.
- Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad. Así mismo, en relación con los procedimientos de análisis, desarrollo y mantenimiento de las aplicaciones, se deben realizar revisiones técnicas y si en algún caso, no se cumple a cabalidad un control establecido dentro de las políticas de seguridad durante la verificación, se deben determinar las causas del incumplimiento.
- Si se encuentra alguna no conformidad como resultado de la revisión, es necesario identificar las causas de ésta, evaluar las acciones de mejora para lograr el cumplimiento, implementar estas acciones y revisar nuevamente para verificar su eficacia.

18.2.2. Cumplimiento con las Políticas y Normas de Seguridad

- Todos los funcionarios públicos, contratistas y terceros de la SCRD, deben velar por el cumplimiento de las normas y procedimientos del SGSPI establecido, las cual está incluida dentro de sus responsabilidades.

19. NORMAS DE POLÍTICA DE TRABAJO REMOTO

19.1. LIDERES DE PROCESO

- Autorizar a los funcionarios públicos y contratistas los permisos de acceso remoto a sistemas de Información y medios de almacenamiento de los cuales dispondrán.
- Identificar los activos de información necesarios para realizar el trabajo remoto.

19.2. A LA OFICINA DE TECNOLÍGIAS DE LA INFORMACIÓN

- Establecer los mecanismos de gestión y recursos técnicos de comunicación para proveer el servicio de conexión remota a los sistemas internos y acceso a la información a la que tendrán acceso los usuarios autorizados.
- Dar soporte técnico a los equipos, conexiones, sistemas de información, medios de almacenamiento y comunicación de propiedad de la SCRD usados en trabajo remoto.
- Restringir las conexiones remotas a los recursos de la plataforma tecnológica de SCRD; únicamente a los equipos autorizados.
- Monitorear el uso de los recursos e infraestructura dispuesta para el trabajo remoto, previniendo y detectando vulnerabilidades, ataques cibernéticos y otras amenazas; así como incidentes de seguridad digital.

19.3. A FUNCIONARIOS PÚBLICOS, CONTRATISTAS Y PERSONAL DE TERCEROS

- En los equipos de cómputo utilizados para realizar el trabajo remoto configurar el inicio de sesión con algún medio de autenticación como password, pin, y/o huella.
- Almacenar la información tratada durante el trabajo remoto en el servicio en la nube que disponga la SCRD para almacenar, proteger y compartir los archivos.
- Resguarda y proteger la información de acuerdo con la clasificación de los activos de información.
- Proteger la información a la que se tiene acceso en los lugares en los que se realiza trabajo remoto.
- Informar inmediatamente de cualquier evento de riesgo que pueda generar compromiso sobre: el equipo de SCRD, la información, credenciales de acceso, los sistemas de información, los medios de almacenamiento y las comunicaciones usados para el trabajo remoto.
- Proteger físicamente los equipos de SCRD que se utilicen para realizar trabajo remoto para prevenir el robo de éstos, transportándolos y guardándolos en un lugar seguro, usando guaya siempre que sea posible, y protegiéndolos, en especial en lugares públicos.
- No conectarse a los sistemas de información, medios de almacenamiento y comunicación usados para el trabajo remoto desde redes públicas, en lo posible usar redes cableadas.
- Usar únicamente las aplicaciones colaborativas y de teleconferencia permitidas por la SCRD, así como sus condiciones de uso, está prohibido ingresar a programas no controlados o autorizados por la SCRD.
- Reforzar las políticas de seguridad aplicables, como evitar hacer clic en enlaces que parecen sospechosos, descargar anexos solamente de fuentes conocidas, no abrir correos de remitentes desconocidos, evitar el uso de redes sociales y aplicaciones de mensajería no corporativa, evitar navegar por páginas no seguras, así como evitar el uso de soportes externos de almacenamiento como dispositivos USB y en caso de utilizarlos, escanearlos con el software antivirus.
- En caso de utilizar equipo personal para el desarrollo de trabajo remoto, es necesario cumplir con las siguientes condiciones:
- Mantener actualizado el Sistema Operativo.
- Garantizar el buen funcionamiento del equipo.
- Se recomienda contar con antivirus instalado, activo y actualizado y licenciamiento de software instalado en dicho equipo de cómputo.

CONTROL DE CAMBIOS

No.	CAMBIOS REALIZADOS
1	Este documento sustituye el Manual de políticas de seguridad y privacidad de la Información de la Secretaría de Cultura, Recreación y Deporte 2021 v1.

No.	CAMBIOS REALIZADOS
2	Se actualizó el numeral 8 con sus respectivos subnumerales, cuya finalidad fue la inclusión de temas de identificación de información relevante interna y externa de la entidad y manejo de información sensible, relacionada con la clasificación de la información en concordancia con la Ley 1712 de Transparencia y Acceso a la Información Pública. Ver solicitud de modificación del 18/07/2022, radicado 20221600266143.

Responsables de elaboración, revisión y aprobación

ELABORADO POR *Persona(s) responsable(s) de crear, proyectar la modificación y/o ajuste del documento*	APROBADO POR *Líder del Proceso quién debe hacer cumplir el contenido establecido en el documento*	REVISADO POR *Persona(s) de la OAP responsable(s) de verificar que el documento contenga los lineamientos establecidos*	AVALADO POR *Jefe de la Oficina Asesora de Planeación*
NOMBRE: Nicolas Andrés Villamil Padilla	NOMBRE: Viviana Margarita Bayuelo Serrano	NOMBRE: Nelson Velandia Angelmiro Vargas	NOMBRE: Carlos Alfonso Gaitán
CARGO: Contratista OTI	CARGO: Jefe de Oficina de Tecnologías de la Información y las comunicaciones	CARGO: Profesional Universitario Profesional Universitario	CARGO: Jefe de Oficina Asesora de Planeación
FIRMA: Electrónica	FIRMA: Electrónica	FIRMA: Electrónica	FIRMA: Electrónica

Radicado: **20231700273393**
Fecha 11-07-2023 11:09

Documento firmado electrónicamente por:

Nicolas Andres Villamil Padilla, CONTRATISTA, Oficina de Tecnologías de la Información, Fecha de Firma: 10-07-2023 15:05:41

Viviana Margarita Bayuelo Serrano, Jefe Oficina de Tecnologías de la Información, Oficina de Tecnologías de la Información, Fecha de Firma: 07-07-2023 16:22:46

Angelmiro Vargas Cardenas, PROFESIONAL UNIVERSITARIO 219-10, Oficina Asesora de Planeación, Fecha de Firma: 05-07-2023 14:52:43

Carlos Alfonso Gaitán Sánchez, Jefe Oficina Asesora de Planeación, Oficina Asesora de Planeación, Fecha de Firma: 11-07-2023 11:09:26

Revisó: Angelmiro Vargas Cardenas - PROFESIONAL UNIVERSITARIO 219-10 - Oficina Asesora de Planeación

db2bfad1edb86740a6382bf0a6f5dadd1d31c20f4d80117ffb09569238f19d1a