TABLA DE CONTENIDO

1. DEFINICIONES

ACTIVO DE INFORMACIÓN: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas.) que tenga valor para la corporación.

ALTO IMPACTO: El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales del Instituto. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.

BAJO IMPACTO: El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

CIFRADO: Es la transformación de datos de un formato comprensible a un formato codificado, que solo se pueden leer o procesar después de haberlos descifrado

CONFIDENCIALIDAD: Propiedad que determina que la información sólo esté disponible y sea revelada a las personas autorizadas.

CONTRASEÑA: Una contraseña o clave es conjunto de caracteres que hacen parte de la información secreta para acceder algún recurso tecnológico. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso.

CONTROL DE ACCESO: Procedimiento el cual tiene como objetivo controlar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y red de la corporación.

CONTROLES TECNOLÓGICOS: Son aquellos controles técnicos aplicados para garantizar la seguridad en la plataforma tecnológica de la corporación.

CORREO ELECTRÓNICO: Es el servicio que permite intercambiar mensajes a través de sistemas de comunicación electrónicos.

DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una Corporación autorizada, cuando ésta así lo requiera

ESCANEOS DE SEGURIDAD: Es un análisis, identificación y reporte muy sistemático de las debilidades en cuestión de seguridad de la información que tiene una plataforma tecnológica

EVALUACIÓN DE RIESGOS: Proceso global de identificación, análisis y estimación de riesgos en la operación del Concejo de Bogotá, D.C.

INCIDENTE DE SEGURIDAD GRAVE: Es un incidente de seguridad que genera un alto impacto.

INCIDENTE DE SEGURIDAD: Evento único o serie de eventos de seguridad de la información inesperada o no deseado que poseen una probabilidad significativa de comprometer la seguridad de la información de la corporación.

INTEGRIDAD: Propiedad de exactitud y completitud de la información.

INTERNET: Es un sistema mundial de redes de computadoras, integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computadora puede, en caso de contar con los permisos apropiados, obtener información, efectuar transacciones, comunicarse y participar en toda gama de procesos públicos y privados puesto en dicha red.

INTRANET: Red de una organización que utiliza tecnologías y protocolos de Internet, pero que sólo está disponible para determinadas personas, por ejemplo, para los empleados de una compañía. Una Intranet también recibe el nombre de red privada.

MEDIO IMPACTO: El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.

MSPI: Modelo de Seguridad y Privacidad de la información, comprende las acciones transversales a los demás procesos, tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

NAVEGACIÓN SEGURA: Es la navegación en internet de forma segura protegida frente amenazas que puedan afectar la seguridad de la información.

PLATAFORMA TECNOLÓGICA: es un conjunto de elementos físicos (hardware) y lógicos (software) a través de los cuales se prestan servicios de tecnologías de la información.

POLÍTICA: Es el marco referencial o lineamiento general emitido por la Alta Dirección, que orienta para las actuaciones, conductas o funciones de los colaboradores y dependencias.

PUNTO DE ACCESO INALÁMBRICO: Es un punto de conexión inalámbrica que permite interconectar los dispositivos móviles como lo son los equipos de cómputo portátiles.

REDES CORPORATIVAS: Conexión de redes empresariales de forma permanente, privada, segura y fiable.

ROL: Es un conjunto de permisos que puede asignarse a un usuario que se registra en un administrador de sistemas. Normalmente, los roles se definen de modo que incluyan permisos que guarden cierta relación y suelen corresponderse con algún rol de la vida real.

SERVICIOS DE COMUNICACIONES: Son aquellos servicios tales como el internet, intranet, directorios compartidos y correo electrónico.

SISTEMA DE INFORMACIÓN: Se refiere a un conjunto de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

TECNOLOGÍA DE LA INFORMACIÓN (TI): Se refiere a los elementos de hardware y software que intervienen en el procesamiento de la información y son utilizados para almacenar, recuperar, transmitir y manipular datos y que permiten llevar a cabo una función propia del Concejo de Bogotá D.C.

TRAZABILIDAD: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo funcionarios, contratistas, terceros, entre otros inequívoco a un individuo o Corporación.

