MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CORPORACIÓN AUTÓNOMA REGIONAL DE CUNDINAMARCA – CAR

Contenido

INTRODUCCIÓN 8
1. OBJETIVOS 8
2. ALCANCE 8
3. REQUISITOS LEGALES Y/O REGLAMENTARIOS 9
4. TÉRMINOS Y DEFINICIONES 11
5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN 15
5.1 Orientación de la dirección para la gestión de la seguridad de la información 15
5.1.1 Políticas para la seguridad de la información 15
5.1.2 Revisión de las políticas para la seguridad de la información 16
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 16
6.1 Organización interna 16
6.1.1 Roles y responsabilidades para la seguridad de la información 16
6.1.2 Separación de deberes 16
6.1.3 Contacto con las autoridades 17
6.1.4 Contacto con grupos de interés especial 17
6.1.5 Seguridad de la Información en Gestión de Proyectos 17
6.2 Dispositivos móviles y teletrabajo 17
6.2.1 Política para dispositivos móviles 17
6.2.2 Teletrabajo 18
7 SEGURIDAD DE LOS RECURSOS HUMANOS 20
7.1 Antes de asumir el empleo 20
7.1.1 Selección 20
7.1.2 Términos y condiciones del empleo 20

7.2 Durante la ejecución del empleo 20
7.2.1 Responsabilidades de la dirección 20
7.2.2 Toma de conciencia, educación y formación en Seguridad de la Información ... 21
7.2.3 Proceso Disciplinario 21
7.3 Terminación y cambio del empleo 24
7.3.1 Terminación o cambio de responsabilidades de empleo 24
8 GESTIÓN DE ACTIVOS 24
8.1 Responsabilidad por los activos 24
8.1.1 Inventario de activos 24
8.1.2 *Propiedad de los Activos* 24
8.1.3 Uso aceptable de los activos 25
8.1.4 Devolución de los activos 25
8.2 Clasificación de la Información 25
8.2.1 Clasificación de la información 25
8.2.2 Etiquetado de la Información 26
8.2.3 Manejo de Activos 26
8.3 Manejo de los medios 26
8.3.1 Gestión de medios removibles 26
8.3.2 Disposición de los medios 26
8.3.3 Transferencia de medios físicos 26
9 CONTROL DE ACCESO 27
9.1 Requisitos del negocio para control de acceso 27
9.1.1 Política de control de acceso 27
9.1.2 Acceso a redes y a servicios en red 27
9.2 Gestión de acceso de usuarios 28
9.2.1 Registro y cancelación del registro de usuarios 28
9.2.2 Suministro de acceso de usuarios 28
9.2.3 Gestión de derechos de acceso privilegiado 28
9.2.4 Gestión de información de autenticación secreta de usuarios 29
9.2.5 Revisión de los derechos de acceso de usuarios 29
9.2.6 Retiro o ajuste de los derechos de acceso 29

9.3 Responsabilidades de los usuarios 30
9.3.1 Uso de información de autenticación secreta 30
9.4 Control de acceso a sistemas y aplicaciones 30
9.4.1 Restricción de acceso a la información 30
9.4.2 Procedimiento de ingreso seguro 30
9.4.3 Sistema de gestión de contraseñas 31
9.4.4 Uso de programas utilitarios privilegiados 31
9.4.5 Control de acceso a códigos fuente de los programas 32
10 CRIPTOGRAFÍA 32
10.1 Controles criptográficos 32
10.1.1 Política sobre el uso de controles criptográficos 32
10.1.2 Gestión de llaves 33
11 SEGURIDAD FÍSICA Y DEL ENTORNO 33
11.1 Áreas seguras 33
11.1.1 Perímetro de Seguridad Física 33
11.1.2 Controles de acceso físico 34
11.1.3 Seguridad de oficinas, recintos e instalaciones 34
11.1.4 Protección contra amenazas externas y ambientales 34
11.1.5 Trabajo en áreas seguras 35
11.1.6 Áreas de despacho y carga 35
11.2 Equipos 35
11.2.1 Ubicación y protección de los equipos 35
11.2.2 Servicios de Suministro 35
11.2.3 Seguridad del Cableado 35
11.2.4 Mantenimiento de Equipos 36
11.2.5 Retiro de activos 36
11.2.6 Seguridad de equipos y activos fuera de las instalaciones 37
11.2.7 Disposición segura o reutilización de equipos 37
11.2.8 Equipos de usuario desatendido 37
11.2.9 Política de escritorio limpio y pantalla limpia 37

