POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Objetivo General

Establecer las políticas que regulan la seguridad y privacidad de la información en la Contraloría Distrital de Medellín y presentar en forma clara y coherente los elementos que la conforman; bajo el liderazgo de la Dirección de Desarrollo Tecnológico.

Objetivos Específicos

. Orientar la implementación del Modelo de Seguridad y Privacidad de la Información en la entidad.
. Crear una cultura de apropiación de la seguridad y privacidad de la información en la Contraloría Distrital de Medellín.
. Gestionar los riesgos de seguridad de la información a fin de mitigar los impactos negativos ante una eventual materialización.
. Proteger los activos de información de la Contraloría Distrital de Medellín.

Alcance y aplicabilidad

Esta política es transversal a todos los procesos y procedimientos institucionales de la Contraloría Distrital de Medellín.

Aplica a todos los usuarios internos y externos de la Entidad (servidores públicos, contratistas, proveedores de bienes, entidades del Estado, entes de control) y otros terceros que desempeñen alguna actividad en las instalaciones de la Contraloría Distrital de Medellín o a nombre de esta.

La presente Política abarca toda la información de la Entidad, con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente.

Responsables

La Alta Dirección es la encargada de asignar y aprobar los recursos humanos y económicos para la implementación del Modelo de Seguridad y Privacidad de la Información.

El responsable de mantener la política de seguridad de la entidad actualizada, a efectos de asegurar su vigencia y nivel de eficacia, es el Director Administrativo de Desarrollo Tecnológico. En cada una de las políticas descritas se indican, además,

otros responsables por cada una de ellas.

Términos y 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, etc.) que tenga valor para la organización.

● **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización. [ISO/IEC 27000:2018]

● **Análisis de riesgos:** proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

● **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

● **Contratista:** Persona natural o jurídica contratada por la SDDE para la adquisición de una obra, bien o servicio, no perteneciente al régimen laboral.

● **Control:** comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

● **Copias de Seguridad:** Es el proceso mediante el cual se realiza la copia de la información existente, con el fin de poder recuperarla y disponerla en caso de que ocurra un fallo que afecte a esta

● **Dato personal:** hace referencia a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

● **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

● **Información:** Es un activo de valor que hace parte de la SDDE, por la cual asume funciones como responsable o encargada de la misma en cumplimiento de los requisitos legales, normativos e institucionales. La información corresponde a todo dato corporativo (tecnológico, administrativo, financiero, contable, entre otros), propio o de Terceros con las cuales dispone de un acuerdo o convenio; y datos personales de las cuales asume un rol como responsable o encargado.

● **Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la

información.

● **Modelo Integrado de Planeación y Gestión- MIPG:** el Sistema de Gestión que deben aplicar las entidades públicas de la Rama ejecutiva, el cual integra y articula los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad con el Sistema de Control Interno.

● **Plan de continuidad del negocio:** plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

Marco Normativo.

La Contraloría Distrital de Medellín por ser una entidad de Control del nivel territorial, debe cumplir con la regulación y la normativa que establece el Estado Colombiano en materia de:

● **Ley 1273 del 05 de enero de 2009.** "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado: de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"

● **Ley Estatutaria 1581 del 17 octubre de 2012,** "Por la cual se dictan disposiciones generales para la protección de datos personales"

● **NTC/ISO 27001:2013.** Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

● **Ley 1712 del 06 de marzo de 2014,** "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

● **Ley 1915 del 12 de julio de 2018,** "Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos".

● **Decreto 1074 del 26 de mayo de 2015.** "Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo". Reglamenta parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

● **Decreto 1078 del 26 de mayo de 2015.** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"

● **Decreto 1083 del 26 de mayo de 2015** sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, ("11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital)

● **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.

● **CONPES 3854 de 2016.** Política de Seguridad Digital del Estado Colombiano.

● **Decreto 612 de 4 de abril de 2018.** "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado."

● **Decreto 1008 del 14 de junio 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. "

● **Guía para la administración de los riesgos** de gestión, corrupción y seguridad digital del Departamento Administrativo para la Función Pública - DAFP

● **Resolución 004 del 28 de noviembre de 2017** "Por la cual se modifica la Resolución 305 de 2008 de la Comisión Distrital de Sistemas"

● **CONPES 3995 del 1 de julio de 2020.** Política Nacional de Confianza y Seguridad Digital.

● **Resolución 1519 de 2020:** "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos

● **Resolución 500 de 2021** "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

● **Decreto 454 del 21 de marzo de 2020.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, con la incorporación de la política de gestión de la información estadística a las políticas de gestión y desempeño institucional.

