2021

Manual

DIR-M-2

Manual de políticas de seguridad y privacidad de la información

Pertenece al proceso
"Direccionamiento Estratégico"

Instituto Caro y Cuervo
Grupo de Planeación
20/05/2021

INFORMACIÓN DEL DOCUMENTO

Versión	Fecha de aprobación	Elaborado por:	Revisado por:	Aprobado por:	Descripción del Cambio
1.0	20/05/2021	Heilin Guarnizo Rodríguez Contratista-oficial de seguridad de la información	Cristian Velandia Coordinador del grupo de Planeación	Comité Institucional de Gestión y Desempeño	Inclusión de la política denominada "5.2.1 gestión de proyectos" Se actualiza la política 5.3.3 terminación y cambio del empleo Se actualiza la política 5.10.2.1 correo electrónico Se articula lo desarrollado en las versiones del documento denominado: ORG-M-04 MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

INTRODUCCIÓN

Las políticas de seguridad y privacidad de la información tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar el adecuado uso de los activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información.

El presente manual se encuentra estructurado con la política general de seguridad de la información y políticas específicas que soportan el Sistema de Gestión de Seguridad de la Información – SGSI las cuales deben ser conocidas y aceptadas por todos los usuarios que tengan acceso a los servicios tecnológicos y a los activos de información de la Entidad.

1. OBJETIVO

Establecer los lineamientos para proteger los activos de información y los datos personales teniendo en cuenta los requisitos legales y la norma ISO 27001:2013, con el fin de asegurar el cumplimiento de los principios de privacidad, integridad, disponibilidad y confidencialidad de la información.

1.1. OBJETIVOS ESPECÍFICOS

- ✓ Implementar el sistema de gestión de seguridad y privacidad de la información soportado en políticas y procedimientos.
- ✓ Definir los roles y responsabilidades que el Instituto Caro y Cuervo requiere para apoyar el desarrollo de los lineamientos del SGSI y que permita el cumplimiento de las políticas de este.
- ✓ Informar a los usuarios de los servicios tecnológicos sobre normas y mecanismos que deben cumplir y utilizar para proteger el hardware, software, canal de comunicaciones, recursos TIC institucionales, así como la información que es procesada, almacenada y transmitida en estos.
- ✓ Comprometer a todo el personal de la entidad, mediante charlas de concientización, que se darán a través del plan de sensibilización del SGSI y como parte integral de la charla de inducción para nuevos perfiles sin importar el tipo de vinculación (funcionarios, contratistas, practicantes, entre otros).
- ✓ Proporcionar las pautas para la protección, tratamiento y uso de los datos personales y sensibles que reposen en las bases de datos y archivos del Instituto.
- ✓ Establecer criterios para la obtención, recolección, uso, tratamiento, procesamiento, intercambio, transferencia y transmisión de datos personales.

2. ALCANCE

Las políticas de seguridad y privacidad son aplicables a todos los funcionarios, contratistas, docentes, estudiantes, consultores eventuales y otros empleados de la entidad, que tengan acceso a la información del Instituto Caro y Cuervo de manera local o remota a los de equipos de cómputo, infraestructura tecnológica, canales de comunicación de la entidad, bases de datos, sistemas de Información y documentos físicos.

3. TÉRMINOS Y DEFINICIONES

Acción correctiva: Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva: medida de tipo proactivo dirigida a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.

Activo: Cualquier elemento que tenga valor para la organización y el contexto de seguridad digital. Son activos, los elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información –TI–, tecnologías de operación –TO–.

Acuerdo de confidencialidad: Documento en el que funcionarios, contratistas y/o terceras partes de la entidad manifiestan su voluntad de mantener la confidencialidad de la información del Instituto Caro y Cuervo, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso, en virtud de la labor que desarrollan.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Bases de datos personales: Conjunto organizado de datos personales que sea objeto de tratamiento.

Controles: Políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. También se utiliza como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Comité institucional de gestión y desempeño: Instancia orientadora del Modelo Integrado de Planeación y Gestión –MIPG–, el cual integra las políticas de gobierno y seguridad digital, por lo que se establece entre sus funciones asegurar la implementación y desarrollo de políticas de gestión en materia de seguridad digital y de la información.

Confidencialidad: Propiedad o característica consistente en que la información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Datos personales sensibles: Aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información –SGSI– de la organización, tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Disponibilidad: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

Encargado del tratamiento de datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del tratamiento.

Evento de seguridad de la información: Presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles o una situación previamente desconocida que puede ser pertinente para la seguridad.

Gestión documental: Conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación.

Gestión de incidentes: Conjunto de acciones y procesos tendientes a brindar a las organizaciones fortalezas y capacidades para responder en forma adecuada a la ocurrencia de incidentes de seguridad informática que afecten real o potencialmente sus servicios.

Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar a seguridad de la información.

Información pública: Toda información que un sujeto obligado genere obtenga, adquiera o controle en su calidad de tal, que ha sido declarada legalmente o por su propietario de conocimiento público y accesible a cualquier persona. Ejemplo: rendición de cuentas.

Información pública clasificada: Información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

Información pública reservada: Información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

No conformidad: Ausencia o fallo de uno o varios requerimientos de la norma ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible o representa un riesgo inaceptable.

No repudio: El emisor no podrá negar el conocimiento de un mensaje de datos ni los compromisos adquiridos a partir de éste.

Plan de continuidad: Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Política: Toda intención y directriz expresada formalmente por la Dirección.

Privacidad: Derecho que tienen todos los titulares de la información, en relación con aquella que involucre datos personales y la clasificada que estos hayan entregado o esté en poder de la entidad, en el marco de las funciones que a ella le compete realizar y que generan en las entidades la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad demostrada: Conducta desplegada por los responsables o encargados del tratamiento de datos personales bajo la cual, a petición de la Superintendencia de Industria y Comercio, deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del tratamiento de datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Sistema de Gestión de Seguridad de la Información –SGSI–: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información, para alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

Titulares de la información: Personas naturales cuyos datos personales sean objeto de tratamiento.

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas, de modo inequívoco, a un individuo o entidad.

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

4. DESCRIPCIÓN

En el presente manual se estructuran y actualizan las políticas del sistema de gestión de seguridad de la información – SGSI en el Instituto Caro y Cuervo, relacionándolas con los controles del Anexo A de la NTC-ISO-27001:2013, incluyendo los objetivos de control, lo anterior en aras de dar cumplimiento a las políticas de gobierno y seguridad digital del modelo integrado de planeación y gestión MIPG.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1. POLÍTICA GENERAL

Objetivo: Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

Dirigida a: Todos

En la presente Política de seguridad y privacidad de la información la Dirección General del Instituto Caro y Cuervo declara su posición y compromiso respecto al cumplimiento de los requisitos aplicables relacionados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de sus activos de información (funcionarios, contratistas, terceros, información, procesos, servicios,

tecnologías de información incluido el hardware y el software), que soportan los procesos de la entidad y apoyan la definición, implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información –SGSI–, por medio de la generación y publicación de sus políticas, procedimientos, guías, manuales e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información en el marco de la norma NTC ISO/IEC 27001.

Para asegurar la dirección estratégica el Instituto Caro y Cuervo establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

1. Minimizar el riesgo de los procesos misionales de la entidad.
2. Cumplir con los principios de seguridad de la información.
3. Definir roles y responsabilidades con el fin de crear compromisos en la protección de la información.
4. Identificar e implementar la tecnología necesaria para fortalecer la seguridad de la información.
5. Implementar el sistema de gestión de seguridad de la información.
6. Proteger los activos de información, con base en los criterios de confidencialidad, integridad y disponibilidad.
7. Proteger la privacidad de los datos personales de los funcionarios, contratistas y terceros administrados y recolectados por el Instituto Caro y Cuervo.
8. Fortalecer la cultura de seguridad y privacidad de la información en los funcionarios, contratistas y terceros del Instituto Caro y Cuervo.
9. Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, funcionarios, contratistas y terceros, que tengan acceso a los activos de información.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deben dar cumplimiento del 100% de la política.

Se establecen los diez (10) principios de seguridad que soportan el SGSI del Instituto Caro y Cuervo:

1. El Instituto Caro y Cuervo decide definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, con base en lineamientos claros, alineados a las necesidades de la entidad y a los requerimientos regulatorios que le aplican a su naturaleza.

2. El Instituto Caro y Cuervo define, comparte y publica los roles y responsabilidades frente a la seguridad y privacidad de la información, aplicables a funcionarios, contratistas o terceros.
3. El Instituto Caro y Cuervo identifica, califica y valora sus activos, como base para analizar los riesgos, vulnerabilidad y amenazas a los que están expuestos y así seleccionar e implementar los controles necesarios para reducir los riesgos a un nivel aceptable.
4. El Instituto Caro y Cuervo protege la información generada, administrada o custodiada por los procesos de la entidad y activos de información, con el fin de minimizar impactos financieros, operativos o legales, mediante la aplicación de controles, de acuerdo con la calificación de la información de su propiedad o en custodia.
5. El Instituto Caro y Cuervo protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. El Instituto Caro y Cuervo implementa controles de acceso a la información, sistemas y recursos de red.
7. El Instituto Caro y Cuervo exige que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
8. El Instituto Caro y Cuervo gestiona los incidentes de seguridad y realiza procesos de auditoría interna que permitan una mejora continua del SGSI.
9. El Instituto Caro y Cuervo garantiza la disponibilidad de sus procesos de negocio y la continuidad de su operación, con base en el impacto que pueden generar los incidentes.
10. El Instituto Caro y Cuervo garantiza el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

La Dirección General se compromete a proporcionar los medios necesarios para la consecución de los objetivos de seguridad establecidos y asume la responsabilidad de motivar y formar en el conocimiento y cumplimiento de esta Política.

El incumplimiento a la Política de seguridad y privacidad de la información traerá consigo las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

Esta política se revisa anualmente o cuando se identifiquen cambios en la entidad, su estructura, sus objetivos o alguna condición que afecte la Política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

5.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.