12 SEGURIDAD DE LAS OPERACIONES 38
12.1 Procedimientos operacionales y responsabilidades 38
12.1.1 Procedimientos de operación documentados 38
12.1.2 Gestión de Cambios 38
12.1.3 Gestión de capacidad 38
12.1.4 Separación de los ambientes de desarrollo, prueba, y operación 39
12.2 Protección contra códigos maliciosos 39
12.2.1 Controles contra códigos maliciosos 39
12.3 Copias de respaldo 39
12.3.1 Respaldo de la información 39
12.4 Registro y seguimiento 40
12.4.1 Registro de eventos 40
12.4.2 Protección de la información de registro 41
12.4.3 Registros del administrador y del operador 41
12.4.4 Sincronización de relojes 41
12.5 Control de software operacional 41
12.5.1 Instalación de software en sistemas operativos 41
12.6 Gestión de la vulnerabilidad técnica 42
12.6.1 Gestión de las vulnerabilidades técnicas 42
12.6.2 Restricciones sobre la instalación de software 42
12.7 Consideraciones sobre auditorias de sistemas de información 43
12.7.1 Controles de auditorías de sistemas de información 43
13 SEGURIDAD DE LAS COMUNICACIONES 43
13.1 Gestión de la seguridad de las redes 43
13.1.1 Controles de redes 43
13.1.2 Seguridad de los servicios de red 44
13.1.3 Separación en las redes 44
13.2 Transferencia de información 44
13.2.1 Políticas y procedimientos de transferencia de información 44
13.2.2 Acuerdos sobre transferencia de información 44
13.2.3 Mensajería electrónica 45

13.2.4 Acuerdos de confidencialidad o de no divulgación 47
14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 47
14.1 Requisitos de seguridad de los sistemas de información 47
14.1.1 Análisis y especificación de requisitos de seguridad de la información 47
14.1.2 Seguridad de servicios de las aplicaciones en redes públicas 47
14.1.3 Protección de transacciones de los servicios de las aplicaciones 48
14.2 Seguridad en los procesos de desarrollo y de soporte 48
14.2.1 Política de desarrollo seguro 48
14.2.2 Procedimiento de control de cambios en sistemas 48
14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación 49
14.2.4 Restricciones en los cambios a los paquetes de software 49
14.2.5 Principios de construcción de los sistemas seguros 49
14.2.6 Ambiente de desarrollo seguro 49
14.2.7 Desarrollo contratado externamente 49
14.2.8 Pruebas de seguridad de sistemas 50
14.2.9 Pruebas de aceptación de sistemas 50
14.3 Datos de prueba 50
14.3.1 Protección de datos de prueba 50
15 RELACIÓN CON LOS PROVEEDORES 50
15.1 Seguridad de la información en las relaciones con los proveedores 50
15.1.1 Política de seguridad de la información para las relaciones con proveedores 50
15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores 51
15.1.3 Cadena de suministro de tecnología de información y comunicación 51
15.2 Gestión de la prestación de servicios de proveedores 52
15.2.1 Seguimiento y revisión de los servicios de los proveedores 52
15.2.2 Gestión de cambios en los servicios de los proveedores 52
16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 53
16.1 Gestión de incidentes y mejoras en la seguridad de la información 53
16.1.1 Responsabilidades y procedimientos 53
16.1.2 Reporte de eventos de seguridad de la información 53

16.1.3 Reporte de debilidades de seguridad de la información 53
16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos 53
16.1.5 Respuesta a incidentes de seguridad de la información. 54
16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información 54
16.1.7 Recolección de evidencia 54
17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO 54
17.1 Continuidad de seguridad de la información 54
17.1.1 Planificación de la continuidad de la seguridad de la información 54
17.1.2 Implementación de la continuidad de la seguridad de la información. 54
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información 55
17.2 Redundancias 55
17.2.1 Disponibilidad de instalaciones de procesamiento de información 55
18 CUMPLIMIENTO 55
18.1 Cumplimiento de los requisitos legales y contractuales 55
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales 55
18.1.2 Derechos de propiedad intelectual 56
18.1.3 Protección de registros 56
18.1.4 . Privacidad y protección de información de datos personales 56
18.1.5 . Reglamentación de controles criptográficos 56
18.2 Revisiones de seguridad de la información 57
18.2.1 *Revisión independiente de la seguridad de la información* 57
18.2.2 Cumplimiento con las políticas y normas de seguridad 57
18.2.3 Revisión del cumplimiento técnico 57
19 ANEXOS 57
T IC-MN-04-FR-XX Compromiso de Confidencialidad 57

INTRODUCCIÓN

La Corporación Autónoma Regional de Cundinamarca – CAR, establece que la información es un activo fundamental para el desarrollo de las actividades de Gobierno, en razón a que es una herramienta de gran importancia para la toma de decisiones, motivo por el cual, la Corporación Autónoma Regional de Cundinamarca – CAR, está comprometida a proteger los activos de información de la entidad (Empleados, información y entorno laboral), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones de gobernabilidad, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores y personas que hagan uso de los activos de información de la Corporación Autónoma Regional de Cundinamarca – CAR; siguiendo las directrices del Modelo de Seguridad y Privacidad de la Información MSPI de MINTIC y la norma NTC ISO 27001:2013.

1. OBJETIVOS

- Definir las pautas, directrices y reglas para generar una adecuada seguridad y protección de la información de los procesos de la Corporación Autónoma Regional de Cundinamarca – CAR.

- Informar al mayor nivel de detalle a los usuarios, directivos, funcionarios y contratistas las normas y mecanismos que deben cumplir en las interacciones con los activos de información de la Corporación Autónoma Regional de Cundinamarca – CAR, y establecer el alcance de las responsabilidades que compromete en la gestión a cada uno de ellos.