● **Directiva Presidencia 03 de 15 de marzo de 2021:** Lineamientos para el Uso de Servicios en la Nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.

● **Decreto 767 de 2022**"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

Principios de la Política de Seguridad y Privacidad de la Información

La Contraloría Distrital de Medellín para el cumplimiento de su misión, visión y Plan Estratégico institucional, apegados a sus valores institucionales, establece los siguientes principios de seguridad de la información:

. Definir, implementar, operar y mejorar de forma continua y cíclica la protección de la información en el SGSI, soportada en lineamientos o políticas claras acordes a las necesidades de la Contraloría Distrital y los requerimientos normativos.

. Establecer las responsabilidades de la protección de la información, las cuales son aceptadas y publicadas por y para todas las partes interesadas.

. Proteger la información generada, administrada, procesada o custodiada por los procesos, su infraestructura y los controles de acceso.

. Proteger la información creada, procesada, transmitida o en custodia con el fin de minimizar los impactos de la materialización de los riesgos que afectan los principios de seguridad y privacidad de la información.

. Sensibilizar al personal de la Contraloría Distrital, partes interesadas, con el propósito de prevenir ataques provenientes de amenazas externas y/o internas.

. Establecer y socializar los lineamientos necesarios para proteger las instalaciones de procesamiento electrónico de datos y de infraestructura tecnológica que soporte la información crítica de la Contraloría Distrital.

. Garantizar la seguridad y privacidad de la información en la operación de los recursos tecnológicos y las redes de telecomunicación.

. Definir e implementar controles de acceso a la información para los sistemas de información y recursos de red.

. Garantiza la inclusión de la seguridad de la información en el ciclo de vida del desarrollo de los sistemas de información.

. Garantizar la adecuada gestión de los eventos de seguridad y privacidad de la información y su socialización a los organismos de vigilancia y control.

. Garantizar la disponibilidad de sus procesos y la continuidad de su operación

basada en el impacto que pueda generar.

. Fomentar el cumplimiento de las obligaciones legales y los requisitos regulatorios y contractuales que se establezcan en el marco de la protección de la información.

Lineamientos de la política de seguridad y privacidad de la información

La presente política se desarrolla en 12 lineamientos para el cumplimiento de los objetivos planteados, los cuales se describen a continuación:

1. Política de Seguridad y organización de la Información

. La Contraloría Distrital de Medellín, reconociendo la importancia de la información como unos de sus activos más valiosos, se compromete con la implementación de políticas de seguridad y privacidad de la información, estableciendo un marco de confianza digital, en el ejercicio de sus deberes con el Estado y los Ciudadanos.

. Para la Entidad, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

2. Política de Seguridad de los Recursos Humanos

. Cuándo utilicen los recursos informáticos tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica. La información generada por el servidor público debe ser institucional y no de uso personal.

. El área que realice la contratación de personal en la entidad debe realizar las verificaciones de los antecedentes de los candidatos al cargo, la formación académica experiencia y demás información que se requiera de acuerdo a las Leyes, reglamentos de la Entidad y ética pertinentes.

. Todos los empleados, los contratistas y los terceros que desempeñen funciones en la entidad, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como su estación de trabajo.

. La Entidad debe establecer directrices para asegurar que los servidores y

contratistas tengan conocimiento sobre los derechos, deberes, responsabilidades en relación a la seguridad de la información.

. La Entidad debe incorporar los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los colaboradores y terceros.

3. Política General de Seguridad Gestión de Activos

La Entidad establece los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismo acorde para el control de riesgos de información.

. Cada activo de información de la Entidad 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 un valor de confidencialidad, integridad, disponibilidad riesgos identificados y/o requerimientos legales de retención.

. Es responsabilidad del Líder de Proceso, Contralores Auxiliares, Jefe de Área o Director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.

. Los servidores y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Entidad.

. Todos los activos de información deben contar con un responsable que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.

4. Política 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 Entidad. Por tanto, se establecen y mantienen controles para resguardar la seguridad de las instalaciones y ambientes de trabajo el acceso de las tareas.

. Los equipos de cómputo que pasen a un estado de retiro o se requieren para la reutilización deberán cumplir los siguientes lineamientos: a) al momento de retirar un equipo en la organización (almacén) el proceso de TI realiza una copia de respaldo de la información almacenada en este activo. b) el proceso de TI realiza el proceso de borrado seguro de la información almacenada en los equipos que van a

ser cedidos o reutilizados en la organización.

. Para los usuarios de las aplicaciones y sistemas de información de la Entidad debe ser obligatorio que las sesiones sean cerradas al finalizar las actividades y no se debe dejar abiertas o desentendidas.

