POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

1 OBJETIVO GENERAL. 3
1.1 Objetivos específicos. 3
2 ALCANCE. 3
3 TÉRMINOS Y DEFINICIONES. 3
4 POLÍTICAS, PROCEDIMIENTOS Y CONTROLES. 12
4.1 Políticas de gestión de activos de información. 12
4.2 Política de uso de los activos de información. 14
4.3 Política de respaldo y restauración de la información. 15
4.4 Política de seguridad dirigida a los recursos humanos. 16
4.5 Política de uso de correo electrónico. 16
4.6 Política de uso de Internet. 18
4.7 Política de gestión de claves de acceso a los sistemas de información. 19
4.8 Política de escritorio y pantalla limpia. 20
4.9 Política de uso de estaciones cliente. 20
4.10 Política de gestión y adquisición de bienes y servicios tecnológicos. 20
4.11 Política de desarrollo y mantenimiento de sistemas de información. 21
4.12 Política para la prestación de servicios por terceros. 22
4.13 Política para la gestión de contenidos de páginas Web (Web master). 23
4.14 Política de uso de mensajería instantánea y redes sociales. 23
4.15 Política de control de acceso a la red de datos LAN. 24
4.16 Política de uso de puntos de red de datos LAN. 24
4.17 Política de uso de dispositivos periféricos y de almacenamiento. 24
4.18 Política de uso de servicios de Impresión. 25
4.19 Política de retención y archivo de datos. 25
4.20 Políticas de seguridad de los centros procesamiento de datos. 26
4.21 Política de seguridad para la telefonía IP. 27
4.22 Política de gestión y uso de la red eléctrica regulada. 27
5 ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD. 28
5.1 Disposiciones. 28
6 DOCUMENTACIÓN SOPORTE. 28
7 FECHA DE VIGENCIA. 29

INTRODUCCIÓN

Las políticas de seguridad de Tecnologías de la Información y las Comunicaciones (TIC) tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de los sistemas de información (servicios de almacenamiento, equipos de cómputo, sistemas de información, redes de voz y datos) y de las personas que interactúan cuando hacen uso de los servicios asociados a ellos, y se aplican a todos los usuarios que utilizan equipos de cómputo y sistemas de información, propiedad del Instituto Caro y Cuervo.

Esta política de seguridad está elaborada de acuerdo con el análisis de riesgos y de vulnerabilidades detectados en los procesos de la entidad, teniendo en cuenta sus activos y los diferentes sistemas de información que se gestionan internamente en el proceso, por consiguiente, el alcance de estas políticas se encuentra sujeto a la dinámica y evolución del Instituto Caro y Cuervo.

Por otro lado, la elaboración de las políticas de seguridad se fundamentan en la norma ISO/IEC 20000/27001 y han sido planteadas, analizadas y revisadas con el fin de no infringir las leyes colombianas y garantías básicas de los usuarios, planteando así una buena forma de gestionar los sistemas de información, mediante el uso de protocolos de seguridad que se deben implantar en una red de datos organizada, como estrategia de seguridad para la protección de la información y dispositivos que la conforman desde:

- ✓ Control de acceso (aplicaciones, base de datos, centro de cómputo, recursos de red)
- ✓ Resguardo de la información
- ✓ Gestión de las redes y las comunicaciones
- ✓ Gestión de la continuidad del negocio
- ✓ Seguridad de la información en los puestos de trabajo
- ✓ Controles de cambios
- ✓ Protección contra intrusión en software en los sistemas de información
- ✓ Monitoreo de la seguridad
- ✓ Utilización de recursos de seguridad
- ✓ Privacidad
- ✓ Autenticidad

- ✓ Disponibilidad.

1 OBJETIVO GENERAL

Establecer los lineamientos generales en materia de gestión y seguridad para proteger los activos de información y las redes de datos y de comunicaciones digitales del Instituto Caro y Cuervo.

1.1 Objetivos específicos

- ✓ Planear, organizar y controlar las actividades que mantengan y garanticen la integridad física de los recursos informáticos, así como el resguardo de los activos de información de la entidad.

- ✓ Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de los administradores de la red.

- ✓ Mejorar la prestación de los servicios con excelentes niveles de seguridad y calidad.

- ✓ Informar a los usuarios de la red sobre normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software institucional de la red, así como la información que es procesada y almacenada en estos.