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

2. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN -MSPI

2.1. OBJETIVOS DEL MSPI

- Implementar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información (MSPI) como mecanismo para brindar a los ciudadanos y colaboradores confianza digital en torno al uso de los datos, al cumplimiento legal y mantener una actitud ética, transparente y en concordancia con la misión y la visión de la Corporación.
- Integrar la seguridad de información con la estrategia organizacional para apoyar los objetivos de la organización, gestionar los riesgos y fortalecer la seguridad en sus componentes de integridad, disponibilidad y confidencialidad.

3. CONTEXTO DE LA ORGANIZACIÓN

3.1. COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO

El Concejo de Bogotá es una corporación político-administrativa de elección popular; es la máxima autoridad política de la capital y la segunda autoridad administrativa más importante de la ciudad después de la Alcaldía Mayor. Ejecuta principalmente dos funciones: actividad normativa y control político. El Concejo de Bogotá está compuesto la plenaria conformada por 45 concejales de diferentes partidos políticos entre los cuales se elige la Mesa Directiva y las Comisiones Permanentes: Comisión Primera del Plan de Desarrollo y Ordenamiento Territorial, Comisión Segunda Permanente de Gobierno y la Comisión Tercera Permanente de Hacienda y Crédito Público, con sus respectivas mesas directivas, adicional cada concejal cuenta con una Unidad de Apoyo Normativo - UAN .

Desde el punto de vista administrativo el Concejo de Bogotá cuenta con las siguientes dependencias: Secretaría General, Dirección Jurídica, Dirección Administrativa, Dirección Financiera, Oficina de Control Interno, Oficina Asesora de Planeación y Oficina Asesora de Comunicaciones

3.2. DETERMINACIÓN DEL ALCANCE DEL MSPI

Estas políticas se aplican en todo el ámbito del Concejo de Bogotá D.C., a sus procesos y personal con algún tipo de vínculo contractual con la Corporación. Por tal motivo, tanto el presidente, como los Honorables Concejales, Secretario General, Subsecretarios, Jefes, Directores, Asesores, Funcionarios, Contratistas y Servidores Públicos en general, sea cual fuere su nivel jerárquico, son responsables del cumplimiento de estas políticas de seguridad de la información.

3.3. REQUISITOS LEGALES Y OTROS REQUISITOS

Ver normograma del Concejo de Bogotá.

4. LIDERAZGO

4.1. ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

- Comité Institucional de Gestión y Desempeño: como órgano articulador del Concejo de Bogotá este comité debe aprobar y hacer el seguimiento a la política de seguridad de la información, así como apoyar su implementación al interior de la Corporación.

- Equipo Técnico de Seguridad de la Información: Comunicar a los funcionarios, contratistas y/o particulares que participan en actividades de forma directa o indirecta con la entidad, la importancia de satisfacer los requisitos de seguridad digital.
- Responsable de Seguridad de la Información: Diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad de la información, y someterlos a decisión del Equipo Técnico de Seguridad de la Información, realizando la implementación y seguimiento de estos.
- Líderes de proceso: Identificar e inventariar los nuevos activos digitales de información y los riesgos cibernéticos asociados a sus procesos.
- Líder del Proceso de Sistemas y Seguridad de la Información: Participar en la elaboración del cronograma de capacitación de seguridad digital en la Corporación. Implementar las mejorar identificadas en la plataforma de seguridad que estén relacionadas con hardware, software, canales de comunicaciones de datos o infraestructura de TI (Tecnologías de la Información).
- Partes interesadas (funcionarios, contratistas y proveedores): cumplir con las políticas de seguridad y privacidad de la información y cláusulas establecidas en el MSPI.