2. ALCANCE

Las Políticas de seguridad de la Información cubren los aspectos de privacidad, acceso, autenticación, mantenimiento y divulgación relacionados con cualquier activo de información, que conllevan a disponer guías y controles que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros, que laboren o tengan relación con la Corporación Autónoma Regional de Cundinamarca – CAR, para alcanzar un adecuado nivel de protección en cuanto a confidencialidad, integridad y disponibilidad de la información.

3. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Con el objeto de mitigar los riesgos relacionados con la autenticidad, la integridad, la disponibilidad, el no repudio, la confidencialidad y la trazabilidad de la información, se tiene que cualquier incidente que viole el marco normativo legal vigente en Colombia, en materia de políticas de seguridad de la Información estará sujeto, entre otras, a lo establecido en las siguientes disposiciones legales:

1. Marco normativo de buenas prácticas para el tratamiento de la información:

DECRETO 555 DEL 9 DE ABRIL 2022*: "Por* el cual se adiciona la sección 6 del título 1, parte 2, libro 2 del Decreto 1072 de 2015, único Reglamentario del Sector Trabajo, y se reglamenta el artículo 17 de la Ley 2069 de 2020, y la Ley 2021 de 2021 y se regula el trabajo remoto.

RESOLUCIÓN 746 DE 11 DE MARZO 2022 "Por el cual establece el Modelo de Seguridad y Privacidad de la información y se definen lineamientos adicionales a los establecidos en la resolución No. 500 de 2021.

DECRETO 338 DE 8 DE MARZO DE 2022*:* "Por la cual se adiciona el Título 21 de la parte 2 del Libro del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea un Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"

DIRECTIVA PRESIDENCIAL 02 DEL 24 DE FEBRERO DE 2022*:* Reiteración de la política pública en materia de seguridad digital.

EL DECRETO 767 DE 2022, "*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"*

DECRETO REGLAMENTARIO 103 DE 2015, compilado en el Decreto Único Reglamentario 1080 de 2015, por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura. Tiene por objeto: *"reglamentar la Ley 1712 de 2014, en lo relativo a la gestión de la información pública*".

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*", la cual tiene por objeto "… *regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información"*.

DECRETO REGLAMENTARIO 1377 DE 2013, *"Por el cual se reglamenta parcialmente la Ley 1581 de 2012", Compilado y derogado parcialmente por el Decreto 1081 de 2015.* Tiene como objeto: *"…reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales".*

NTC/ISO 27002:2013, recomendaciones y buenas prácticas para la gestión de seguridad de la información.

NTC-ISO-IEC 27001:2013, *"Sistemas de Gestión de Seguridad de la Información"*

ISO/IEC 27032:2012 *Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad.*

LEY 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. De conformidad con su artículo 1, tiene por objeto *"(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma*".

LEY 527 DE 1999 *"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".*

La Corporación Autónoma Regional de Cundinamarca - CAR, mediante la Resolución 1245 de 2012, actualizó las políticas de seguridad informática y a través de la Resolución No. 2518 de 2015 de la Corporación Autónoma Regional de Cundinamarca, adoptó las políticas de gestión de la información, las cuales fueron modificadas con la Resolución 1651 de 2016; de otra parte, mediante la Resolución 3293 de 2019, se actualizó las políticas de seguridad de la información

2. Marco Normativo Sancionatorio:

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

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

LEY 1952 DE 2019 "Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario."

LEY 1273 DE ENERO 5 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 734 DE 2002 "por la cual se expide el Código Disciplinario Único".

4. TÉRMINOS Y DEFINICIONES

Se definen a continuación los siguientes términos técnicos:

Activo: Recurso del sistema de información o cualquier elemento que tenga valor para la organización.

Activo de Información: Todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información de la institución. Ej. Bases de datos, sistemas operacionales, redes, sistemas de información y comunicaciones, documentos impresos, fichas, formularios y recursos humanos

Administrador del Sistema: Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está dirigida por la Gerencia de informática y se realizará por conducto de las Coordinaciones de la misma.

Administrador de Correo: Persona responsable de solucionar problemas en el correo electrónico, responder preguntas a los usuarios y otros asuntos en un servidor.

Análisis de riesgos: Proceso sistemático que permite identificar y determinar el impacto o grado de vulnerabilidad de los activos de la organización.

Ataque Cibernético: Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado, por lo general con intenciones insanas y perjudiciales.

Brecha de Seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Buzón: También conocido como cuenta de correo, es un espacio exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a la Corporación Autónoma Regional de Cundinamarca – CAR.

Centro de Cómputo: También conocido como Centro de Procesamiento de Datos, o Data Center es una instalación que se encarga del procesamiento de datos e información de manera sistematizada. El procesamiento se lleva a cabo con la utilización de computadoras (Hardware) y programas (Software) necesarios para cumplir con dicha tarea.

Chat: Comunicación simultánea y sincronizada entre dos o más personas a través de Internet.

Confidencialidad: Característica de la información por medio de la cual no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados. La información debe ser vista o estar disponible solo a las personas autorizadas.

Control: Mecanismo para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

Correo Electrónico: También conocido como E-mail, es un servicio de red que permite a los usuarios enviar y recibir textos, imágenes, videos, audio, programas, a través de internet.