- ✓ Comprometer a todo el personal de la entidad, mediante charlas de concientización, que se darán a través del plan de capacitaciones de Talento Humano y como parte integral de la charla de inducción para nuevos funcionarios contratistas o de planta.

- ✓ Transformar a todos los funcionarios en interventores del sistema de seguridad mediante las charlas de concientización.

2 ALCANCE

Esta política es aplicable a todos los empleados, contratistas, consultores eventuales y otros empleados de la entidad, incluyendo a todo el personal externo que cuenten con un equipo conectado a la red de datos, ya sea por conexión inalámbrica o de cable. Así mismo es aplicable a todo el equipo y servicios propietarios o arrendados, que de alguna manera tengan que utilizar local o remotamente la red o recursos tecnológicos de la entidad y los servicios e intercambio de archivos y programas.

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.

Aceptación del riesgo: decisión informada de aceptar y asumir las consecuencias de un riesgo concreto.

Activo: según [ISO/IEC 13335-12004], cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Es todo activo que contiene información, el cual posee un valor y es necesario para realizar los procesos misionales y operativos del Instituto Caro y Cuervo. Estos activos se pueden clasificar de la siguiente manera:

Datos: son todos aquellos elementos básicos de la información en cualquier formato que se generan, recogen, gestionan, transmiten y destruyen en el Instituto Caro y Cuervo. Ejemplo: documento de Word "Estudios previos para la adquisición de servicios.docx"

Aplicaciones: es todo el software que se emplea para la gestión de la información. Ejemplo: WebSafi.

Personal: personas que tienen algún tipo de vínculo con el Instituto Caro y Cuervo (funcionarios, contratistas, profesores, estudiantes, visitantes y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la entidad).

Servicios: son de dos clases: actividades internas que un área de la entidad suministra a otra, y externos, aquellos que la entidad suministra a clientes y usuarios. Ejemplo: nómina, mesa de ayuda.

Tecnología: equipos utilizados para gestionar la información y las comunicaciones. Ejemplo: computadores, teléfonos, impresoras, entre otros.

Instalaciones: espacios físicos (edificios, oficinas, etc.) en donde se alojan los sistemas de información. Ejemplo: oficina de TI.

Equipamiento auxiliar: activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: planta eléctrica, aire acondicionado.

Administración de riesgos: gestión de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza a través de una secuencia de actividades que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Administración de incidentes de seguridad: un sistema de seguimiento de incidentes (denominado en inglés como *issue tracking system*, *trouble ticket system* o *incident ticket system*) es un paquete de software que administra y mantiene listas de incidentes, conforme son requeridos por una institución. Un sistema de seguimiento de incidencias también contiene una base de conocimiento con información de cada cliente,

soluciones a problemas comunes y otros datos relacionados. Un sistema de reportes de incidencias es similar a un sistema de seguimiento de errores (*bugtracker*) y, en algunas ocasiones, una entidad de software puede tener ambos, y algunos *bugtrackers* pueden ser usados como un sistema de seguimiento de incidentes, y viceversa.

Alcance: ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si solo incluye una parte de la organización.

Alerta: notificación formal de que se ha producido por un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: según (ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: según (ISO/IEC Guía 73:2002), uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditabilidad: los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Auditor: persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoria: proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso. Propiedad que garantiza que la identidad de un sujeto o recurso es la que declara. Se aplica a entidades tales como usuarios, procesos, sistemas de información.

Base de datos de gestión de configuraciones (CMDB, *Configuration Management Database*)**:** es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.

B57799: estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, se publicó la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información —no es certificable— y la parte segunda, especifica el sistema de gestión de seguridad de la información —es certificable—. La parte primera es el origen de ISO 17799 e ISO 27002, y la parte segunda, de ISO 27001. Como tal, el estándar ha sido derogado por la aparición de estos últimos.

Características de la Información: las principales son la confidencialidad, la disponibilidad y la integridad.

***Checklist*:** Véase *lista de chequeo*.

CMS: un sistema de gestión de contenidos o CMS (*Content Management System*) es un programa informático que permite crear una estructura de soporte para la creación y administración de contenidos, principalmente en páginas web, por parte de los *web masters*.