5. POLÍTICAS

5.1. Políticas de dispositivos móviles

- La Corporación establece las condiciones para el uso seguro de los dispositivos móviles (portátiles, teléfonos, inteligentes, tabletas, entre otros) institucionales que hagan uso de servicios de la Corporación como son: Establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.
- Los funcionarios y contratistas no están autorizados a cambiar la configuración, ni la instalación/desinstalación de las aplicaciones móviles de los dispositivos móviles institucionales que se les entregue como recurso para la ejecución de sus obligaciones o funciones.
- Es responsabilidad del servidor público al que se le asignó el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Los servidores públicos deben evitar conectar los dispositivos móviles institucionales a puertos USB de computadores públicos, hoteles o cafés internet, terminales, y demás sitios de acceso público.
- Los servidores públicos y contratistas deben notificar los dispositivos móviles institucionales con sospecha de infección por malware al personal técnico responsable de la Corporación para el proceso de análisis, evaluación y tratamiento.
- Todos los dispositivos móviles propiedad de la Corporación pueden ser monitoreados y sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

5.2. Políticas de teletrabajo

- La Corporación brinda los lineamientos de seguridad digital para la protección de la información a la que se tiene acceso, se procesa o almacena en lugares en los que se realiza Teletrabajo y se hace uso de los recursos tecnológicos autorizados por la Corporación para el desarrollo de las actividades de Teletrabajo.
- Toda información gestionada por la Corporación, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con esta.
- La Corporación establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de la Corporación, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.
- La Corporación establece el proceso de implementación de teletrabajo, de acuerdo con la normativa y los lineamientos exigidos, con el fin de proteger la información.
- La Corporación revisa la seguridad física y del entorno del sitio donde se va a teletrabajar, con el fin de proteger la confidencialidad, integridad y disponibilidad.

5.3. Políticas de seguridad del recurso humano

- El área que realice la contratación de personal en la Corporación realiza las verificaciones de los antecedentes (procuraduría, contraloría, policía) de los candidatos al cargo, la formación académica, experiencia y demás información que se requiera, de acuerdo con las leyes, reglamentos de la Corporación y ética pertinente.
- Todo servidor público y contratista debe recibir inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Corporación.
- La Corporación establece directrices para asegurar que los servidores públicos y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación con la seguridad de la información.
- La Corporación dentro de su proceso de vinculación servidores públicos o contratistas solicitará la suscripción de los compromisos de confidencialidad y aceptación de políticas de seguridad de la información establecidos por el Concejo de Bogotá D.C.
- El proceso de Talento Humano junto con los responsables de la contratación realizan el proceso de desvinculación, licencias, vacaciones o cambio de labores de los servidores públicos y contratistas llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin, Así mismo, los directores, jefes, supervisores de contrato o líderes deben informar la desvinculación o cambio de labores de acuerdo con los procedimientos, está información debe ser entregada oportunamente al proceso de Sistemas y Seguridad de la Información - SSI.
- La Corporación debe incorporar los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros.
- El incumplimiento o la violación de las políticas de seguridad de la información de la Corporación, por parte de las personas relacionadas en el alcance de la presente política, se les aplicará lo establecido en el proceso de investigaciones disciplinarias.

5.4. Políticas de gestión de activos

- La Corporación establece los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información.
- Cada activo de información de la Corporación debe tener un responsable que debe velar por su seguridad. Los propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención.
- Es responsabilidad del líder de proceso, jefe de área o director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.
- Los servidores públicos y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Corporación.

5.5. Políticas de control de acceso

- La Corporación define los lineamientos para asegurar un acceso controlado, físico o lógico, a la información y plataforma tecnológica, considerándolas importantes para el sistema de gestión de seguridad de la información.
- La Corporación establece procedimientos enfocados a garantizar el cumplimiento de las políticas de seguridad de la Información.
- Todos los servidores públicos y contratistas con acceso a un sistema de información o a la red informática institucional, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña y serán responsables de las acciones realizadas por el usuario que les ha sido asignado.
- Si una Entidad, empresa o personal externo requiere acceso a información sensible o crítica, se deben suscribir acuerdos de confidencialidad o de no divulgación para salvaguardar la información, así como el cumplimiento de la normatividad vigente para la Corporación.
- Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.
- Se realiza seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.
- Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministradas de acceso a la red, sistemas de información, aplicaciones, entre otros.

5.6. Políticas de seguridad física y del entorno

- Las oficinas administrativas, áreas de procesamiento de información, equipos tecnológicos y de soporte, información de medios físicos entre otros, son base para el cumplimiento de los objetivos de la Corporación, por tanto, se establecen y mantienen controles para resguardar la seguridad de las instalaciones y ambientes de trabajo, el acceso a las áreas.