Cuentas de Correo: Son espacios de buzones para la recepción, envió y almacenamiento de mensajes de correo electrónico en internet.

Contraseña o Password: Es una forma de autenticación privada, compuesta por un conjunto de números, letras y caracteres, que permiten al usuario tener acceso a un computador, a un archivo y/o a un programa.

Disponibilidad: Es la garantía de poder acceder a los activos de la información cuando sea necesario, por personal autorizado.

Dispositivo móvil: Elemento electrónico de tamaño pequeño, con capacidades de procesamiento de datos, conexión a Internet y memoria Son ejemplos de estos: celulares inteligentes, tabletas y portátiles.

El Teletrabajador: es la persona que el marco de la relación laboral dependiente utiliza las tecnologías de la información y comunicación como medio o fin para realizar su actividad laboral fuera del local del empleador, en cualquiera de las formas definidas por la ley.

Evento de Seguridad de La información: Ocurrencia identificada de una situación de sistema, servicio o red que indica una posible violación de la política de seguridad de la

información o falla de salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad de un activo de información.

Firewall: Dispositivo que permite bloquear o filtrar el acceso en redes de comunicación.

Firma Digital: La firma digital hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

Funcionarios: Las personas naturales que ejercen la función pública establecen una relación laboral con el Estado y son en consecuencia funcionarios públicos.

Hacker: Persona dedicada a realizar entradas no autorizadas a los sistemas, por medio de redes de comunicación como Internet, con el objeto de encontrar vulnerabilidades en los sistemas.

Host: Termino usado en informática para referirse a los computadores conectados a la red, que proveen y/o utilizan servicios de ella. Los usuarios deben utilizar hosts para tener acceso a la red

Incidente de Seguridad de la información: Es la identificación de la ocurrencia de un hecho que está relacionado con los activos de información, que indica una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

Infraestructura de Procesamiento de Información: Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

Integridad: La propiedad de salvaguardar la exactitud y completitud de los activos de información.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.

Intranet: Red privada dentro de una empresa, que utiliza el mismo software y protocolos empleados en la Internet global, pero que es de uso interno.

LAN: (Local Area Network). (Red de Área Local). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.

Malware: Código malicioso o cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema informático.

Pasante: Prácticas profesionales que desarrollan personas que están culminando sus estudios o que recién han egresado de la carrera.

Política: Son instrucciones mandatarias que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

Programas utilitarios: Los programas utilitarios, son programas diseñados para realizar una función determinada, Que sirve para ejercer tareas específicas o diversas en un dispositivo, por ejemplo, un editor, un depurador de código o un programa para recuperar datos perdidos o borrados accidentalmente en el disco duro.

Red: Se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

Riesgo residual: Es el riesgo remanente, después de la implantación de las medidas de seguridad determinadas en el plan de seguridad de la información.

Servidores Públicos: Concepto genérico que emplea la Constitución Política para comprender a los miembros de las corporaciones públicas y a los empleados y trabajadores del Estado y de sus entidades descentralizadas territorialmente y por servicios; todos ellos están "al servicio del Estado y de la comunidad" y deben ejercer sus funciones "en la forma prevista en la Constitución, la ley y el reglamento.

Sistema de Gestión de Seguridad de la información: SGSI La parte del sistema total de gestión, basada en un enfoque de riesgo de negocios, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
Seguridad: Mecanismos de control que evita el uso no autorizado de recursos.

Seguridad de la Información: Son medidas preventivas que incluyen factores de confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, aceptabilidad y confiabilidad de la información.

Servidor: Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

Servidor de Correo: Dispositivo y/o aplicación informática, cuya función es gestionar el tráfico de ficheros a través del correo electrónico, su misión es la de almacenar, en su disco duro, los mensajes que envía y que reciben los usuarios.

Sistema Operativo: Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora, servidor o dispositivo móvil.

Teletrabajo: Es una forma de organización laboral, que se efectúa en el marco de un contrato de trabajo o de una relación laboral dependiente, que consiste en el desempeño

de actividades remuneradas utilizando como soporte las tecnologías de la información y la comunicación -TIC para el contacto entre el trabajador y empleador sin requerirse la presencia física del trabajador en un sitio específico de trabajo. (LEY 1221 DE 2008)

Trabajo en Casa. Se entiende como trabajo en casa la habilitación al servidor público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones (Ley 2088 de 2021).

Terceros: Se entiende por tercero a toda persona, jurídica o natural ajena la Corporación Autónoma Regional de Cundinamarca – CAR, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

Troyano: Es un programa con una determinada función o utilidad, pero que contiene código oculto para ejecutar acciones no esperadas por el usuario.

Virus: Software malicioso que tiene por objeto alterar el normal funcionamiento de una computadora, reemplazando así programas ejecutables, sin la autorización ni el conocimiento del usuario.

5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

5.1 Orientación de la dirección para la gestión de la seguridad de la información

5.1.1 Políticas para la seguridad de la información

Las políticas de seguridad de la información se deben verificar, definir, implementar, revisar y actualizar para mantener salvaguardados los activos de la Entidad.