Dirigida a: Grupo de planeación y Dirección General

El Instituto Caro y Cuervo establecerá los roles y responsabilidades que involucran la administración y operación del SGSI para funcionarios y terceros en el manual del sistema de gestión de seguridad de la información y las correspondientes a la alta dirección se encuentran en el acto administrativo por el cual se crea y conforma el Comité Institucional de Gestión y Desempeño.

5.2.1. Gestión de proyectos

Dirigida a: Todos, grupo de las TIC

Todas las adquisiciones y proyectos que tengan cualquier componente tecnológico tal como licenciamiento, software, sistemas de información, dispositivos de red, computadores, impresoras, escáner, entre otros deben contar con la revisión y aprobación del grupo de las TIC con el objetivo de garantizar la prestación y soporte de los servicios digitales dentro de los acuerdos de niveles de servicio de esta dependencia, es por esto que debe involucrarse al grupo de las TIC desde la fase de planeación del proyecto.

5.2.2. Dispositivos móviles

Objetivo: Garantizar la seguridad del uso de dispositivos móviles.

Dirigida a: Todos, Grupo de las TIC

Para los funcionarios y contratistas a quienes el Instituto Caro y Cuervo les asigna dispositivos móviles institucionales (portátiles, tabletas, celulares) para el desempeño de sus labores, deben obedecer las siguientes directrices:

- El grupo de las TIC tiene como función exclusiva el mantenimiento y la instalación de software en los computadores, que son propiedad del Instituto Caro y Cuervo; ellos son los únicos usuarios con credenciales de acceso para realizar este tipo de actividades.

- En los dispositivos móviles no se permite guardar información personal, música u otro tipo de información que no se encuentre relacionada con las funciones por las cuales fue contratado en la Entidad.
- Los requerimientos tales como la instalación de un software adicional, configuraciones y/o soporte técnico se deben solicitar a través de la mesa de ayuda dispuesta por el grupo de las TIC.
- El préstamo de computadores portátiles se debe tramitar a través de la mesa de ayuda con anticipación y se proveerá según disponibilidad.
- En caso de pérdida o robo de dispositivos móviles propiedad del Instituto Caro y Cuervo, se debe reportar a través de correo electrónico al coordinador del grupo de recursos físicos y a las autoridades pertinentes.
- Los dispositivos móviles deben contar con un software antivirus instalado y actualizado.
- El grupo de las TIC debe configurar únicamente perfiles institucionales, es decir, el ingreso a estos equipos debe realizarse mediante usuario y contraseña.

Lineamientos para dispositivos móviles personales y que se conectan a los servicios tecnológicos de la Entidad: Los dispositivos móviles que no sean propiedad del Instituto Caro y Cuervo tales como computadoras portátiles, celulares, tabletas, entre otros. Pueden conectarse a la red pública dispuesta por la Entidad y deben obedecer las siguientes directrices:

- Los dispositivos móviles personales como (portátiles, tabletas, IPad, cámaras y PDA) deben ser registrados en las porterías de la Entidad con el objetivo de poder realizar su retiro sin requerir autorización del grupo de las TIC.
- Se debe solicitar autorización al grupo de las TIC para conectarse a la red cableada o a la red inalámbrica corporativa.
- El dispositivo móvil debe tener instalado un software antivirus el cual debe encontrarse activo y actualizado, así como el cortafuegos habilitado.
- El ingreso a dicho dispositivo móvil debe realizarse a través de usuario y contraseña o huella dactilar.
- No debe tener instalado software de escaneo de redes u otros programas objetables.
- El grupo de las TIC no prestará servicio de soporte técnico (revisión, mantenimiento, trámite de garantías y/o reparación de hardware) a equipos que no sean propiedad del Instituto Caro y Cuervo.
- El Instituto Caro y Cuervo no se hará responsable, en caso de pérdida o daño, de algún equipo informático de uso personal que haya sido ingresado a sus diferentes instalaciones.
- En caso de robo o pérdida del dispositivo móvil personal el usuario está obligado a cambiar inmediatamente las contraseñas de acceso a los sistemas de información y aplicaciones de

la Entidad, esto en aras de proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.

- No se permite el uso de dispositivos móviles personales en las dependencias donde se administra o custodia información reservada, el coordinador, jefe o subdirector es el responsable de hacer el respectivo seguimiento.

5.3. SEGURIDAD TALENTO HUMANO

5.3.1. Antes de asumir el empleo

Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

Dirigida a: Grupo de talento humano y Grupo de gestión contractual

El grupo de talento humano para el caso de los funcionarios y el grupo de gestión contractual para el caso de los contratistas, deben llevar a cabo una verificación de los antecedentes de todos los candidatos a un empleo de acuerdo con la normatividad vigente.

Los acuerdos contractuales con funcionarios y contratistas deben establecer sus responsabilidades y las del Instituto en cuanto a seguridad de la información.

Se debe asegurar que todos los funcionarios y terceros a los que se brinde información clasificada y/o reservada deben firmar un acuerdo de confidencialidad y no divulgación antes de obtener accesos a esta.

Se debe establecer las responsabilidades y derechos legales de los colaboradores con relación a leyes sobre derechos de autor o legislación sobre protección de datos.

5.3.2. Antes de asumir el empleo

Objetivo: Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

Dirigida a: Grupo de talento humano, Grupo de gestión contractual, Grupo de planeación, Subdirección administrativa y financiera, Líder del proceso disciplinario, Unidad de control interno, supervisores de contrato.

El grupo de Talento Humano, desde su plan de capacitaciones e inducción debe asegurar que los funcionarios y contratistas del Instituto Caro y Cuervo comprendan sus responsabilidades en relación con las políticas de seguridad de la información de la entidad y actúen de manera consistente frente a las mismas, para reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de esta.

El Instituto Caro y Cuervo debe contar con un proceso formal para emprender acciones contra funcionarios o terceros que hayan cometido una violación a la seguridad y privacidad e la información.

Los funcionarios y terceros deben cumplir a cabalidad las políticas y procedimientos de seguridad y privacidad de la información, implementados en el Instituto, entendiendo que cualquier incumplimiento puede conducir a procesos disciplinarios o sanciones de acuerdo con la normatividad vigente.

Es responsabilidad de los funcionarios y terceros proteger los activos que estén bajo su custodia contra acceso, divulgación, modificación, destrucción o interferencia no autorizada, haciendo cumplir las medidas de seguridad implementadas por la Entidad, cabe precisar que los responsables por propender el buen uso de los activos de información por parte de contratistas y terceras partes son los supervisores de contrato.

5.3.3. Terminación y cambio de empleo

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

Dirigida a: Grupo de talento humano, Grupo de gestión contractual, Grupo de las TIC.

El grupo de talento humano y/o de gestión contractual debe reportar al grupo de las TIC las novedades administrativas tales como: el retiro de un funcionario o una terminación o cesión de contrato para el caso de los contratistas para retirar credenciales de acceso a los diferentes sistemas de información, verificar la entrega de la información y supervisar la correcta devolución de los equipos y recursos asignados al usuario de la red.

El grupo de talento humano debe reportar al grupo de las TIC los movimientos internos de personal en la entidad, y así ajustar los nuevos roles, revocar los privilegios de acceso a los sistemas de información y datos sensibles del área a la que perteneció el funcionario.

Se debe comunicar al colaborador, las responsabilidades y deberes de seguridad y privacidad de la información que permanecen válidos después de la terminación o cambio de empleo o de contrato.

El grupo de las TIC debe dar el visto bueno al proceso de paz y salvo después de validar que se han desactivado las cuentas de acceso a los servicios tecnológicos del Instituto y que el jefe inmediato o supervisor ha recibido la copia de respaldo de la información, la paz y salvo debe ser requisito para completar el proceso de desvinculación.

Los usuarios de los servicios tecnológicos que terminen su vínculo contractual con la entidad, se les desactivará inmediatamente sus cuentas de acceso, incluyendo la del correo electrónico. El grupo de las TIC dispondrá de una semana para realizar la copia de respaldo de la información del equipo y del correo en formato .pst, en caso de que la cuenta de acceso no tenga ningún tipo de actividad en un periodo de (5) cinco meses se eliminará dicha cuenta.

Para las cuentas de acceso de los funcionarios una vez recibido el acto administrativo por parte del grupo de talento humano, el grupo de las TIC, deben mantener activos los accesos por un lapso de 15 días hábiles dando cumplimiento a la Ley 951 del 2005 en las condiciones para la entrega del cargo.

5.4. GESTIÓN DE ACTIVOS

5.4.1. Identificación de activos

Objetivo: Identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

Dirigida a: Lideres de proceso, coordinadores de los grupos de trabajo.

Los líderes de proceso son los responsables de identificar y mantener actualizados los activos de información de su respectivo proceso asignando por cada activo un responsable y custodio, conforme al documento establecido para la gestión de activos, los activos deben quedar registrados en el sistema de información dispuesto por el grupo de las TIC.

5.4.1.1. Uso aceptable de los activos

Dirigida a: Todos

Los activos de información pertenecen al Instituto Caro y Cuervo, y el uso de estos debe emplearse exclusivamente con propósitos institucionales.

El grupo de las TIC controla el software y los equipos autorizados que podrán ser utilizados por los usuarios de la red de datos del Instituto Caro y Cuervo para la creación, edición y desarrollo de nuevos activos de información.

El grupo de las TIC es la única dependencia autorizada para realizar la instalación y configuración de hardware y software.

El Instituto Caro y Cuervo proporcionará al usuario los equipos informáticos necesarios para el cumplimiento de sus obligaciones y/o funciones, los datos y la información creados, almacenados y recibidos serán propiedad de Instituto Caro y Cuervo.

Los usuarios de la red de datos institucional son responsables del acceso a redes externas, deben verificar que todos los archivos o material recibido a través de medios electrónicos se encuentran libres de software malintencionado, mediante la ejecución de la herramienta de escaneo en busca de software malintencionado que poseen los antivirus para detectar posibles virus insertados.

Todos los funcionarios y terceros deben hacer buen uso de los activos de información a los cuales tienen acceso y que son propiedad del Instituto Caro y Cuervo, de igual forma son responsables de todas las transacciones o acciones efectuadas con su "cuenta de usuario".