CobiT - *Control Objectives for Information and related Technology*: Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Compromiso de la Dirección: Criterios firmes de la dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Cómputo forense: también llamada informática forense, computación forense, análisis forense digital o exanimación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Confiabilidad: capacidad de un producto para realizar su función de la manera prevista. La confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un periodo de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: acceso a la información únicamente por usuarios autorizados, Según [ISO/IEC13335-1:2004]: característica/propiedad en la cual la información no está disponible o revelada a individuos, entidades o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido (Nota: control es sinónimo de salvaguarda).

Control correctivo: control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control de detección: punto que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio: control que reduce la posibilidad de materialización de una amenaza; por .ejemplo, por medio de avisos disuasorios.

Control preventivo: control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Declaración de aplicabilidad: documento que enumera los controles aplicados por el SGSI de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos, además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma ISO 27001.

Denegación de servicios: acción iniciada por una persona u otra causa que incapacite el hardware o el software, o ambos y después niegue el servicio.

Desastre: cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva: Según [ISO/IEC 13335-1: 2004]: una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Según [ISO/IEC 13335-1: 2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002], proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Según [ISO/IEC TR 18044:2004], suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva: información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

Gestión de claves: controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el

tratamiento de riesgos. Según [ISO/IEC Guía 73:2002], actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Gusanos: programa de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Siempre dañan la red (aunque sea simplemente consumiendo ancho de banda).

Impacto: resultado de un incidente de seguridad de la información.

Incidente: según [ISO/IEC TR 18044:2004], evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: la información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras. Puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Ingeniería social: en el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza, en ocasiones. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004], propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.

IPS: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger los sistemas computacionales de ataques y abusos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyos objetivos son establecer, promocionar y gestionar estándares.

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1° de julio de 2007. No es certificable.

ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005.

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005, el 1° de julio de 2007.

ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

ISO/IEC TR 13335-3: "Information technology. Guidelines for the management of IT Security.Techniquesforthemanagement of IT Security". Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

ISO/IEC TR 18044: "Information technology. Security techniques. Information security incident management". Guía de utilidad para la gestión de incidentes de seguridad de la información.

ITIL IT Infrastructure Library: Un marco de gestión de los servicios de tecnologías de la información.

Keyloggers: Aplicaciones que registran el teclado efectuado por un usuario.

Legalidad: el principio de legalidad o primacía de la ley es un principio fundamental del derecho público, conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, seguridad de información, seguridad informática y garantía de la información.

Lista de chequeo: lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría; sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

No conformidad: situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave: ausencia o fallo de uno o varios requerimientos de la 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: los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que estos no puedan ser negados posteriormente.

PDCA Plan-Do-Check-Act: modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Phishing: tipo de delito encuadrado dentro del ámbito de las estafas que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Plan de continuidad del negocio (Bussines Continuity Plan): 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.

Plan de tratamiento de riesgos (Risk treatment plan): documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005], intención y dirección general expresada formalmente por la Dirección.

Política dé escritorio despejado: política de la empresa que indica a los funcionarios, contratistas y demás colaboradores del DAPRE el deber de dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar el día.

Protección a la duplicidad: la protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, instalar un software de computadora en varias computadoras o subir la música a reproductores de audio digital para facilitar el acceso y escucharla.

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002], combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: Según [ISOIIEC Guía 73:2002], el riesgo que permanece tras el tratamiento del riesgo.

Salvaguarda: Véase: control.

Segregación de tareas: separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: según [ISO/IEC 27002:20005], preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Selección de controles: proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI Sistema de Gestión de la Seguridad de la Información: según [ISO/IEC 27001: 20005], la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos).

Servicios de tratamiento de información: Según [ISO/IEC 27002:20005], cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

***Spamming*:** Se llama spam al correo basura o *sms basura* a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina *spamming*. La vía más usada es el correo electrónico.

***Sniffers*:** programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

***Spoofing*:** falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac *Address*.

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002], proceso de selección e implementación de medidas para modificar el riesgo.

Trazabilidad: propiedad que garantiza que las acciones de una entidad se puede rastrear únicamente hasta dicha entidad.

Troyano: aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores del Instituto Caro y Cuervo, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red del Instituto Caro y Cuervo y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: según [ISO/IEC Guía 73:2002], proceso completo de análisis y evaluación de riesgos.