Las políticas de Seguridad de la Información establecidas mediante resolución Número 3293 de 2019, tiene como objetivos:

- Definir las pautas, directrices y reglas para generar una adecuada seguridad y protección de la información de los procesos de la Corporación, estableciendo dentro del plan estratégico de TI su liderazgo y desarrollo.
- Informar al mayor nivel de detalle a los usuarios, directivos, funcionarios y contratistas las normas y mecanismos que deben cumplir en las interacciones con

los activos de información de la Corporación, y establecer el alcance de las responsabilidades que compromete en la gestión a cada uno de ellos.

- Asegurar el cumplimento de los controles, para prevenir o mitigar sus riesgos; en aras del cumplimiento de las políticas y objetivos de seguridad de la información; de tal manera que se garantice la integridad, confidencialidad y disponibilidad de la información y la mejora continua.

5.1.2 Revisión de las políticas para la seguridad de la información

Las políticas de seguridad de la información serán aprobadas por la Dirección, a través de acto administrativo.

Las políticas de seguridad de la información serán revisadas anualmente o cuando se requiera hacer actualización de estas.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Organización interna

6.1.1 Roles y responsabilidades para la seguridad de la información

La Corporación, crea un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, así como la creación del Comité de seguridad de la información.

Comité de seguridad de la información: se creará mediante acto administrativo expedido por la dirección General de la Corporación, en donde se definirán los integrantes, funciones y demás lineamientos.

Oficial de Seguridad de la Información: las funciones de Oficial de seguridad de la Información serán definidas y asignadas por la Oficina de Tecnologías de la Información y las Comunicaciones.

6.1.2 Separación de deberes

La Corporación, establece la separación de deberes para controlar el cumplimiento de operación de la seguridad de la información.

Esta política garantizará que existen responsabilidades claramente asignadas en todos los niveles organizacionales para la gestión de seguridad de los activos de la información; se contará con un comité de seguridad de la información conformado por personal idóneo, que apoyará como asesor interno de seguridad, con el objetivo de direccionar y hacer cumplir los lineamientos de La Corporación en la materia de Seguridad de la información y revisar las posibles incidencias y acciones que se deben tomar.

Todos los servidores públicos con acceso a los activos de información de la Corporación tendrán el compromiso con la seguridad de cumplir las políticas y normas que la Corporación dicte, así como reportar los incidentes que se pueda detectar.

6.1.3 Contacto con las autoridades

La Corporación, mantendrá contacto apropiado con las autoridades pertinentes relacionadas a la seguridad de la Información, atendiendo las recomendaciones de los responsables en seguridad de la información.

6.1.4 Contacto con grupos de interés especial

La Corporación, mantendrá contacto apropiado con grupos de interés especializados con la seguridad de la Información.

La oficina de tecnologías de la Información y las Comunicaciones establecerá acuerdos que permitan identificar los requisitos necesarios para la protección de la información.

6.1.5 Seguridad de la Información en Gestión de Proyectos

La seguridad de la información se debe integrar en la gestión de proyectos de la Corporación, para identificar que posibles riesgos pueden ocurrir, y tratarlos como parte de la gestión de proyectos.

6.2 Dispositivos móviles y teletrabajo

6.2.1 Política para dispositivos móviles

El uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, está permitido para el acceso a los aplicativos Web institucionales y el acceso al correo electrónico institucional, para lo cual el servidor público tendrá asignado un usuario y contraseña con los respectivos niveles de acceso de acuerdo con el rol asignado.

Los dispositivos móviles de propiedad de la Corporación, asignados a los servidores públicos son para uso de las actividades propias del cargo o desempeño laboral y deben estar protegidos con una contraseña de inicio de sesión.

Está prohibido el uso de dispositivos móviles de propiedad de la Corporación para guardar información personal; igualmente está prohibido realizar instalación de software no autorizado.

Los dispositivos móviles de propiedad del servidor público los podrá utilizar para el acceso a los aplicativos web y correo electrónico institucional, bajo el compromiso de uso de software legal y antivirus actualizado.

Si el usuario del dispositivo móvil requiere acceso a recursos o aplicativos no publicados en la web, deberá hacer la solicitud de una conexión VPN a la Oficina de las Tecnologías de la Información y las Comunicaciones OTIC, la cual se configura sólo con acceso a los recursos solicitados.

La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC adoptará las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móviles.

6.2.2 Teletrabajo

El Teletrabajo deberá estar autorizado y reglamentado por la Oficina de Talento Humano, de acuerdo con la Ley 1221 de 2008: “Por la cual se establecen normas para promover y regular el Teletrabajo…” y el Decreto 884 de 2012: “Por medio del cual se reglamenta la Ley 1221 de 2008, y definirá los compromisos del buen uso de la información”.

El acceso remoto a los recursos corporativos desde los equipos de teletrabajo debe realizarse a través de una conexión VPN que se provee desde la Oficina de las Tecnologías de la Información y las Comunicaciones OTIC y sólo se debe permitir acceso a los recursos para los cuales se haya autorizado. El acceso al correo electrónico y los aplicativos Web institucionales se hará normalmente a través de los Navegadores.