. Las áreas dentro de las cuales se encuentra el Centro de Datos, Centro de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismo de protección física y ambiental y controles de acceso adecuados para la protección de la información.

5. Política control de Acceso

. La entidad debe definir los lineamientos para asegurar un acceso físico o lógico a la información y plataforma tecnológica considerándolas importantes para el sistema de gestión de seguridad de información.

. La Entidad debe establecer procedimientos la creación de datos de acceso suministro de acceso a la información revisión perdida de los accesos otorgados, y desactivación o eliminación de las cuentas de usuarios una vez finalizada la relación contractual.

. 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 identificación de usuario y contraseña y será responsables de las acciones realizadas por el usuario que le ha sido asignado.

. Las claves son de uso personal e intransferible, y es responsabilidad del usuario el uso de las credenciales asignadas.

. Se debe realizar 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.

6. Políticas Seguras en las Operaciones

. La entidad debe documentar los procesos operacionales a nivel de TI, para reducir riesgos asociados con ausencia de personal y afectaciones en la infraestructura tecnológica.

. La entidad debe garantizar que las operaciones tecnológicas se gesten de forma correcta y se brinde seguridad a las instalaciones de procesamiento de información.

. Según la clasificación de la información establecida por la entidad se debe

establecer medidas de respaldo de la información, a través de dispositivos de almacenamientos NAS y en la nube.

. Los responsables de TI deben definir 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.

7. Política Seguridad de las Comunicaciones

. El proceso de TI debe realizar el bloqueo a las páginas de contenido para adulto, mensajería instantánea y demás página que no sean de uso institucional, mediante el uso de periférico de seguridad firewall, software de protección antivirus y el control que mejor se ajuste a la necesidad.

. La Entidad debe asegurar la protección de las redes y la transferencia de información. Para dar cumplimiento se deben firmar acuerdos de confidencialidad y de no divulgación entre la Entidad y entidades externas con las cuales se intercambie información e implementar controles de seguridad al monitoreo de red.

8. Políticas Adquisición y Mantenimiento de Sistemas

. La entidad debe buscar que la Seguridad de la Información sea parte integral cuando hay adquisición de Software que presten servicio con revisión técnica y de seguridad de las aplicaciones, para detectar vulnerabilidades antes de salir a producción y la aplicación del procesamiento gestión de cambios.

. La entidad debe asegurar que se diseñe e implemente los requerimientos de seguridad en el software, que sea adquirido, que incluya control de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas.

. La entidad debe establecer 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 forma local.

9. Políticas de Relaciones con los Proveedores

. Para los proveedores críticos de tecnología, así como de procesos misionales, la entidad debe exigir 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 entidad.

. La entidad debe controlar las relaciones con proveedores y en particular aquellos que tienen acceso a la información. La información está 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 criticó de TI o de los procesos misionales, deben aplicarse mediante el procedimiento de gestión de cambio establecido en la entidad.

. La entidad debe realizar revisiones periódicas al cumplimiento de las políticas de Seguridad y Privacidad de la Información a los proveedores.

10. Políticas de Gestión de incidentes de Seguridad

. Todos los servidores y contratistas deben conocer el método de reporte de eventos e incidentes de Seguridad de Información.

. La entidad debe asegurar que todos los servidores 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 revise el debido proceso.

. La entidad debe establecer y ejecutar los procedimientos para identificar, valorar y dar un tratamiento adecuado a los incidentes, hacer una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.

. La entidad debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurra en un futuro.

. La Dirección de Desarrollo Tecnológico debe contar con una bitácora de los incidentes de Seguridad de la información reportados y atendidos.

11. Políticas de Controles Criptográficos

La entidad debe asegurar 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 cifradas como son: cifrado de la información cuando se requiere transferir o almacenar información sensible o critica, uso de

protocolos seguros para las redes Wifi, uso de protocolo HTTPS con un nivel de cifrado actualizado.

. Acceso remoto a la red y los sistemas de información de la entidad desde una red externa, debe ser a través de conexiones seguras.

. Factor de doble autenticación para conexiones externas y correo electrónico

. Se debe contar con buenas prácticas para la gestión de llaves.

12. Política de Cumplimiento

. La entidad debe gestionar la Seguridad de la Información, de tal manera 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, los tiempos de retención de registros y los delitos informáticos. (Actualización del normograma)

. La entidad debe asegurar 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 Entidad. Debe determinar las responsabilidades para gestionar la protección de datos personales.

Vigencia

La Política de Seguridad y Privacidad de la Información, de la Contraloría Distrital de Medellín, será revisada anualmente o antes, si existiesen modificaciones que así lo requieran.