Virus: tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

Vulnerabilidad: debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004], debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4 POLÍTICAS, PROCEDIMIENTOS Y CONTROLES

4.1 Políticas de gestión de activos de información

Se considera información todo tipo de datos generados de manera digital, escrito en papel, formularios, o trasmitido mediante una red de datos o dispositivos móviles de almacenamiento, lo cual constituye un estado de conocimiento. Los funcionarios, contratistas y en general los usuarios de la red, responsables de la información del Instituto Caro y Cuervo, deben identificar los riesgos a los que está expuesta la información, teniendo en cuenta que esta pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como valiosa para el Instituto Caro y Cuervo; independiente del tipo de activo, se deben considerar las siguientes características.

- ✓ Los activos de información son reconocidos como valiosos para el Instituto Caro y Cuervo.
- ✓ No son fácilmente reemplazables sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
- ✓ Forman parte de la identidad y su vulneración puede poner en un nivel de riesgo las operaciones misionales y/o estratégicas del Instituto Caro y Cuervo.
- ✓ El Instituto Caro y Cuervo cuenta con un sistema de información que permite registrar y clasificar los activos de información de acuerdo con el marco normativo nacional.

La oficina de tecnologías de la información y las comunicaciones (TIC) del Instituto Caro y Cuervo proveerá y mantendrá un sistema de información para la clasificación de los activos de información de la entidad, de acuerdo con los niveles de seguridad establecidos en cada una de los procesos, teniendo como base la información registrada por los líderes de cada proceso en el sistema de activos de información http://activosinf.caroycuervo.gov.co.

Los procedimientos de seguridad de la información están bajo la responsabilidad de los coordinadores de área o líderes de grupo y deben asegurarse de que todos en el grupo cumplen con las políticas y estándares de seguridad de la información del Instituto Caro y Cuervo.

Los coordinadores de las diferentes áreas del Instituto Caro y Cuervo son los responsables de mantener actualizado el inventario de los activos de información, los cuales están registrados en http://activosinf.caroycuervo.gov.co. Estos activos se mantendrán en una base de datos bajo custodia del grupo de las TIC.

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.

Los activos de información pertenecen al Instituto Caro y Cuervo, y el uso de los mismos 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 del Instituto Caro y Cuervo instalará copias de los programas que han sido adquiridos en los equipos asignados a cada uno de los funcionarios que requieren de un computador para el desempeño de sus actividades. El uso de programas sin su respectiva licencia y sin la autorización del Instituto Caro y Cuervo, 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.

El Instituto Caro y Cuervo proporcionará al usuario los equipos informáticos y los programas instalados en ellos. Los datos y la información creados, almacenados y recibidos serán propiedad de Instituto Caro y Cuervo.

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.

El grupo de las TIC del Instituto Caro y Cuervo respaldará de manera frecuente la información vital en los equipos dispuestos para esto, a fin de garantizar la seguridad y recuperación en caso de un desastre o de un incidente con los equipos de procesamiento.

Los usuarios de la red de datos del Instituto Caro y Cuervo solo podrán realizar *backup* de sus archivos personales o de información pública.

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 clasificación

de la información y los niveles de seguridad establecidos en http://activosinf.caroycuervo.gov.co. 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.

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.

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.

Los funcionarios y contratistas del grupo de las TIC se obligan a no revelar a terceras personas la información a la que tengan acceso en el ejercicio de sus funciones, de acuerdo con la guía de clasificación de la información y según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.

Los funcionarios y contratistas del Instituto Caro y Cuervo son responsables de los recursos tecnológicos y de software que les sean asignados. Por lo tanto, son los responsables de la información que administran en los equipos asignados por la entidad y deben abstenerse de almacenar en ellos información no institucional, de acuerdo con la guía de clasificación de la información.

4.2 Política de uso de los activos de información

El grupo de las TIC es responsable de realizar el aseguramiento de los accesos a internet, a redes de terceros y de la entidad; este compromiso incluye —pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos—prevenir la introducción y propagación de virus, dada la constante evolución de nuevos ataques cibernéticos a los que están expuestos los sistemas de información; por tal razón, el grupo de las TIC continuamente implementará nuevos protocolos para mantener la seguridad de la red de datos.

El grupo de las TIC del Instituto Caro y Cuervo controlará los cambios o modificaciones que se deban hacer sobre la infraestructura tecnológica.