Las conexiones remotas a los recursos informáticos deberán hacerse a través de VPN, las cuales deben ser configuradas por la oficina de tecnologías de la información y las comunicaciones.

Los equipos de cómputo para teletrabajo deben ser asignados por la Corporación y deben cumplir con una línea base definida en cuanto a configuración, controles y software instalado.

En los equipos de cómputo de los usuarios de Teletrabajo, no se deberá almacenar información corporativa. Esta información deberá quedar en un repositorio en un servidor de archivos definido para tal fin, en donde se controle el acceso. Para este caso la Corporación tiene disponible la intranet, el One Drive (nube privada Corporación) y servidores.

La información del repositorio del servidor de archivos definido para usuarios de Teletrabajo está sujeta de una política de respaldo y retención. De requerir un backups especial lo debe solicitar a la Oficina de las TIC.

Si la clasificación de la información que produzca procese o transfiera el usuario teletrabajador lo requiere, se deben celebrar acuerdos de confidencialidad o de no divulgación.

La contraseña de inicio de sesión en el equipo de cómputo del usuario de teletrabajo debe tener una vigencia definida de acuerdo con las políticas de seguridad de la información.

La base de firmas y definiciones del producto de protección antivirus debe actualizarse cuando el equipo de cómputo del teletrabajador se conecta desde el sitio remoto.

El equipo de cómputo del teletrabajador debe descargar y aplicar las actualizaciones de seguridad del sistema Operativo y otras actualizaciones de software que requiera para sus funciones.

Los usuarios de teletrabajo deben aceptar la política de uso y restricción de software. Esta señala que no pueden instalar ningún software en el equipo o usar alguno que se encuentra por fuera de la línea base definida por la Oficina de las Tecnologías de la Información y las Comunicaciones.

El usuario de teletrabajo debe conocer y cumplir las políticas de seguridad de la información y de protección de datos personales establecidas en la Corporación

7 SEGURIDAD DE LOS RECURSOS HUMANOS

7.1 Antes de asumir el empleo

7.1.1 Selección

Se debe verificar las hojas de vida del personal a contratar, para determinar la veracidad de la información.

Se debe establecer procedimientos para la vinculación de los servidores públicos a la Corporación.

La información del personal a contratar para los cargos de la Corporación se debe manejar de acuerdo con la reglamentación pertinente sobre la privacidad de la información y tratamiento de datos personales.

7.1.2 Términos y condiciones del empleo

Toda vinculación laboral formalizada por la Corporación será determinada de acuerdo con la normatividad vigente.

Se establecerá acuerdos de confidencialidad para el manejo y acceso de la información.

Los servidores públicos responsables del manejo de la información deben cumplir las políticas y procedimientos relacionados con la Seguridad de la información.

7.2 Durante la ejecución del empleo

7.2.1 Responsabilidades de la dirección

La dirección establece las políticas de Seguridad de la Información, las cuales son de obligatorio cumplimiento por los servidores públicos y terceros que tengan acceso a la información de la Corporación.

7.2.2 Toma de conciencia, educación y formación en Seguridad de la Información

La Corporación, debe asegurar que todos los funcionarios, contratistas y/o terceros con acceso al manejo de la información, reciban la capacitación y sensibilización sobre las Políticas de Seguridad de la Información.

La Corporación, debe asegurar que todos los Servidores públicos que tengan definidas responsabilidades de Seguridad de la Información, sean competentes para desempeñar sus funciones y que cuenten con la capacitación y entrenamiento requeridos para ello.

7.2.3 Proceso Disciplinario

Dentro de la estrategia de seguridad de la información, La Corporación, seguirá el proceso establecido en la Ley 734 de 2002 y la Ley 1952 de 2019, para investigar a los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información.

El proceso disciplinario también se debe utilizar como medida preventiva para evitar que los funcionarios, contratistas y los otros colaboradores de la Corporación violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad sin justificación alguna.

El adelantamiento de los procesos disciplinarios corresponde a la Dirección de Control Disciplinario Interno y de la Procuraduría General de la Nación, de acuerdo con las competencias señaladas en la ley.

Actuaciones que conllevan a la violación de la seguridad de la información en la Corporación, son entre otras:

- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, “documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada)”.
- No guardar la información digital, producto del procesamiento de la información perteneciente a la Corporación.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.

- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la Entidad.
- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Utilizar equipos electrónicos o tecnológicos desatendidos o a través de sistemas de interconexión inalámbrica, que sirvan para transmitir, recibir y almacenar datos.
- Permitir el acceso de funcionarios a la red corporativa, sin la autorización de La Oficina de Tecnologías de la Información y las Comunicaciones - OTIC de La Corporación.
- Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos por La Corporación o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la Corporación.
- No cumplir con las actividades designadas para la protección de los activos de información de la Corporación.
- Destruir o desechar de forma incorrecta la documentación institucional.
- Descuidar documentación con información pública reservada o clasificada de la Entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
- Registrar información pública reservada o clasificada, en pos-it, apuntes, agendas, libretas, etc., sin el debido cuidado.
- Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca a la Corporación o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de la Corporación, sin la debida autorización.
- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de la Corporación Autónoma Regional de Cundinamarca – CAR para beneficio personal.