5.4.1.2. Acciones prohibidas sobre el uso de los activos de información

Dirigida a: Todos

A continuación, se mencionan actos de mal uso, sin embargo, estos no se limitan a:

a) La utilización, transmisión o almacenamiento de cualquier archivo físico, digital o electrónico, dato o registro de información que viole la política de confidencialidad o las directrices o políticas en materia de gestión de la información está prohibido.
b) Los servicios tecnológicos no podrán ser utilizados, para divulgar, propagar o almacenar contenido que razonablemente puede considerarse una amenaza, acoso u ofensa para cualquier persona, contenido de tipo personal o comercial de publicidad, promociones, ofertas, prácticas de juegos en línea, programas destructivos (virus), material político/religioso o cualquier otro uso que no esté vinculado con las labores institucionales.
c) No se permite la navegación en internet a sitios de alto riesgo, de contenido: pornográfico, terroristas, racistas, comunidades sociales, o cualquier contenido que represente riesgo para la red de la Entidad.
d) No se permite la manipulación de las impresoras, ni la apertura de los computadores, cualquier reporte para solución de fallas debe ser reportado a la mesa de ayuda al grupo de las TIC.
e) No se permite crear datos falsos o engañosos a través del uso de los servicios tecnológicos de la Entidad.

f) Los usuarios no deben ofrecer acceso a los servicios tecnológicos (ej. Redes LAN o red WIFI) o poner a disposición datos a personas no autorizadas, la única dependencia que puede proveer acceso a los servicios tecnológicos es el grupo de las TIC.
g) No se permite dañar, borrar, deteriorar, alterar, ocultar o suprimir datos.
h) No se permite el uso de peer-to-peer para el intercambio de archivos a fin de obtener ilegalmente material con derechos de autor y la instalación de software que no ha sido aprobado para su uso.
i) Realizar copias no autorizadas de material protegido por derechos de autor propiedad del Instituto Caro y Cuervo que incluye, pero no está limitado a información física, digitalizada o distribución de fotografías, audios o videos.
j) Utilizar programas sin su respectiva licencia obtenidos a partir de otras fuentes puede implicar amenazas legales y de seguridad de la información para la entidad, por lo que esta práctica no está autorizada.
k) Suplantar o facilitar la cuenta de usuario, enviar correos electrónicos a nombre de otro usuario sin autorización o suplantándolo.
l) Redireccionar los correos electrónicos institucionales a cuentas de correo personales.
m) Burlar los mecanismos de seguridad, autenticación, autorización o de auditoria, de cualquier servicio de red, aplicación, servidor o cuenta de usuario.

5.4.1.3. Devolución de los activos

Dirigida a: Todos, supervisores y jefes

Al finalizar su empleo o contrato, los colaboradores deben devolver todos los activos de información que se encuentren a su cargo y que fueron suministrados por el Instituto Caro y Cuervo para el cumplimiento de sus funciones u objeto del contrato.

5.4.2. Calificación de los activos

Objetivo: Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.

Dirigida a: Los líderes de proceso, coordinadores de los grupos de trabajo

Los líderes de proceso deben calificar sus activos de información de acuerdo con el documento para la gestión de activos creado para tal fin y valorados de acuerdo con la confidencialidad, integridad y disponibilidad en aras de procurar que los activos reciben un nivel apropiado de protección de acuerdo

con la importancia para el proceso y la Entidad, la calificación proporcionada a los activos debe quedar registrada en el sistema de información dispuesto por el grupo de las TIC.

5.4.2.1. Etiquetado de la información

Dirigida a: Grupo de gestión documental, Grupo de las TIC, Grupo de planeación

Se debe desarrollar e implementar procedimientos, mecanismos o herramientas para el etiquetado de la información acorde con los niveles de clasificación definidos y adoptados, dichas etiquetas permiten reconocer fácilmente la importancia del activo.

Para los sistemas de información que contienen información sensible o crítica se deben implementar mecanismos que indiquen la calificación e identificación de la información.

La información que se intercambie con otras entidades debe incluir la calificación correspondiente y se debe informar a su destinatario la interpretación de la calificación para que se asignen las protecciones necesarias.

5.4.3. Gestión de medios removibles

Objetivo: Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.

Dirigida a: Todos

Los medios removibles son todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores. Por ejemplo: memorias USB, discos duros externos, entre otros, el uso de estos puede ocasionalmente generar riesgos para la entidad al ser conectados en la red de la Entidad, ya que son susceptibles a la transmisión de virus. Para utilizar medios removibles se debe realizar un escaneo en busca de virus, antes de copiar o consultar información en estos medios.

Es responsabilidad del usuario hacer el cifrado de todo medio removible (incluso los de propiedad personal) en los cuales se almacene y transporte información del Instituto y sea calificada como clasificada o reservada.

En caso de olvido de la contraseña asignada para el cifrado del medio removible y pérdida de la clave de recuperación provista, el usuario responsable de uso del medio removible asumirá las consecuencias producto de la pérdida de la información institucional que se encuentre almacenada en dicho medio.

Los medios removibles no son alternativa de respaldo de información, son de uso temporal; siendo responsabilidad de los usuarios mantener copias de la información en los repositorios institucionales.

5.4.3.1. Disposición de los medios removibles

Dirigida a: Grupo de las TIC

El grupo de las TIC ejecutará el debido proceso para la eliminación de datos en los medios de almacenamiento que vayan a ser reemplazados, efectuando un proceso de borrado seguro y posteriormente la eliminación o destrucción en forma adecuada.

El grupo de las TIC establecerá los lineamientos necesarios para dar de baja el software y los equipos de cómputo que presenten obsolescencia o daño irreparable.

5.4.3.2. Transferencia de medios físicos

Dirigida a: Grupo de gestión documental

Los medios que contienen información (física o digital) se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte, siguiendo los lineamientos establecidos por el grupo de gestión documental que controlan el servicio de envíos y entregas internamente entre la sede Yerbabuena y Casa Caro y Cuervo.

5.5. CONTROL DE ACCESO

5.5.1. Requisitos del Negocio para Control de Acceso.

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información

Dirigida a: Grupo de las TIC, Grupo de recursos físicos, jefes y supervisores

El grupo de las TIC debe implementar procedimientos para la asignación de privilegios de acceso a los sistemas de información, carpetas compartidas, bases de datos y servicios tecnológicos, en cuanto a la definición de procedimientos para mantener el acceso controlado físico a las instalaciones de la Entidad el grupo de recursos físicos es el responsable, estos procedimientos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los jefes y supervisores son los únicos autorizados para solicitar los accesos físicos, la creación de las cuentas de usuario y la asignación de permisos a los diferentes servicios tecnológicos y sistemas de información para los integrantes de su grupo de trabajo, considerando el mínimo de privilegios necesarios para que contratistas y/o funcionarios puedan desempeñar sus obligaciones y/o funciones.

5.5.1.1. Acceso a redes y a servicios en red.

Dirigida a: Todos, Grupo de las TIC

La conexión remota a la red de área local del Instituto Caro y Cuervo debe realizarse a través de una conexión VPN segura suministrada por el grupo de las TIC. El servicio de acceso remoto por VPN permite a los usuarios el acceso a los activos de información disponibles solo desde la red interna desde un sitio remoto a través de internet.

El grupo de las TIC realizará un análisis de los equipos personales que requieran conexión VPN y telefonía VoIP, con el fin de verificar que estos equipos cuentan con las condiciones necesarias de seguridad para conectarse a la red de área local de la entidad a través de operadores externos.

El Instituto Caro y Cuervo debe contar con un dispositivo de seguridad perimetral para la conexión a internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.

Los puntos de conexión de la red datos del Instituto Caro y Cuervo son para uso exclusivo de los equipos propiedad de la entidad, la instalación, activación y gestión de los puntos de red es responsabilidad del grupo de las TIC.

5.5.2. Gestión de acceso de usuarios.

Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.

Dirigida a: Coordinadores, supervisores, Grupo de las TIC, todos.

Los jefes o supervisores de contrato deberán solicitar al Grupo de las TIC a través de la mesa de ayuda, la creación de las cuentas de usuario y la asignación de permisos a los diferentes servicios tecnológicos y sistemas de información para los integrantes de su grupo de trabajo.

Los accesos con privilegios especiales deben contar con la aprobación de la Coordinación del Grupo de las TIC y deben de estar debidamente justificados, los responsables del manejo de usuarios privilegiados deben aceptar su responsabilidad frente al uso del usuario asignado.

Para los usuarios con derechos de uso privilegiado utilizados para la administración de infraestructura, aplicaciones y sistemas de información, la coordinación del grupo de las TIC debe controlarlos mediante un proceso formal de autorización, asignando credenciales diferentes para las actividades regulares, segmentados por cada sistema o proceso, donde se definan los requisitos para la expiración de estos, con especial atención a las cuentas configuradas para usuarios externos con propósitos específicos y por tiempo limitado.

Los usuarios de la red de datos del Instituto Caro y Cuervo contarán con las debidas credenciales de acceso a los equipos, sistemas y/o aplicativos informáticos necesarios para el correcto desempeño de sus actividades.

El grupo de las TIC debe implementar mecanismos para que los usuarios cambien su contraseña de acceso al usarla por primera vez en los sistemas de información o servicios a los que se les permita el acceso.

Los propietarios y custodios deben realizar revisiones periódicas por lo menos una vez en el año a los derechos de acceso de los usuarios en los diferentes sistemas de información, de dominio y de la red.

Los funcionarios y contratistas solo tendrán acceso a los datos y recursos autorizados por el Instituto Caro y Cuervo, y serán responsables disciplinaria y legalmente por la divulgación no autorizada de información que se clasifique como reservada o clasificada.

5.5.3. Responsabilidades de los usuarios.

Objetivo: Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.