Los usuarios de la red de datos del Instituto no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos. Estos actos incluyen el envío de correo electrónico masivo con fines no institucionales, práctica de juegos en línea, consulta de sitios web no permitidos, entre otros.

Los usuarios de la red de datos del Instituto son responsables de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.

Los usuarios de la red de datos deberán acceder a los sistemas de información utilizando una cuenta de usuario y una contraseña válida en la red.

Los usuarios de la red de datos institucional son responsables del acceso redes externas. Deben verificar que todos los archivos o material recibido a través de medios magnéticos, electrónicos o descargas de internet 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.

4.3 Política de respaldo y restauración de la información

Todas las copias de información crítica deben almacenarse en un área adecuada y con control de acceso. Las copias de respaldo se mantendrán con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y/o por requerimiento legal.

La oficina de las TIC adoptará planes de recuperación de emergencia para todas las aplicaciones que manejen información crítica. Dichos planes se actualizarán periódicamente, y serán probados y revisados.

La oficina de las TIC mantendrá al menos una copia de la información en un servidor de archivos ubicado en la sede alterna del Instituto Caro y Cuervo. A su vez, realizará periódicamente pruebas de funcionamiento y ejecución de los procesos de *backup*. La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.

La oficina 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.

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.

El Instituto Caro y Cuervo ofrece un espacio de almacenamiento de la información institucional a sus funcionarios en un servidor de archivos con los permisos necesarios para que almacenen los archivos que considere importantes, y sobre ellos el grupo de las TIC garantizará la integridad, disponibilidad y autenticidad, siempre y cuando los usuarios cumplan los lineamientos de uso y administración de las contraseñas de acceso a los sistemas de información.

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.

Los funcionarios 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 administradores de los servidores de *backups* realizarán periódicamente pruebas de restauración de la información mediante la rotación de los medios y en un ambiente de pruebas controlado, con el objetivo de garantizar que los medios se encuentran funcionando adecuadamente.

4.4 Política de seguridad dirigida a los recursos humanos

Los responsables por propender el buen uso de los activos de información por parte de contratistas y terceras partes son los supervisores de contrato.

El grupo de Talento Humano, desde su plan de capacitaciones, 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.

Según el tipo de vinculación de personal a la entidad, los grupo de talento humano y/o de gestión contractual deben reportar al grupo de las TIC el retiro de un funcionario o contratista para revocar 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.

Los contratistas y terceras partes deben acogerse a las políticas de seguridad física y las políticas de seguridad lógica implementadas en la entidad.

4.5 Política de uso de correo electrónico.

El instituto Caro y Cuervo debe ofrecer a sus funcionarios 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.

Los servicios de correo electrónico institucional se emplean para una finalidad 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. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en el Instituto Caro y Cuervo, y no debe utilizarse para ningún otro fin.

El servicio de correo electrónico institucional no debe utilizarse para el envío de mensajes cadena.

El servicio de correo electrónico institucional no debe usarse para el envío de mensajes masivos y, en casos excepcionales, se debe utilizar la opción de copia oculta para todos los destinatarios.

El servicio de correo electrónico institucional no debe ser utilizado para el envío de 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.

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 usuarios del servicio de correo electrónico institucional no deben realizar 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 que se desvinculen de la entidad, se les eliminará la cuenta de correo, posterior a la firma de paz y salvo.

El grupo de las TIC realizará una copia de respaldo de las cuentas de correo institucional que sean eliminadas en formato .pst.

La apariencia de la firma de correo electrónico está establecida por los parámetros de la imagen institucional de la entidad y ningún funcionario 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".*

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

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

Todos los mensajes pueden ser sujetos de análisis y conservación permanente por parte del Instituto Caro y Cuervo, teniendo en cuenta la naturaleza de su existencia.

Todo usuario del servicio de correo electrónico es responsable por la destrucción de los mensajes cuyo origen sea desconocido, y por lo tanto asumirá la responsabilidad y las consecuencias que pueda ocasionar la ejecución de cualquier archivo adjunto.

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 y se debe reenviar el correo a la cuenta tics@caroycuervo.gov.co con la frase “mensaje sospechoso” en el asunto.

La única cuenta de correo electrónico autorizada para tratar temas institucionales es la asignada por el grupo de las TIC.

4.6 Política de uso de internet

Los usuarios de la red de servicios de internet del Instituto Caro y Cuervo deben hacer uso razonable y sus propósitos de empleo son laborales.