- El que sin autorización acceda en todo o parte del sistema informático o se mantenga dentro del mismo en contra de la voluntad de la Corporación.
- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones de la Corporación, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de la Corporación.
- El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de la Corporación.
- El que viole datos personales de las bases de datos de la Corporación.
- El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por la Corporación.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la Corporación o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la Corporación a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de la Corporación
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
- Sustraer de las instalaciones la Corporación, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o Entidades no autorizadas.
- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de la Corporación, para traslado, reasignación o para disposición final.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la Corporación o de alguno de sus funcionarios.
- Realizar cambios no autorizados en la plataforma tecnológica de la Corporación.
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC de la Corporación.
- Copiar sin autorización los programas de la Corporación, o violar los derechos de autor o acuerdos de licenciamiento.

7.3 Terminación y cambio del empleo

7.3.1 Terminación o cambio de responsabilidades de empleo

Es deber de todo servidor público, que labore en la Corporación, al dejar de prestar sus servicios, debe entregar toda la información producto del trabajo realizado, conforme lo dicta el documento que lo vincula formalmente con la Corporación. Una vez retirado, debe comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la Corporación, directamente o a través de terceros.

Todos los privilegios para el uso de los sistemas de información de la Corporación deben terminar inmediatamente después de que el servidor cesa de prestar sus servicios a la Corporación.

8 GESTIÓN DE ACTIVOS

8.1 Responsabilidad por los activos

8.1.1 Inventario de activos

La Corporación, mantiene un inventario actualizado de sus activos de información, quedando bajo la responsabilidad de cada propietario de información y centralizado por La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

8.1.2 *Propiedad de los Activos*

La Corporación, es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de la Corporación (denominados “usuarios”) que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).

La Corporación, es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

8.1.3 Uso aceptable de los activos

La Entidad implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones.

Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, fotos y cualquier tipo de archivo que no sean de carácter institucional.

Los usuarios deben usar los equipos de manera adecuada y responsable, no podrán realizar cambios relacionados con la configuración del equipo (hardware y software), tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo.

8.1.4 Devolución de los activos

Es deber de todo servidor público, contratista y/o pasante que labore en la Corporación, al dejar de prestar sus servicios, entregar toda información del producto del trabajo realizado y hacer entrega de los equipos y recursos tecnológicos en perfecto estado, conforme al procedimiento establecido para los funcionarios y para los contratistas y pasantes de acuerdo con las condiciones establecidas en el contrato o convenio. Una vez retirado, debe comprometerse a no utilizar, comercializar o divulgar la información generada o conocida durante la gestión en la Corporación, directamente o a través de terceros.

8.2 Clasificación de la Información

8.2.1 Clasificación de la información

La Corporación, consiente de la necesidad de asegurar que la información reciba el nivel de protección apropiado, establecerá los lineamientos para la clasificación de la información de acuerdo con lo establecido por la ley,

Los usuarios responsables de la información de la Corporación deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

8.2.2 Etiquetado de la Información

Se deben desarrollar lineamientos o guías para el Etiquetado y Manejo de la Información, de acuerdo con el esquema de clasificación definido por la Corporación.

8.2.3 Manejo de Activos

Se deben desarrollar procedimientos o guías o lineamientos, para el manejo de activos de la Información, de acuerdo con el esquema de clasificación definido por la Corporación. Así mismo se debe considerar su procesamiento y almacenamiento.

Se deben determinar restricciones de acceso de los activos de información de acuerdo a su nivel de clasificación.

8.3 Manejo de los medios

8.3.1 Gestión de medios removibles

Se deben desarrollar un procedimiento o guía o lineamientos, para el uso de medios removibles, teniendo en cuenta la clasificación de la información realizada por la Corporación.

La Corporación se reserva el derecho de restringir el uso de medios removibles. Mientras esté permitido, es responsabilidad de los usuarios que el medio removible conectado esté libre de virus y/o código malicioso, que pueda poner en riesgo la Integridad, confidencialidad y disponibilidad de la información y de los recursos tecnológicos de la Corporación

8.3.2 Disposición de los medios

Se deben desarrollar procedimientos o guías o lineamientos, para la disposición segura de los medios que contengan información corporativa y que no se encuentren en uso.

8.3.3 Transferencia de medios físicos

La Corporación establece mecanismos seguros, que permitan proteger la información contra acceso no autorizado, uso indebido o corrupción durante el transporte, ya sea directamente o a través de terceros.

9 CONTROL DE ACCESO

9.1 Requisitos del negocio para control de acceso

9.1.1 Política de control de acceso

El acceso a los activos de información de la Corporación estará permitido únicamente a los usuarios autorizados, de acuerdo con los roles y permisos asignados.

El funcionario que disponga de usuario(s) de acceso a los activos de información, será responsable de su uso, el cual es personal e intransferible.

9.1.2 Acceso a redes y a servicios en red

Asegurar la operación correcta y segura de los puntos de red.