Dirigida a: Todos

Todos los funcionarios y terceros deben mantener la confidencialidad de la información y cumplir con las políticas de seguridad de la información para el uso de información secreta para la autenticación (cuentas de acceso), asegurándose que no sea divulgada o compartida con otros colaboradores o personal externo. Además, se debe dar cumplimiento a lo siguiente:

- Evitar escribir la información secreta (usuarios, contraseñas, etc.) en papeles o archivos electrónicos o almacenarla en los navegadores de internet.
- Todo usuario autorizado debe cambiar las contraseñas cada vez que exista o haya algún indicio de una posible vulnerabilidad del sistema.
- Las claves o contraseñas de acceso a los sistemas de información deben poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
- Evitar usar las mismas contraseñas para fines personales y laborales.
- La información calificada como clasificada y/o reservada del Instituto, no debe estar disponible para consulta en los sistemas públicos del Instituto o ser accedida por medio de buscadores desde internet.

5.5.4. Control de acceso a sistemas y aplicaciones.

Objetivo: Prevenir el uso no autorizado de sistemas y aplicaciones

Dirigida a: Todos, Grupo de las TIC

Cada usuario es responsable de la cuenta de usuario y clave que le ha sido asignada necesaria para acceder a la información, servicios tecnológicos y/o sistemas de información de la Entidad. Los usuarios y claves son personales e intransferibles y no deben prestarse, divulgarse, ni permitir que otros utilicen sus cuentas de usuario, ni utilizar las cuentas de usuario de otros usuarios.

Los usuarios deben terminar las sesiones activas cuando finalice su actividad o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.

El grupo de las TIC debe restringir y controlar el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones, siguiendo las siguientes directrices mínimas:

- Usar procedimientos documentados de identificación, autenticación y autorización de los programas utilitarios.
- Limitar el uso de programas utilitarios al número mínimo de usuarios confiables y autorizados, teniendo en cuenta el tiempo de uso previsto.
- Retirar o inhabilitar todos los programas innecesarios.

El grupo de las TIC debe controlar el acceso a códigos fuente de programas y elementos asociados (diseños, especificaciones, planes de prueba, resultados), para evitar la introducción de funcionalidades no autorizadas o cambios involuntarios, así mismo, para mantener la confidencialidad de la propiedad intelectual.

- Las librerías de programas fuente, no deberían estar contenidas en los ambientes de producción.
- Se debe documentar y hacer cumplir los procedimientos establecidos para la gestión de códigos fuente y las librerías de los programas.
- Mantener un registro de auditoría de todos los accesos a la librería de fuentes de programas.
- Se debe llevar un control de cambios adecuado para el mantenimiento y copia de las librerías de fuentes de programas.

5.5.4.1. Control de acceso a sistemas y aplicaciones externas

Dirigida a: Todos, Grupo de las TIC

Los líderes de proceso, coordinadores y/o subdirectores deben notificar al grupo de las TIC y registrar en el aplicativo de activos de información, los accesos a sistemas, aplicativos y servicios tecnológicos externos a los cuales se encuentra inscrito el Instituto, ejemplo (SIRECI, CHIP, COLEXCOL, SNIES, SIIF, SCIENTI, entre otros), en el reporte se debe entregar la información de cuáles son las cuentas de correo electrónico que se encuentran inscritas para el acceso y reporte a dichas plataformas, fecha de inscripción, fecha de caducidad, así mismo se debe indicar siempre una cuenta de correo electrónico alterna que funcione como respaldo en caso de alguna novedad con la cuenta principal.

5.5.4.2. Gestión de contraseñas.

Dirigida a: Todos, Grupo de las TIC

Es responsabilidad de funcionarios y terceros utilizar contraseñas fuertes para realizar la autenticación y acceso a la información, las aplicaciones y/o los sistemas de información de la Entidad.

El cambio de contraseña para inicio de sesión en cualquier sistema de información de la entidad solo podrá ser solicitado por el titular de la cuenta.

La contraseña de la cuenta de usuario asignada por primera vez debe ser inmediatamente cambiada en el primer inicio de sesión, cumpliendo con los siguientes requisitos:

- Las contraseñas deben estar compuestas al menos por ocho caracteres alfanuméricos.
- Contener caracteres de las tres siguientes clases de caracteres:
  - ✓ Caracteres en mayúsculas y minúsculas (es decir, Aa-Zz)
  - ✓ Base de 10 dígitos (es decir, 0-9)
  - ✓ Puntuación y otros caracteres (es decir, @#$%^&*() _+|~-= \ `{}[]:";'<>?,./).
  - ✓ No pueden tener caracteres consecutivos (ABCD, 12345)

Las contraseñas se deben cambiar obligatoriamente cada treinta días, o cuando lo establezca el sistema de información.

Las contraseñas no deben ser reveladas a ninguna persona, incluyendo al personal del grupo de las TIC, y no deben ser registradas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y que el método de almacenamiento esté aprobado por el grupo de las TIC.

Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro, utilizando herramientas que permitan la protección de dichas claves. A esta herramienta solo debe tener acceso líder de la oficina de las TIC y el asesor de apoyo.

Las cuentas de usuario y contraseña de administradores son de uso personal e intransferible. El personal del grupo de las TIC debe emplear obligatoriamente contraseñas con un alto nivel de complejidad de acuerdo con el rol asignado.

5.6. CRIPTOGRAFIA

5.6.1. Controles criptográficos

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.

Dirigida a: El grupo de las TIC

El grupo de las TIC debe definir e implementar lineamientos para la aplicación de controles criptográficos para la protección de la información y contar con un método seguro de gestión de llaves criptográficas.

El grupo de las TIC debe implementar técnicas de cifrado para la transferencia de información etiquetada como clasificada y/o reservada fuera del Instituto con el propósito de proteger su confidencialidad e integridad.

Los desarrolladores internos y externos deben asegurarse de que los controles criptográficos, de los sistemas de información desarrollados para el Instituto, cumplen con los lineamientos establecidos por el grupo de las TIC.

5.7. SEGURIDAD FÍSICA Y DEL ENTORNO

5.7.1. Áreas seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización

Dirigida a: Grupo de recursos físicos

El grupo de recursos físicos debe establecer y comunicar los protocolos de seguridad física para el acceso a las instalaciones del Instituto.

El grupo de recursos físicos debe definir perímetros de seguridad y usarlos para proteger áreas que contengan activos de información críticos (ejemplo: museos, biblioteca, imprenta, archivo central) e instalaciones de manejo de información (centro de datos), teniendo en cuenta lo siguiente:

- El techo, las paredes y los pisos deber ser de construcción sólida.

- Todas las puertas externas deberían tener mecanismos de control que eviten el acceso no autorizado.
- Las puertas y ventanas se deben mantener cerradas con llave cuando no hay supervisión.
- Para las ventanas se debe considerar protección contra acceso.
- Se debe contar con un área de recepción con vigilancia para controlar el acceso físico a las instalaciones, restringiendo el acceso únicamente para el personal autorizado.
- Se deben instalar sistemas para la detección de intrusos.
- Deben contar con mecanismos que permitan cumplir con los requerimientos ambientales de temperatura y humedad.

El grupo de recursos físicos debe establecer un protocolo de seguridad para apoyar al proceso de gestión de museos en las funciones de exhibición, difusión, custodia, conservación y administración de los bienes patrimoniales y valores que se encuentra en los depósitos de museos.

Se debe contar con un registro de acceso a las áreas seguras con fecha, hora de entrada, hora de salida, nombre y firma de la persona autorizada.

Cuando sea viable, las áreas restringidas no tener indicaciones sobre su propósito, sin señales que identifiquen las actividades de procesamiento de información o de la documentación que custodia.

No está permitida la toma de fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de la entidad, a menos que esté autorizado por escrito por el jefe de la dependencia restringida.

En las áreas que contengan activos de información críticos se debe indicar la prohibición de acceso no autorizado, no está permitido fumar, comer o beber dentro o cerca de estos.

Las áreas de despacho y carga de materiales se deben administrar de forma que el personal de despacho no tenga acceso a áreas de procesamiento de información, los materiales que ingresen se deben inspeccionar, para verificar la presencia de materiales peligrosos, todos los materiales que ingresen deben ser registrados de acuerdo con los procedimientos establecidos del grupo de recursos físicos.

Todos los funcionarios y terceros deben portar en un lugar visible el carné que los identifica como funcionarios o contratistas de la Entidad para el acceso a la Entidad y utilizarlos mientras se encuentren dentro de ella.

Todos los visitantes que ingresen al Instituto deben ser registrados y deben portar una tarjeta que los identifique como visitantes en un lugar visible. Debe notificarse inmediatamente al personal de seguridad si se encuentran visitantes sin identificación visible.

Toda persona que tenga acceso a las instalaciones del Instituto deberá registrar al momento de su entrada, el equipo de cómputo, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción el cual podrá retirar el mismo día firmando la salida del equipo.

5.7.1.1. Política de los centros de procesamiento de datos.

Dirigida a: Grupo de las TIC

El acceso a los centros de datos es permitido solo a personal autorizado. El grupo de las TIC debe garantizar que las puertas de acceso estén protegidas por un sistema de control de acceso o por un sistema que permita el ingreso solo a personal que pertenece al grupo de las TIC o personal autorizado por la coordinación del grupo de las TIC.

Los centros de datos deben ser limpiados al menos una vez por semana para disminuir al máximo los niveles de polvo y de contaminación. Esta actividad debe ser supervisada por un funcionario del grupo de las TIC, quien debe instruir al personal de limpieza respecto a los cuidados y precauciones mínimos a seguir durante esta actividad.

Los centros de datos deberán contar con un equipo de aire acondicionado que mantenga una temperatura no mayor a 21 grados centígrados, y con unidades de potencia ininterrumpida UPS, que proporcionen respaldo a los mismos, y garantizar el servicio de energía eléctrica durante una falla temporal del fluido eléctrico de la red pública y permitir el intercambio automático del sistema de energía redundante.

Los centros de datos deberán contar con un entorno físico que se rija a los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos en los equipos de telecomunicaciones y servidores. Deberán contar con un extintor especial para equipos de cómputo y con pisos elaborados en materiales no inflamables.

Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual para determinar la efectividad del sistema.