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.

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 a 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.

El acceso a sitios web con contenido clasificado 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.

4.7 Política de gestión de claves de acceso a los sistemas de información

El grupo de las TIC llevará a cabo un cronograma de charlas de sensibilización orientadas a las buenas prácticas de seguridad en la selección, uso y protección de las credenciales de acceso a los sistemas de información.

Los usuarios de la red de datos son los directamente responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos y/o servicios informáticos del Instituto Caro y Cuervo.

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 o su jefe inmediato, en caso de que el usuario titular se encuentre ausente en la entidad.

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

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.

Las contraseñas deben estar compuestas al menos por ocho caracteres alfanuméricos.

Las contraseñas se deben cambiar obligatoriamente la primera vez que el usuario ingrese al sistema. De igual manera, 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.

4.8 Política de escritorio y pantalla limpia

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.

Los usuarios deben bloquear la sesión de su computador en los momentos en que no estén utilizando el equipo o cuando, por cualquier motivo, deban dejar su puesto de trabajo.

Los documentos impresos de carácter confidencial no se deben dejar en el escritorio sin custodia.

4.9 Política de uso de estaciones cliente

Los funcionarios 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.

4.10 Política de gestión y adquisición de bienes y servicios tecnológicos

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 específica 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 considera como una violación a las políticas de seguridad de la información del Instituto Caro y Cuervo.

La solicitud de instalación de aplicativos, sistemas y equipos informáticos deben ser solicitados a través de la mesa de ayuda con su correspondiente justificación para su validación.

La oficina de las TIC mantendrá bajo custodia todos los medios originales de tipo magnético o electrónico de software y sus respectivos manuales y licencias de uso adquiridos por el Instituto Caro y Cuervo, así como las claves para descargar el software de fabricantes que los publiquen en sus páginas web y las claves de administración de los equipos informáticos, sistemas de información o aplicativos.

El software adquirido por el Instituto Caro y Cuervo es de su propiedad. La copia no autorizada de programas o de su documentación implica una violación a la política general de la entidad. Por tal razón, aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por la entidad o las sanciones que especifique la ley.

El Instituto Caro y Cuervo se reserva el derecho a proteger su buen nombre y sus inversiones en hardware y software fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas propiedad de la entidad. Estos controles pueden incluir valoraciones periódicas del uso de los programas y auditorías anunciadas y no anunciadas, a través de mantenimientos preventivos que ofrecen información detallada de los equipos de cómputo asignados a los funcionarios y que se mantendrán como parte de la hoja de vida de los mismos en el sistema de información de mesa de ayuda.

Los servicios tecnológicos como páginas web, propiedad del Instituto Caro y Cuervo, no podrán ser utilizados para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

4.11 Política de desarrollo y mantenimiento de sistemas de información

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.

Los proyectos de tecnologías de la información de cada proceso deben ser sometidos a un análisis de requerimientos con el acompañamiento del grupo de las TIC, con el fin de identificar las necesidades y

garantizar el máximo aprovechamiento de la capacidad de los recursos TIC y de los recursos económicos que se destinaran para cada proyecto.

El grupo de las TIC se asegurará de que los sistemas de información o aplicativos informáticos desarrollados por el grupo de las TIC, incluyan controles de seguridad y cumplan con las políticas de seguridad de la información. De igual manera, esta oficina se asegurará de que los desarrollos propios de la entidad estén completamente documentados y que las diferentes versiones sean preservadas adecuadamente.

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.

4.12 Política para la prestación de servicios por terceros

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 CC-PSIS-12. 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 identificará los riesgos a los que puede estar expuesta la información y los servicios de procesamiento de información que involucren partes externas al Instituto Caro y Cuervo. El resultado del análisis de riesgos se dará a través del acuerdo de nivel de servicios y será la base para el establecimiento de los controles, que será establecido por el grupo de las TIC antes de firmar cada contrato.

Con el fin de proteger la información de ambas partes, se formalizará un acuerdo de confidencialidad. Este deberá definir claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir.

Si la información intercambiada lo amerita, y teniendo en cuenta la clasificación 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.

La oficina de las TIC elaboró la guía técnica para la evaluación de soluciones de software CC-PSIS-12, 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.