- Los equipos de cómputo que pasen a un estado de retiro o se requieran para la reutilización deberán cumplir los siguientes lineamientos: a. Al momento de retirar un equipo en la organización (almacén), el proceso de Sistemas y Seguridad de la Información - SSI realiza una copia de respaldo de la información almacenada en este activo. b. El proceso de SSI realiza el proceso de borrado seguro de la información almacenada en los equipos que van a ser cedidos o reutilizados en la organización.
- Los servidores públicos y contratistas garantizan que no se disponga información de la Corporación en los escritorios de los equipos y que esta no estará almacenada y fácilmente copiada o accedida por alguien sin autorización desde un computador desatendido.
- Para todos los usuarios de las aplicaciones y sistemas de información de la Corporación, es obligatorio que las sesiones sean cerradas al finalizar las actividades y no se deben dejar abiertas o desatendidas.
- Todos los visitantes, sin excepción, deben portar la tarjeta de identificación de visitante o escarapela en un lugar visible mientras permanezcan en un lugar dentro de las instalaciones de la Corporación.
- Las áreas dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

5.7. Políticas de Controles Criptográficos

- Los discos duros internos, externos y memorias USB utilizados por las diferentes áreas o procesos de la Corporación, están cifrados mediante algoritmos de cifrado simétrico. El personal de cada proceso es quien debe solicitar el cifrado de la información que esté clasificada como crítica o sensible por la Corporación.
- La Corporación asegura el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la integridad y el no repudio de la información. Por lo cual, establece técnicas criptográficas y cifrado como son: Cifrado de la información cuando se requiere trasferir o almacenar información sensible o crítica, uso de protocolos seguros para las redes Wifi, uso de protocolo HTTPS con un nivel de cifrado actualizado.
- El acceso remoto a la red y los sistemas de información de la Corporación desde una red externa, será a través de conexiones seguras.
- Se debe contar con buenas prácticas para la gestión de llaves.

5.8. Políticas de seguridad en las operaciones

- La Corporación documenta los procesos operacionales a nivel de TI, para reducir riesgos asociados con ausencia de personal y afectaciones en la infraestructura tecnológica.
- La Corporación garantiza que las operaciones Tecnológicas se gesten de forma correctas y se brinde seguridad a las instalaciones de procesamiento de información
- Según la clasificación de la información establecida por la Corporación, se establecen las medidas de respaldo de la información a través de mecanismos como cintas, discos de almacenamiento o en la nube

- Los responsables de TI definen anualmente un cronograma de pruebas de restauración que permita validar la integridad y disponibilidad de la información almacenada, garantizando la confiabilidad del proceso ejecutado para copias de respaldo.
- El proceso de SSI es el encargado de aplicar los parches, controles o remediaciones derivadas de la ejecución de pruebas periódicas de análisis de vulnerabilidades.

5.9. Políticas de seguridad de las comunicaciones

- El Proceso de SSI realiza el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso de servidor proxy, firewall o control que mejor se ajuste a la necesidad.
- La Corporación asegura la protección de las redes y la trasferencia de información. Para dar cumplimiento se deben firmar acuerdos de confidencialidad y de no divulgación entre la Corporación y entidades externas con las cuales se intercambie información e implementar controles de seguridad al monitoreo de la red.
- El proceso de SSI implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Corporación.
- La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del activo tipo información involucrada.