El mantenimiento de los equipos de potencia ininterrumpida UPS estará a cargo del grupo de las TIC y deberá incluirse en un su plan de adquisición anual para adelantar procesos de contratación de suministro de repuestos y mantenimientos preventivos y correctivos.

Los cables de potencia deben estar separados de los de comunicaciones, según las normas técnicas y los equipos de los centros de datos que lo requieran, y han de monitorearse para poder detectar las fallas que se puedan presentar.

5.8. EQUIPOS

5.8.1. Ubicación y protección de los equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones del Instituto.

Dirigida a: Todos

Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las posibilidades de acceso no autorizado, adoptando controles para minimizar el riesgo de amenazas físicas y ambientales como; robo, incendio, explosivos, humo, agua, polvo, vibración, interferencia en el suministro eléctrico o de comunicaciones, entre otros.

5.8.1.1. Política de uso de estaciones cliente.

Dirigida a: Todos, Grupo de las TIC

Los funcionarios y contratistas de soporte técnico del grupo de las TIC tienen como función exclusiva el mantenimiento y la instalación de software en los computadores, que son propiedad del Instituto Caro y Cuervo; ellos son los únicos usuarios con credenciales de acceso para realizar este tipo de actividades.

Los usuarios podrán trabajar la información institucional en modo borrador sobre los discos locales del computador asignado, sin embargo, deberán realizar la copia de sus archivos en la carpeta de *Mis documentos.*

El préstamo de computadores portátiles se debe tramitar a través de la mesa de ayuda con anticipación y se proveerá según disponibilidad.

Los equipos de cómputo que ingresan temporalmente a las diferentes instalaciones del Instituto Caro y Cuervo, que sean de propiedad de contratistas o terceros, deben ser registrados en las porterías de la entidad para poder realizar su retiro sin requerir autorización del grupo de las TIC.

El Instituto Caro y Cuervo no se hará responsable, en caso de pérdida o daño, de algún equipo informático de uso personal que haya sido ingresado a sus diferentes instalaciones.

Los funcionarios del grupo de las TIC no prestarán servicio de soporte técnico (revisión, mantenimiento y/o reparación de hardware) a equipos que no sean propiedad del Instituto Caro y Cuervo.

5.8.1.2. Política de uso de servicios de impresión.

Dirigida a: Todos, Grupo de las TIC

Para el uso de los servicios de impresión, los usuarios deben iniciar sesión con una cuenta válida en los equipos de cómputo asignados por el grupo de las TIC del Instituto Caro y Cuervo. Para la impresión de documentos, servicios de escaneo o servicios de fotocopia, los usuarios deben contar con un código válido.

La impresión de documentos a color está permitido solo para los usuarios que adelantan tareas de diseño y creación de material gráfico. Los usuarios que por razones justificadas en el desarrollo de sus actividades institucionales requieran la habilitación de este servicio, deben solicitar al jefe o supervisor que formalice la activación de este servicio a través de la mesa de ayuda.

Las impresoras son para uso exclusivamente institucional. No se permite la impresión de documentos personales o trabajos ajenos a las funciones institucionales, por lo que es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión, escáner y fotocopiado, para que no se afecte su correcto funcionamiento.

Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta debe reportar a través de la mesa de ayuda.

5.8.1.3. Seguridad del cableado.

Dirigida a: Grupo de las TIC

El grupo de las TIC debe garantizar que el cableado de la red debe ser protegido de interferencias mediante técnicas conocidas en el mercado como, por ejemplo, canaletas de dos divisiones. Además de realizar lo siguiente:

- Validar que las conexiones dentro de los centros de datos deben estar libres de contactos e instalaciones eléctricas en mal estado.
- Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
- Deben existir planos que describan las conexiones del cableado.
- El acceso a los centros de cableado (Racks), debe estar protegido.

5.8.1.4. Mantenimiento de los equipos.

Dirigida a: Grupo de recursos físicos, Grupo de las TIC

El grupo de recursos físicos es el responsable de liderar y gestionar el cumplimiento del plan de mantenimiento de todos los activos de la Entidad.

Las actividades de mantenimiento de los servidores, elementos de comunicaciones o cualquiera que pueda ocasionar una suspensión en los servicios tecnológicos, deben ser programadas y realizadas por el personal autorizado por la coordinación del grupo de las TIC.

Para los casos en que se requieran realizar actividades de mantenimiento de los sistemas eléctricos debe notificarse al grupo de las TIC con antelación para la programación de ventanas de mantenimiento y garantizar la continuidad de los servicios tecnológicos.

El grupo de las TIC debe mantener contratos de soporte y mantenimiento de los equipos críticos.

Los equipos que requieran salir de las instalaciones del Instituto por motivos de garantía o mantenimiento deben estar debidamente autorizados por el grupo de las TIC y se debe garantizar que en dichos elementos no se encuentra información clasificada o reservada.

Cuando un dispositivo vaya a ser reasignado o dado de baja debe contar con aprobación del grupo de las TIC, así mismo debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando procedimientos de borrado seguro.

5.8.1.5. Ingreso y retiro de los activos.

Dirigida a: Todos, Grupo de recursos físicos

Todo elemento que ingrese al Instituto debe ser inspeccionado por el equipo de vigilancia con el objetivo de identificar material peligroso y a su vez debe ser revisado por el grupo de recursos físicos con el fin de revisar que este coincida con su respectiva autorización de ingreso.

El grupo de recursos físicos debe mantener el inventario de activos actualizado por lo que se le debe notificar todo elemento que ingrese o se retire del Instituto siguiendo los procedimientos establecidos.

El traslado entre sedes y oficinas del Instituto Caro y Cuervo de todo activo de información está a cargo del área de recursos físicos para el control de inventarios.

5.8.1.6. Equipos de usuario desatendido.

Dirigida a: Todos

Es responsabilidad de funcionarios y terceros bloquear la sesión de su estación de en los momentos en que no estén utilizando el equipo o cuando, por cualquier motivo, deban dejar su puesto de trabajo,

la cual se podrá desbloquear sólo con la introducción de la contraseña del usuario, al finalizar sus actividades deben cerrar todas las aplicaciones y apagar el equipo de cómputo.

5.8.1.7. Política de escritorio y pantalla limpia.

Dirigida a: Todos

Los usuarios del Instituto Caro y Cuervo deben conservar su escritorio libre de información propia de la entidad que pueda ser alcanzada, copiada, no respaldada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

5.9. SEGURIDAD DE LAS OPERACIONES

5.9.1. Procedimientos operacionales y responsabilidades

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Dirigida a: Grupo de las TIC

El grupo de las TIC debe documentar los procedimientos de operación para:

- Indicar como realiza el control de cambios sobre los servicios tecnológicos del Instituto, identificándolos, planificándolos, poniéndolos a prueba y aprobándolos formalmente, así como valorando los impactos, tiempos de no disponibilidad de los servicios, comunicación a las áreas pertinentes e incluir procedimientos y responsabilidades para abortar cambios no exitosos, eventos no previstos y recuperarse de ellos.
- Especificar como realiza una gestión de capacidad de los recursos de red, de la infraestructura tecnológica y sistemas de información críticos, en el cual se deben definir los umbrales de alerta e identificar proyecciones de crecimiento que permita mantener la continuidad y la disponibilidad de los servicios tecnológicos.
- Desarrollar un procedimiento de separación de ambientes que permita realizar una transición de los diferentes sistemas desde el ambiente de desarrollo hacia el de producción, con el fin de evitar problemas operacionales que pueden desencadenar en incidentes críticos.

5.9.2. Política de protección contra software malicioso

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

Dirigida a: Grupo de las TIC

Se debe tener instalado como mínimo un software antivirus debidamente licenciado, activo y actualizado que brinde protección contra código malicioso en todos los recursos informáticos de la Entidad, asegurándose que estas herramientas no puedan ser deshabilitadas.

El grupo de las TIC debe documentar como se realiza la protección contra códigos maliciosos teniendo en cuenta los controles que utiliza (hardware o software), como se instalan y se actualizan las plataformas de detección, documentación sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso, implementación de procedimientos para recolectar información de manera regular como suscripción a listas de correo.

El grupo de las TIC debe implementar controles que impidan la modificación de las configuraciones del equipo de cómputo o del software instalado con énfasis en el sistema operativo y antivirus.

5.9.3. Copias de respaldo

Objetivo: Proteger contra la pérdida de datos

Dirigida a: Grupo de las TIC, todos

El grupo de las TIC debe contar con un procedimiento para la realización de las copias de respaldo documentado, definido y publicado en el sistema de gestión de calidad para todos los sistemas de información y repositorios de información institucional en el que los criterios definidos se adapten a las necesidades de las diferentes áreas del Instituto.

Adicionalmente, el grupo de las TIC deberá establecer mecanismos de restauración de copias de seguridad, los cuales serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

Las copias de respaldo críticas deben almacenarse en un área diferente a la sede principal del Instituto y con control de acceso, en aras de restaurar los servicios tecnológicos luego de la materialización de amenazas tales como cortes del fluido electrónico, inundaciones, terremotos, sismos, catástrofes, entre otros.

Las diferentes áreas del Instituto Caro y Cuervo deben realizar una limpieza periódica de archivos y documentos obsoletos o inservibles con el fin de optimizar el uso de los recursos de almacenamiento que ofrece la entidad a sus usuarios.

Los funcionarios y terceros deben almacenar su información en la carpeta “Mis Documentos”. De esta manera el grupo de las TIC garantizará el respaldo de la información y una eventual restauración en caso de ser requerida.

Los usuarios de la red de datos del Instituto Caro y Cuervo no podrán copiar información clasificada o reservada sin la debida autorización de su jefe inmediato, de acuerdo con las normas de calificación de la información y los niveles de seguridad establecidos en el sistema de información dispuesto para ello. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución serán sancionadas de acuerdo con las normas y legislación vigentes.

5.9.4. Registro y seguimiento

Objetivo: Registrar eventos y generar evidencia.