4.13 Política para la gestión de contenidos de páginas web (*Web master*).

Las áreas que requieran publicar contenido en los sitios web, deben tramitar una solicitud formal a través de la mesa de ayuda, de la oficina de 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, deben ser previamente revisados y aprobados 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.

4.14 Política de uso de mensajería instantánea y redes sociales

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.

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 uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.

No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.

4.15 Política de control de acceso a la red de datos LAN

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

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 la entidad, la cual debe ser aprobada, registrada y auditada, a excepción de los casos que autorice la oficina TIC.

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 quipos cuentan con las mínimas 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 implementará los protocolos de seguridad necesarios que posee la entidad 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; en todo caso se deben revisar y proponer controles en concordancia con las políticas de seguridad de la información. Los resultados de la revisión de requerimientos de seguridad, acordados con servicios prestados por terceros, se documentarán y preservarán para futuras referencias o para demostrar el cumplimiento con las políticas y con los controles de seguridad.

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.

4.16 Política de uso de puntos de red de datos LAN

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.

4.17 Política de uso de dispositivos periféricos y de almacenamiento

El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.) puede ocasionalmente generar riesgos para la entidad al ser conectados en los computadores, ya que son susceptibles a la transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada.

Para utilizar dispositivos de almacenamiento externo, el usuario debe realizar un escaneo en busca de virus, antes de copiar o consultar información en estos medios.

Los dispositivos de apoyo (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por el Instituto Caro y Cuervo.

Todos los incidentes relacionados con los equipos periféricos que puedan afectar la seguridad de la información, deben ser reportados a través de la mesa de ayuda del Instituto Caro y Cuervo.

4.18 Política de uso de servicios de Impresión

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 coordinador del área que formalice la activación del mismo 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.

4.19 Política de retención y archivo de datos

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.

4.20 Políticas de seguridad de los centros procesamiento de datos

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 el instituto.

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.

El personal del grupo de las TIC debe velar por que se cumpla con el registro en la bitácora de acceso al centro de datos de las personas ajenas a la oficina que ingresen y que hayan sido autorizadas previamente para adelantar cualquier tipo de actividad o revisión.

En las instalaciones de los centros de datos o centros de cableado no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

Las conexiones dentro de los centros de datos deben estar libres de contactos e instalaciones eléctricas en mal estado.

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 cableado de la red debe ser protegido de interferencias mediante técnicas conocidas en el mercado como, por ejemplo, canaletas de dos divisiones.

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.

4.21 Política de seguridad para la telefonía IP

La oficina 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.

Los aparatos telefónicos son un recurso que la entidad pone a disposición de los usuarios para facilitar el desarrollo de sus funciones. En este sentido, como se indica en las Políticas Generales descritas en este documento, los recursos son propiedad de la entidad y no de la persona a quién fue asignada para su uso.

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.

Los usuarios deben reportar cualquier cambio a través de la mesa de ayuda, a fin de actualizar la base de datos de usuarios del servicio telefónico y poder eliminar el servicio o modificar el perfil.

4.22 Política de gestión y uso de la red eléctrica regulada

La oficina de las TIC deberá mantener actualizados los planos de la red eléctrica regulada. De igual manera, mantendrá vigentes los contratos de soporte y mantenimiento de los equipos críticos de tecnología.

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.

Las tomas eléctricas de red regulada son de uso exclusivo para la conexión de computadores. Los demás elementos deberán conectarse a la red no regulada.

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 ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, la oficina de las TIC se reserva el derecho a modificar esta política cuando sea necesario. En todo caso, los cambios realizados en esta política serán divulgados a los usuarios de la red de datos 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.

5.1 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 las mismas.

6 DOCUMENTACIÓN SOPORTE

ISO/IEC 27001, Política General de la Seguridad de la información, así como normatividad interna y regulación vigente.
Ley 527 de 1999, Presidencia de la república, define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.

ISO/IEC 20000, gestión de servicios de TI.

NNSI/TIA – 942, estándar para el diseño e instalación de infraestructura de centros de datos.

Ley 1273 de 2009, de la protección de la información y de los datos.

Artículo 269I, hurto por medios informáticos y semejantes.

Artículo 269J, transferencia no consentida de activos.

7 FECHA DE VIGENCIA

Las presentes disposiciones rigen a partir de la fecha de aprobación por la alta dirección y será válida hasta que sea sustituida por una política posterior.