5.10. Políticas de adquisición, desarrollo y mantenimiento de sistemas

- La Corporación garantiza que los sistemas de información estén asociados a lineamientos, procesos, buenas prácticas y demás requisitos que sirvan para regular los desarrollos de software internos en un ambiente controlado, así mismo se identifican y gestionan los posibles riesgos referentes a seguridad de la información durante todo el ciclo de vida del software.
- La Corporación busca que la Seguridad de la Información sea parte integral dentro ciclo de vida de desarrollo de los sistemas de información y en la adquisición de aquellos que presentan servicios a la Corporación, para ello establece el procedimiento de desarrollo seguro de software, la revisión técnica y de seguridad de las aplicaciones para detectar vulnerabilidades antes de salir a producción y la aplicación del procedimiento gestión de cambios.
- La Corporación asegura que se diseñe e implemente los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.
- La Corporación establece controles técnicos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.
- La Corporación cuenta con un ambiente de desarrollo y de pruebas seguro o, en su defecto, exige al proveedor mediante los contratos, que éste cuente con los controles de seguridad de la información sobre los ambientes.
- Los datos de pruebas que se utilicen durante todo el ciclo de vida de los sistemas de información deben ser seleccionados, utilizados y eliminados de forma segura.
- La Corporación deberá contar con una metodología de desarrollo seguro de software.

5.11. Políticas de relaciones con los proveedores

- Para proveedores críticos de tecnología, así como de procesos misionales, la Corporación exige que cuente con planes de continuidad de negocio y recuperación de desastres definidos e implementados, de modo que proveedor contratado puedan responder ante eventuales escenarios que afecten el suministro de servicios o productos a la Corporación.
- La Corporación controla las relaciones con proveedores, y en particular aquellos que tienen acceso a la información. La información está suficientemente protegida con base a los acuerdos y contratos correspondientes. Esta protección debe contemplarse antes, durante y a la finalización del servicio.
- Cualquier cambio que se realice con algún proveedor crítico de TI o de los procesos misionales, debe aplicarse mediante el procedimiento de gestión de cambios establecido en la Corporación.
- La Corporación realizará revisiones al cumplimiento de las Políticas de Seguridad y Privacidad de la Información por parte de los Proveedores.

5.12. Políticas de gestión de incidentes

- Todos los servidores públicos y contratistas deben conocer el método de reporte de eventos e incidentes de seguridad de la información.
- La Corporación debe asegurarse que todos los servidores públicos y contratistas conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información. Por lo tanto, se debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.
- En la gestión del incidente y cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables o comunicar a un ente competente para que realice el debido proceso.
- La Corporación establece y ejecuta procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.
- La Corporación debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.
- La Corporación cuenta con una bitácora de los incidentes de seguridad de la información reportados y atendidos.

5.13. Políticas de cumplimiento

- La Corporación gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros y los delitos informáticos.
- La Corporación asegura el conocimiento y cumplimiento de las obligaciones legales en materia de seguridad de la información. Por lo anterior, garantiza el cumplimiento de los derechos de propiedad intelectual de terceros controlando la adquisición y uso del software en la Corporación. Debe determinar las responsabilidades para gestionar la protección de datos personales.

6. APOYO O SOPORTE

6.1. TOMA DE CONCIENCIA

- La Dirección Administrativa brindará los lineamientos para que los servidores públicos, contratistas y proveedores de la Corporación tomen conciencia del cumplimiento de las políticas de seguridad de la información y reciban la educación y formación sobre las políticas y procedimientos relacionados.
- El proceso de Talento Humano y el supervisor del contrato deberán velar por que los servidores públicos, contratistas y proveedores de la Corporación, que desempeñen funciones en el mismo reciban entrenamiento y actualización periódica en materia de Seguridad de la Información.
- Será responsabilidad de Talento Humano, incorporar la aplicación de las políticas de seguridad de la información en su plan de capacitación institucional, y velar por la correcta inducción de los funcionarios nuevos en materia de seguridad de la información.

6.2. COMUNICACIÓN

- El presente manual de políticas de Seguridad y Privacidad de la Información será comunicado a todas las partes interesadas de la Corporación, a través de las tecnologías de la información y medios físicos de ser necesario.
- El Concejo de Bogotá D.C. deberá establecer los canales accesibles para la comunicación permanente de todas las políticas, procedimientos u otros documentos que hagan parte del Modelo de Seguridad y Privacidad de la Información (MSPI), algunos canales accesibles y formales para la comunicación son: Correo Electrónico, intranet, comunicación impresa, charlas y capacitaciones.