Dirigida a: Grupo de las TIC

El grupo de las TIC debe definir una metodología para la revisión y custodia de eventos (Event Logs), que permita, identificar las actividades por usuario, excepciones, fallas y eventos de seguridad que no den espacio a la alteración, uso no autorizado o repudio, en caso de presentarse materialización del riesgo y ser utilizados como medio probatorio.

El grupo de las TIC no debe modificar, borrar o desactivar registros (logs) de sus actividades propias, ni de los usuarios de los sistemas de información y telecomunicaciones, de igual forma se deben realizar las configuraciones de seguridad necesarias para evitar la eliminación o cambios no autorizados a los registros de información.

El grupo de las TIC debe mantener los relojes de todos los equipos y dispositivos sincronizados a un único servidor NTP (Nertwork Time Protocol – protocolo de tiempo en la red), se debe restringir a los usuarios la administración de fecha y hora de los sistemas de información, aplicaciones o equipos de cómputo a su cargo.

5.9.5. Control de software operacional

Objetivo: Asegurar la integridad de los sistemas operacionales

Dirigida a: Grupo de las TIC, todos

El grupo de las TIC debe mantener un procedimiento de control de instalación y cambios de los sistemas operativos administrados por el grupo; para mantener operativas las aplicaciones basadas en estos y que permitan procedimientos de retroceso (RollBack) exitosos, en este procedimiento se debe incluir la elaboración de copias de respaldo que puedan responder a planes de contingencia.

No se permite la descarga e instalación de software, archivos de audio, medios audiovisuales que atenten contra los derechos de autor, la infraestructura tecnológica y la seguridad de la información.

5.9.6. Gestión de vulnerabilidad técnica

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas

Dirigida a: Grupo de las TIC

Se debe contar con una metodología de identificación de vulnerabilidades técnicas en los sistemas de información y servicios tecnológicos del Instituto, como resultado de estas deben elaborarse planes de mejoramiento que permita a los responsables aplicar los controles de mitigación que correspondan, previa evaluación en un ambiente de pruebas.

5.10. SEGURIDAD DE LAS COMUNICACIONES

5.10.1. Gestión de seguridad de redes

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

Dirigida a: Grupo de las TIC

El grupo de las TIC debe disponer de una zona desmilitarizada o DMZ, entre la red interna y la red externa (internet) con el objetivo limitar conexiones desde la red interna hacia Internet y conexiones desde internet hacia la red interna del Instituto.

Los protocolos y servicios TCP/UDP que no se requieran en los servidores deben permanecer bloqueados por defecto; no se habilitarán puertos o servicios, a menos que sean solicitados y aprobados por el administrador de seguridad de la red del Instituto Caro y Cuervo.

Por seguridad y para propósitos de mantenimiento, se podrá monitorear en cualquier momento el tráfico de la red. Esta labor será realizada solo por el personal autorizado por la coordinación de las TIC, garantizando a los usuarios que no existirá revisión interna de archivos o documentos.

Las redes de datos y comunicaciones del Instituto deben estar gestionadas y controladas para la protección de la información y sus aplicaciones, gestión de red y configuración de redes virtuales o creación de subredes que permitan separar los servicios de información, usuarios y sistemas.

5.10.2. Transferencia de información

Objetivo: Mantener la seguridad de la información transferida dentro de una Entidad y con cualquier entidad externa.

Dirigida a: Grupo de las TIC, Grupo de gestión contractual

El Instituto Caro y Cuervo implementará los protocolos de seguridad necesarios para la transferencia de archivos. Cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de seguridad de la información con esa entidad a través de un acuerdo de niveles de servicio.

Los canales de red utilizados para la transferencia de información deberán contar con un mecanismo que no permita la fuga o interceptación de información, en su defecto la información que viaja por estos deberá estar cifrada.

5.10.2.1. Política de uso de correo electrónico

Dirigida a: Todos, Grupo de las TIC, comunicaciones

El Instituto Caro y Cuervo debe ofrecer a sus estudiantes, funcionarios y contratistas un servicio que permita el intercambio de mensajes a través de una cuenta de correo electrónico institucional para facilitar el desarrollo de sus funciones. Por lo anterior, los usuarios del correo electrónico institucional son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

Las cuentas de correo electrónico institucional son propiedad del Instituto Caro y Cuervo, y son asignadas a usuarios que tengan algún tipo de vinculación con la entidad, bien sea como personal de planta, contratistas, profesores, estudiantes o egresados y deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la entidad.

Los servicios de correo electrónico institucional se emplean para una finalidad académica, operativa y administrativa institucional. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura tecnológica del Instituto Caro y Cuervo se consideran bajo el control de la entidad.

El servicio de correo electrónico institucional no debe utilizarse para el envío de mensajes masivos. Para las comunicaciones que requieran la divulgación a través de correo masivo, se debe realizar la solicitud a la cuenta de correo institucional comunicacioninterna@caroycuervo.gov.co, si el contenido requiere publicación de piezas graficas que incluyen el logo o imagen del Instituto, deberá contar con la aprobación del coordinador del grupo de comunicaciones.

El servicio de correo electrónico institucional no debe ser utilizado para el envío de mensajes personales, de tipo cadena, ni mensajes de gran tamaño que puedan congestionar la red; para ello deben emplearse otros medios como, por ejemplo, los servicios de la nube de archivos digitales, tampoco se permite el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.

Los usuarios del servicio de correo electrónico institucional deben habilitar el servicio de autorrespuesta en el evento en que se encuentren ausentes por largos periodos, ya sea por el periodo de vacaciones, incapacidades, licencia, etc.

Los jefes y supervisores de los usuarios que terminan su vínculo laboral o contractual con el Instituto deben indicar al grupo de las TIC, cuál será el ***usuario/buzón delegado*** al que se redireccionarán las comunicaciones de las cuentas de correo electrónico que tienen acceso a plataformas externas y que puedan recibir información de interés para la Entidad, es decir la información de tipo misional o estratégica, si no lo hace el grupo de las TIC deberá redireccionará los correos al jefe inmediato.

Para las cuentas de correo electrónico de los egresados del Instituto, se les mantendrá activa su cuenta y deberán cumplir las políticas de seguridad, sin embargo, si un egresado no hace uso de su cuenta de correo por un periodo de tiempo de (2) dos años o se evidencia un uso indebido del correo que comprometa la reputación de la Entidad o vaya en contra de las políticas de seguridad y privacidad de la información se suspenderá dicha cuenta.

La apariencia de la firma de correo electrónico está establecida por los parámetros de la imagen institucional de la entidad y ningún funcionario o contratista está autorizado para alterar la forma o la información contenida.

Los correos electrónicos contienen una nota respecto al manejo del contenido y seguridad del mensaje enviado con la siguiente información:

"AVISO IMPORTANTE: Este mensaje de correo electrónico y sus anexos son únicamente para uso del destinario ya que puede contener información pública reservada o información pública clasificada, las cuales no son de carácter público. Si usted no es el destinatario, le solicitamos no leer, copiar, reenviar, difundir, distribuir o guardar este mensaje y sus anexos. Cualquier revisión, retransmisión, diseminación o uso del mismo, así como cualquier acción que se tome respecto a la información contenida por personas o entidades diferentes al propósito original de la misma, es ilegal.

Si usted es el destinatario, le solicitamos dar un manejo adecuado a la información; en caso de que se identifique algún hecho extraño, por favor informarlo al correo tics@caroycuervo.gov.co".

Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo con la calificación de la información establecida por el Instituto Caro y Cuervo.

Los mensajes de origen desconocido o con contenido sospechoso no deben ser respondidos, ni sus archivos adjuntos abiertos, ni establecer conexión con los enlaces que aparezcan en el mensaje ya

que podrían contener códigos maliciosos (virus, troyanos, keylogger, gusanos, etc.). Se debe reenviar el correo a la cuenta tics@caroycuervo.gov.co con la frase "mensaje sospechoso" en el asunto.

5.10.2.2. Publicación de la dirección de correo electrónico como dato de contacto

El Instituto cuenta con dos tipos de correo, el primero es el correo institucional de las dependencias ejemplo (contactenos@caroycuervo.gov.co), el cual puede ser accedido y utilizado para finalidades netamente relacionadas con el área que corresponde, por los funcionarios y/o contratistas que el coordinador de la dependencia haya establecido. Todo envío sea interno o externo que se realice a través de este correo debe contar con el aval de su respectivo coordinador pues él es el responsable del uso y manejo que se le dé a dicha cuenta.

El segundo tipo de correo es el correo institucional personal ejemplo (pepe.correa@caroycuervo.gov.co) el cual contiene el nombre y apellido del titular de la cuenta y el único responsable del uso y manejo que se le dé a este servicio, por lo cual este acceso es personal e intransferible.

Para la atención y gestión de trámites, eventos, proyectos, servicios o procesos de actividad se deben vincular las cuentas de correo institucionales de las dependencias en lugar de las cuentas de correo institucionales personales, esto con el fin de mantener la continuidad del servicio y garantizar la disponibilidad de la información.

Se debe limitar la publicación de los correos electrónicos de funcionarios y/o contratistas, salvo las directrices estipuladas por la normatividad vigente tal es el caso del directorio publicado en el portal institucional y el aplicativo SIGEP, donde el usuario debe publicar su correo institucional personal y no el correo de la dependencia.

5.10.2.3. Política de redes sociales

Dirigida a: Comunicaciones

El responsable de la comunidad virtual del Instituto Caro y Cuervo será el único que administre las cuentas de las redes sociales oficiales de la entidad, en ningún caso el contenido publicado podrá ser utilizado para beneficios personales o de terceros, así como tampoco se permite que las publicaciones reflejen las opiniones o sentimientos personales del administrador.

La información que se publique o divulgue por cualquier medio de internet, de cualquier funcionario o contratista del Instituto Caro y Cuervo, que sea creada a nombre personal, como redes sociales (Twitter, Facebook, YouTube, LinkedIn o blogs), se considera fuera del alcance del SGSI, y por lo

tanto su confiabilidad, integridad, veracidad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

El responsable de las redes sociales, el grupo de comunicaciones y los servidores públicos deberán dar cumplimiento a los lineamientos dados por el gobierno nacional sobre el manejo y uso de redes sociales de acuerdo con lo estipulado en la circular N. 01 del 22 de marzo del 2019 por la Presidencia de la Republica.

5.10.2.4. Política para la gestión de contenidos de páginas WEB (Web máster)

Dirigida a: Comunicaciones

Los responsables de los contenidos de las páginas web (Web masters) son los únicos autorizados para realizar publicaciones en los sitios web de la entidad.

El contenido web a publicar en los diferentes sitios web de la entidad, debe ser previamente revisado y aprobado por el funcionario de la oficina de comunicaciones y por el corrector de estilo o quien haga sus veces.

Los web masters son responsables de mantener respaldo de los contenidos web.

Los web masters deben proporcionar las condiciones necesarias para la actualización de la versión del software, la cual será ejecutada por los administradores de los servidores y el equipo desarrollador.

Los Web master deben disponer de un archivo actualizado con la información de la página inicial del sitio, en caso de que se requiera revertir los cambios o actualizaciones.

Para la publicación de contenido en los sitios web, los web masters deben llevar un registro de publicaciones y coordinar con el administrador web del grupo de las TIC los lineamientos técnicos y de diseño de los sitios web.

La oficina de comunicaciones deberá contar con una “política editorial y actualización de contenidos web”, y, basados en esta política, mantener una bitácora que permita auditar la publicación o modificación de información oficial en las páginas web.

Las claves de acceso a los sistemas de gestión de contenidos o CMS (Content Management System), que utilizan los web masters para la administración de los sitios Web, son estrictamente confidenciales, personales e intransferibles.

5.10.2.5. Política de uso de internet

Dirigida a: Todos

Los usuarios de la red deben ser conscientes del uso adecuado de internet, y deben evitar el acceso a sitios potencialmente peligrosos o que puedan afectar el buen desempeño de la red. El grupo de las TIC inhabilitará el acceso a sitios web identificados como peligrosos o de alto consumo de ancho de banda, de acuerdo con su categoría, y serán clasificados en el documento correspondiente a fin de proteger y no comprometer la seguridad y el desempeño de la red y los recursos informáticos de la entidad.

No se permite la navegación a sitios con contenidos que representen peligro para la entidad como pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes asociadas a estos riesgos.

El acceso a sitios web con contenido calificado como potencialmente peligroso, con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del coordinador de proceso o el supervisor de contrato. Sin embargo, el grupo de las TIC analizará el sitio web que deba ser habilitado para verificar que el mismo es seguro y que no representa un peligro para la red de datos de la entidad.

La descarga de archivos de internet debe hacerse con propósitos laborales y de forma razonable para no afectar el servicio de Internet y la red de datos en general.

5.10.2.6. Política de seguridad para la telefonía IP

Dirigida a: El Grupo de las TIC, Grupo de recursos físicos, Subdirección administrativa y financiera, todos

El grupo de las TIC administrará y gestionará el uso de las extensiones telefónicas y las configuraciones asociadas para planificar el crecimiento futuro, así como para atender oportunamente las averías y/o cambio de perfil de usuario.

El grupo de las TIC administra y gestiona los equipos de telefonía IP, así como los equipos de autoatención y correo de voz. La configuración o cambio de opciones en la grabación de autoatención, debe ser aprobada por la subdirección administrativa.

El grupo de las TIC mantendrá un inventario de los aparatos telefónicos para la gestión propia de esta oficina, sin perjuicio de los bienes devolutivos registrados en recursos físicos para la administración, reposición, detección de necesidades y resguardo de los bienes de la Institución.

La solicitud del aparato telefónico debe hacerse al grupo de recursos físicos del Instituto Caro y Cuervo y su asignación estará sujeta a la disponibilidad.

La solicitud de creación de una nueva extensión debe gestionarse a través de la mesa de ayuda, y es el supervisor de contrato o el líder de área quien realiza dicha solicitud.

Las llamadas a larga distancia nacional, internacional y telefonía móvil están habilitadas solo a funcionarios autorizados por la subdirección administrativa.

Los usuarios deben notificar a la oficina de las TIC sobre cualquier anomalía en el servicio telefónico o cuando exista la sospecha del uso indebido del mismo.

5.10.2.7. Acuerdos de confidencialidad

Dirigida a: Grupo de talento humano, Grupo de gestión contractual, todos

Todo funcionario del Instituto Caro y Cuervo debe firmar en señal de aceptación el acuerdo de confidencialidad en el proceso de vinculación con la Entidad, para el caso de los contratistas el grupo de gestión contractual deberá incluir cláusulas de confidencialidad en los contratos de prestación de servicios.

5.11. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

5.11.1. Requisitos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.

Dirigida a: Grupo de las TIC, Grupo de Investigación, todos los coordinadores

La adquisición de aplicativos o software informático debe ser aprobado o adquirido por el grupo de las TIC, en concordancia con la política de adquisición de bienes del Instituto Caro y Cuervo, según lo definido en el proceso de adquisición de bienes y servicios, y las necesidades específicas de cada proceso.

El grupo de las TIC realizará periódicamente una revisión del software utilizado en cada una de las áreas. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerada como una violación a las políticas de seguridad de la información del Instituto Caro y Cuervo.

El grupo de las TIC mantendrá bajo custodia todos los medios originales de tipo magnético o electrónico de software con sus respectivos manuales y licencias de uso adquiridos por el Instituto Caro y Cuervo, así como las claves para descargar desde la WEB el software de fabricantes y las claves de administración de los equipos informáticos, sistemas de información o aplicativos.

Los desarrollos y proyectos que se deban adelantar en la entidad y que involucren componentes de TI, deben ser informados al grupo de las TIC, a fin de contar con el acompañamiento apropiado y con la aprobación de viabilidad para su ejecución. Si se omite esta política, la entidad no se hace responsable ante ningún tercero por los requerimientos que se generen en cuanto a la legalización de las licencias, servicios de soporte o mantenimiento de productos.

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

Dirigida a: Grupo de las TIC

El grupo de las TIC debe identificar durante la etapa de levantamiento de requerimientos funcionales los requisitos de seguridad de la información, incluyendo las configuraciones de red para proteger la información que se administra en las bases de datos y que son transmitidas, estos requerimientos deben quedar documentarlos como parte del proyecto de tecnologías de la información, esto aplica para nuevos o para mejoras de los sistemas de información y servicios tecnológicos existentes que se desarrollen en el Instituto o que sean adquiridos a través de un tercero estos requisitos además deben formar parte de las fases desarrollo, implementación y mantenimiento.

5.11.1.2. Seguridad de servicios de las aplicaciones en redes públicas

Dirigida a: Grupo de las TIC

Los sistemas de información o servicios tecnológicos que transmitan y/o transfieran información sobre redes públicas deben incluir un mecanismo de cifrado de los datos que se transportan, así mismo se deben aplicar controles tales como el uso de métodos fuertes de autenticación, certificados digitales, autorización de documentos mediante firmas digitales, funcionamiento con certificados SSL y los demás que apliquen.

5.11.1.3. Protección de transacciones de los servicios de las aplicaciones

Dirigida a: Grupo de las TIC

Los servicios o sistemas asociados a transacciones electrónicas se deben proteger para evitar transmisiones incompletas, alteraciones, envíos errados o divulgación no autorizada, utilizando controles para evitar la duplicación de información en las transacciones, a través de mecanismos o protocolos como uso de certificados SSL, el uso de criptografía y otros.

5.11.2. Seguridad en los procesos de desarrollo y soporte

Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

Dirigida a: Grupo de las TIC, proveedores externos (Desarrolladores de software)

El grupo de las TIC debe asegurar que los sistemas de información o aplicativos informáticos que desarrolla internamente incluyen controles de seguridad, estén completamente documentados y que las diferentes versiones sean preservadas adecuadamente.

Los funcionarios o terceros que realicen desarrollos para el Instituto deben aplicar los lineamientos de desarrollo seguro durante todo el ciclo de vida de estos.

El grupo de las TIC debe implementar procedimientos que permitan tener un control en la generación de cambios o mejoras en el código fuente de los sistemas de información y servicios tecnológicos de la entidad, igualmente debe cerciorarse de que los funcionarios o terceros que tienen el rol de programador posean acceso sólo a la parte del código necesaria para desarrollar su trabajo.

5.11.3. Datos de prueba

Objetivo: Asegurar la protección de los datos usados para ensayos

Dirigida a: Lideres de proceso, Grupo de las TIC

El propietario del sistema de información o el servicio tecnológico desarrollado, debe realizar las pruebas de funcionamiento y de seguridad del desarrollo interno o externo adquirido y debe firmar la aceptación de las pruebas a través del acta de terminación de contrato. Se solicitará al grupo de las TIC el acompañamiento y la metodología para la realización de las pruebas de aceptación de sistemas.

Los datos de prueba no deben contener información clasificada o reservada, de ser necesario este contenido se deben utilizar mecanismos de enmascaramiento o sustitución de datos.

Los entornos de pruebas para nuevos desarrollos o para sistemas de información críticos que se encuentren habilitados deben ser autorizados por el grupo de las TIC, y en caso de ser necesario el acceso desde fuera de la red LAN del Instituto Caro y Cuervo, se asignará una dirección IP diferente a las direcciones públicas de producción.

5.12. RELACIONES CON LOS PROVEEDORES

5.12.1. Seguridad de la información en las relaciones con los proveedores

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

Dirigida a: Proveedores externos, Grupo de gestión contractual, Grupo de las TIC

Todo proveedor debe cumplir con los lineamientos establecidos en la contratación pública y las políticas de seguridad de la información del Instituto Caro y Cuervo.

El grupo de gestión contractual debe establecer los lineamientos para el cumplimiento de la política de seguridad y privacidad de la información, requisitos legales y regulatorios en todos los contratos con proveedores o terceros, incluyendo el reporte de fallas o incidentes que se presenten o evidencien en la ejecución de sus actividades, las políticas relacionadas con la protección de datos personales, información, derechos de autor y propiedad intelectual.