7. EVALUACIÓN DEL DESEMPEÑO

7.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

- Se deben establecer los indicadores de medición de los Objetivos de Seguridad y Privacidad de la Información.
- Se deben realizar revisiones mínimo una vez al año del cumplimiento de las políticas de Seguridad y Privacidad de la Información.
- Incluir el criterio de seguridad en los planes de auditoría anual.
- Dar respuesta a los incidentes de seguridad de la información reportados por la Corporación.

7.2. REVISIÓN POR LA DIRECCIÓN

El Comité Institucional de Gestión y Desempeño CIGD debe revisar periódicamente el Sistema de Gestión de Seguridad de la Información de la Corporación, para asegurarse de que su conveniencia, adecuación y eficacia son continuas.
La revisión por la dirección debe incluir consideraciones sobre:

- Seguimiento de tareas, actividades o acciones asignadas en la reunión anterior.

- Informe de resultados de las revisiones del Modelo de Seguridad de la Información al interior de los procesos.
- Resultados del último ciclo de auditoría interna al MSPI (informe de Auditoría Interna).
- Cambios en las cuestiones internas y externas que sean pertinentes al MSPI.
- Propuestas o mejoras al MSPI por parte de los servidores públicos y contratistas.
- Estado de acciones correctivas y de mejora (se evalúa la eficacia de las acciones), para Seguridad de la Información sólo aplica las acciones correctivas y de mejora.
- Retroalimentación de las partes interesadas.
- Resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos.
- Vulnerabilidades y amenazas no tratadas adecuadamente en la valoración previa de los riesgos.
- Revisión anual de la política, objetivos de Seguridad de la Información (su contenido y cumplimiento en los diferentes procesos) por medio de planes de acción.

7. CONTROL DE CAMBIOS		
Versión	Descripción	Fecha
01	Creación del documento	Dic-204
02	Modificación y Actualización Total del Manual de conformidad con la NTC - ISO/IEC 27001 :2013	27-oct-2017
03	Se modifica textos numerales: 8.3.1.3, 8.3.1.3.1, 8.3.1.3.2, 8.3.1.3.3, 8.3.1.3.4, 8.3.2.2, 8.3.2.3, 8.4.1.1, 8.17.2, 8.17.2.1. Se Incluyen numerales: 8.3.1.4, 8.3.1.4.1, 8.3.1.4.2, 8.3.1.4.3, 8.3.1.4.4, 8.3.2.4, 8.3.2.4.1, 8.3.2.4.2, 8.3.2.4.3, 8.17.3, 8.17.3.1, 8.17.3.1.1, 8.17.3.2, 8.17.3.2.1, 8.17.3.2.2, 8.17.3.2.3, 8.17.3.3. Se eliminan numerales: 8.3.2.3.1, 8.3.2.3.2, 8.3.2.3.3, 8.17.2.1.1, 8.17.2.2, 8.17.2.2.1, 8.17.2.2.2, 8.17.2.2.3, 8.17.2.3, 8.17.2.3.1, 8.17.2.3.2, 8.17.2.3.3, 8.17 .2.3.4, 8.17.2.3.5, 8.17.2.3.6, 8.17.2.3.7, 8.17.2.3.8	10-may-2018
04	Se realiza actualización del manual en términos del Modelo de Seguridad y Privacidad de la Información MSPI conforme a la política de seguridad de la Información del Modelo Integrado de Planeación y Gestión.	29-Jun-2021

8. RUTA DE APROBACIÓN

ELABORÓ O ACTUALIZÓ:	REVISIÓN METODOLÓGICA OAP:	APROBÓ:
 FRANCISCO JAVIER BERNAL GARCÍA profesional Especializado 222-04 Dirección Administrativa – Proceso de Sistemas y Seguridad de la Información. Apoyo: RUBÉN ESTEBAN BUITRAGO DAZA Contratista proceso sistemas y seguridad de la información JEFFERSON FARUK CAMPOS RAMÍREZ Contratista proceso sistemas y seguridad de la información	 DIANA CAROLINA ÁVILA PINZÓN Profesional Universitario 219-03 Oficina Asesora de Planeación	 JEFFERSON PINZÓN HERNÁNDEZ Director Administrativo 009-02 Dirección Administrativa