Con el fin de proteger la información y teniendo en cuenta la calificación de la información según los niveles de seguridad, se debe preparar y legalizar un acuerdo de confidencialidad entre la entidad y el tercero, conforme al objetivo y al alcance del contrato, el cual debe quedar firmado por ambas partes. En todos los casos deben firmarse acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad de la información y con los objetivos de la entidad.

El grupo de las TIC establecerá los requerimientos mínimos de seguridad, infraestructura y calidad de servicio, así como las características técnicas de servidores, sistemas operativos, lenguajes de programación, motores de bases de datos, etc., para la adquisición de servicios con terceros a través de la guía técnica para la evaluación de soluciones de software. Estos requisitos son fundamentales para llevar a cabo los procesos contractuales que se deriven de la necesidad de contratar servicios con terceros o desarrollos.

El grupo de las TIC elaboró la guía técnica para la evaluación de soluciones de software, la cual debe ser diligenciada por aquellos terceros que aspiran a ofrecer servicios al Instituto Caro y Cuervo, en concordancia con la política de seguridad.

5.13. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

5.13.1. Gestión de incidentes y mejoras en la seguridad de la información

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.

Dirigida a: Todos, Grupo de planeación, Grupo de las TIC

Funcionarios y terceros deben informar de cualquier evento o incidente que afecte la confidencialidad, privacidad, integridad o disponibilidad de los servicios tecnológicos, de acuerdo con lo establecido en el procedimiento reporte de incidentes de seguridad de la información, para la gestión de estos que permitan ejecutar de manera organizada las actividades de planificación, atención de incidentes y mejora continua.

Se deben definir los responsables para la gestión del tratamiento de incidentes de seguridad de la información para asegurar respuestas eficientes, documentar y mantener actualizada una gestión de conocimiento actualizada por los incidentes o eventos presentados. Así mismo definir los responsables de solucionar e implementar controles necesarios para evitar su repetición.

En el Instituto Caro y Cuervo la atención de incidentes en la infraestructura tecnológica deberá estar a cargo del grupo de las TIC, el oficial de seguridad de la información y para los casos que aplique el acompañamiento del CSIRT (Computer Security Incident Response) - Equipo de Respuesta a Incidentes de Seguridad de la Información de MINTIC.

5.14. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

5.14.1. Continuidad de seguridad de la información

Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.

Dirigida a: Proveedores externos, Líderes de proceso, Grupo de las TIC, Grupo de planeación

Los proveedores de servicios críticos deben contar con planes de continuidad que permitan desarrollar pruebas periódicas de los mismos.

Se debe realizar la identificación de activos digitales críticos para el Instituto Caro y Cuervo, sobre los cuales se debe realizar una gestión de riesgos con esta información debe procederse a realizar un análisis de impacto del Instituto que servirá para la construcción y actualización del plan de continuidad de los servicios tecnológicos críticos.

El plan de continuidad debe ser documentado, probado y actualizado de forma periódica o cuando ocurra un evento que afecte la prestación u operación de los servicios del Instituto Caro y cuervo, este documento debe ser conocido por el grupo de las TIC y los responsables de los activos de información.

Se debe generar documentación de las pruebas realizadas al plan de continuidad que incluya lecciones aprendidas y acciones de mejora, esta información debe ser acceso a los colaboradores interesados o participantes de las pruebas.

5.14.2. Redundancias

Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información

Dirigida a: Grupo de las TIC

El grupo de las TIC debe realizar las configuraciones de los servicios tecnológicos procurando asegurar la disponibilidad de servicio ejemplo de esto son los arreglos RAID de discos, directorio activo con servicio de réplica, entre otros.

El grupo de las TIC debe implementar la infraestructura necesaria para contar con redundancia en los sistemas de información o servicios críticos del Instituto.

El grupo de las TIC debe probar periódicamente las arquitecturas o servicios redundantes asegurando su operación luego de presentarse un evento.

La información que manejan los funcionarios y que hace parte de la misión funcional de la entidad, será respaldada en los servidores de archivos dispuestos para esto en cada una de las sedes, y así mismo cada uno de estos servidores realizará una réplica de los datos en la sede alterna, para mantener de esta manera un respaldo adicional fuera de las instalaciones donde se encuentran ubicados estos servidores.

5.15. CUMPLIMIENTO

5.15.1. Cumplimiento de requisitos legales y contractuales

Objetivo: Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

Dirigida a: Grupo de gestión contractual, Grupo de planeación

El Instituto Caro y Cuervo debe contar con el documento de requisitos legales el cual debe estar documentado, actualizado y publicado.

5.15.1.1. Política de retención y archivo de datos

Dirigida a: Grupo de gestión documental, Todos

La política de retención de archivos debe establecer cuánto tiempo estos se mantendrán almacenados en formato digital en el Instituto Caro y Cuervo, de acuerdo con las tablas de retención documental (TRD).

Las reglas y los principios generales que regulan la función archivística del Estado se encuentran definidos por la Ley 594 de 2000, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.

La ley 594 de 2000, en los artículos 19 y 21, prevé el uso de las TIC en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

5.15.1.2. Derechos de propiedad intelectual

Dirigida a: Grupo de gestión contractual, Asesor Jurídico, Grupo de las TIC

El Instituto Caro y Cuervo es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por funcionarios y contratistas, derivadas del objeto del cumplimiento de funciones y obligaciones asignadas, como las necesarias para el cumplimiento del objeto del contrato.

El Instituto Caro y Cuervo es el legítimo propietario de los activos de información. Así mismo, los administradores de estos activos son los funcionarios y contratistas de la entidad y son quienes están autorizados y responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura tecnológica.

5.15.1.3. Privacidad y protección de información de datos personales

Dirigida a: Asesor Jurídico, Grupo de planeación, Grupo de recursos físicos, Grupo de las TIC, todos

El Instituto Caro y Cuervo debe documentar una política de tratamiento de datos personales, la cual debe ser publicada en el portal WEB institucional indicando a los titulares las finalidades específicas por las cuales se hace la recolección de sus datos.

Toda dependencia que por su naturaleza genere información impresa y física de los ciudadanos, funcionarios y contratistas catalogada como sensible de acuerdo con la Ley 1581 de 2012, debe abstenerse de reutilizar este papel como reciclable y a su vez debe garantizar la destrucción de estos documentos cuando ya no sean requeridos para ningún proceso y trámite.

Toda dependencia, servicio tecnológico o sistema de información que recolecte información personal de ciudadanos, funcionarios y terceros, debe solicitar al titular de los datos de forma previa la autorización de tratamiento de sus datos personales. Estas autorizaciones se deben guardar y estar disponibles para cuando sean requeridas.

Las zonas de videovigilancia deben contar con un aviso de privacidad que indique a los usuarios que ingresen a las instalaciones del Instituto, que están siendo grabados y monitoreados por razones de seguridad. Para este caso se entiende que el usuario que ingrese a las instalaciones del Instituto acepta el registro de su imagen de acuerdo con lo indicado en la política de tratamiento de datos personales.

5.15.2. Revisiones de seguridad de la información

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.

Dirigida a: Unidad de control interno, Grupo de planeación, Grupo de las TIC

La unidad de control interno debe realizar auditorías internas verificando la implementación del Sistema de Gestión de Seguridad de la Información - SGSI, así como el cumplimiento de políticas y documentos generados.

El oficial de seguridad de la información se encuentra facultado para hacer las respectivas revisiones e inspecciones al cumplimiento de los lineamientos establecidos por el sistema de gestión de seguridad de la información.

El Grupo de las TIC debe verificar periódicamente que los servicios tecnológicos, sistemas de información y la Infraestructura tecnológica cumplen con los lineamientos de seguridad de la información.

6. SANCIONES POR INCUMPLIMIENTO

Una vez detectada la utilización irregular de las cuentas de acceso a través de las herramientas de monitoreo y análisis de tráfico por parte del Grupo de las TIC se procederá de la siguiente forma:

Previa verificación de la incidencia de seguridad se suspende el acceso al activo de información afectado y de forma temporal o definitiva el ingreso a internet o los servicios tecnológicos proporcionados por parte del Grupo de las TIC, según las circunstancias del hecho.

a) Tratándose de servidores públicos, deberá informarse por escrito al jefe inmediato del servidor con copia al líder del proceso Disciplinario en aras de verificar, realizar seguimiento y determinar si hay lugar a iniciar acción disciplinaria.

b) Cuando se trata de contratistas se informará por escrito al supervisor del contrato con copia al líder del proceso de gestión contractual y al asesor jurídico quienes decidirán acerca de las acciones a seguir, de conformidad con las estipulaciones contractuales y la normatividad legal sobre la materia.

7. ACTUALIZACION

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, el grupo de planeación se reserva el derecho a modificar esta política cuando sea necesario.

En todo caso, los cambios realizados en esta política serán divulgados a funcionarios y terceros del Instituto Caro y Cuervo. Es responsabilidad de cada uno de los usuarios la lectura y conocimiento de las Políticas de Seguridad contempladas en este documento.

8. DISPOSICIONES

Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su difusión.

Las normas y políticas, objeto de este documento, podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando.

Una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.

La falta de conocimiento de las normas aquí descritas por parte de los funcionarios, contratistas o terceros no los libera de la aplicación de sanciones por el incumplimiento de estas.

9. REQUISITOS LEGALES

Los requisitos legales que soportan el presente manual pueden ser consultados en el portal WEB institucional www.caroycuervo.gov.co

Gobierno Digital: El objetivo de la política de Gobierno Digital es: "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital" a través de los habilitadores transversales entre ellos seguridad y privacidad que busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información.

ISO/IEC 27001:2013 Esta norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización.

Ley 1273 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 1712 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 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 1499 de 2017 Actualiza el Modelo Integrado de Planeación y Gestión – MIPG

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.

Decreto 1078 de 2015 Decreta la estructura del sector de tecnologías de la información y las comunicaciones

CONPES 3854 de 2016: Política Nacional de Seguridad digital. Se crean las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, mediante mecanismos de participación y permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para comportamientos responsables en el entorno digital.

CONPES 3701 de 2015 Lineamientos de políticas para ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.