La conexión remota a la red de área local de la Corporación debe realizarse a través de una conexión VPN segura suministrada por la Entidad, la cual debe ser aprobada, registrada, por La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC

Las direcciones internas, configuraciones e información relacionada con la topología y diseño de los sistemas de comunicación y redes de la entidad serán restringidas, de tal forma que no sean conocidas por usuarios internos, clientes o personas ajenas a la entidad sin la previa autorización de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

Todas las conexiones a redes externas que accedan a la red interna de la Entidad pasarán a través de un punto adicional de control como: firewall, Gateway, o servidor de acceso.

Los usuarios que tengan acceso a direcciones IP públicas no pueden establecer conexiones a redes de acceso a información privadas, a menos que hayan sido aprobadas por la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

La administración remota de equipos o de la infraestructura de cómputo debe dejar evidencia escrita de la justificación por las que se asigna, al igual que de la responsabilidad que tiene el funcionario a quien se otorga este permiso, dicha solicitud debe ser realizada

por el jefe del Área correspondiente y debe ser avalada por la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

9.2 Gestión de acceso de usuarios

9.2.1 Registro y cancelación del registro de usuarios

La oficina de Tecnologías de la Información y las Comunicaciones debe desarrollar un procedimiento o guía o lineamientos, para el registro y cancelación del registro de usuarios, así mismo, habilitar y deshabilitar el acceso a los sistemas de información y servicios de red.

9.2.2 Suministro de acceso de usuarios

El acceso de usuarios será autorizado por la Oficina de Tecnologías de la información, con el fin de prevenir el acceso de usuarios no autorizados a los sistemas de información e infraestructura Tecnológica, el cual se realizará mediante un procedimiento o guía o lineamientos.

Ningún usuario deberá acceder a la red o a los servicios TIC de la Corporación, utilizando una cuenta de usuario o clave de otro usuario.

Es responsabilidad del usuario cualquier acción que realice en el uso de las cuentas y claves asignadas.

La Corporación suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

9.2.3 Gestión de derechos de acceso privilegiado

La oficina de Tecnologías de la Información y las Comunicaciones debe desarrollar un procedimiento o guía o lineamientos, para el registro y cancelación del registro de usuarios privilegiados.

La Corporación, a través de la Oficina de Tecnologías de la Información y las comunicaciones, protegerá los recursos de la infraestructura tecnológica, servicios de red, y sistemas de información, para que sean operados y administrados en condiciones

controladas y de seguridad, que permitan un seguimiento de las actividades de los usuarios administradores de los privilegios sobre los recursos tecnológicos y sistemas de información.

La Ofician de Tecnologías de la Información y las comunicaciones, es la encargada de restringir las conexiones remotas a los recursos tecnológicos; solamente, se deben permitir a estos accesos a personal autorizado, de acuerdo con las funciones establecidas.

9.2.4 Gestión de información de autenticación secreta de usuarios

La oficina de Tecnologías de la Información y las Comunicaciones debe desarrollar un procedimiento o guía o lineamientos, para la gestión de autenticación secreta de usuarios.

Los usuarios son los responsables de mantener la confidencialidad de la información de autenticación secreta personal, siendo responsabilidad de cada usuario velar por la confidencialidad de la información que está protegida como reserva legal o clasificada como confidencial y/o crítica.

9.2.5 Revisión de los derechos de acceso de usuarios

La oficina de Tecnologías de la Información y las Comunicaciones debe desarrollar un procedimiento o guía o lineamientos, para revisión de los derechos de acceso de usuarios

La Corporación, a través de la Oficina de Tecnologías de la Información y las Comunicaciones, velara por que los responsables de los activos de información revisen periódicamente los derechos de acceso asignado, de los usuarios de los sistemas de información o aplicativo a su cargo.

9.2.6 Retiro o ajuste de los derechos de acceso

La Oficina de Tecnologías de la Información y las Comunicaciones, es la encargada de retirar los privilegios de acceso a la información, inactivar las cuentas de usuario de acceso de correo, sistemas de información, bases de datos, y servicios de red a todos los funcionarios, contratista, proveedores o terceros, en el momento de finalización de su contrato, prestación de servicios o convenios.

9.3 Responsabilidades de los usuarios

9.3.1 Uso de información de autenticación secreta

Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.

Los usuarios súper-administradores y sus correspondientes contraseñas a las consolas administrables se dejan en custodia en el área segura donde designe la Entidad, las credenciales allí contenidas deben ser modificadas de manera periódica o cuando amerite.

Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas, de no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

El personal de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del jefe de La Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

Los usuarios y claves de los administradores de sistemas y/o del personal de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC, son de uso personal e intransferible.

El personal de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad de acuerdo con el rol asignado.

9.4 Control de acceso a sistemas y aplicaciones

9.4.1 Restricción de acceso a la información

Las aplicaciones tendrán configuración de usuarios con diferentes niveles de acceso a la información que contiene.

9.4.2 Procedimiento de ingreso seguro

Definir los lineamientos para la configuración de cuentas de usuario y contraseñas a todos los servidores públicos y terceros que tiene acceso a los servicios tecnológicos, servicios de red y sistemas de información, con el fin de asegurar una administración adecuada de las cuentas de usuario y contraseñas.

Está prohibido compartir la cuenta de usuario y contraseña con otros funcionarios, contratistas y/o terceros.

9.4.3 Sistema de gestión de contraseñas

Todo usuario de los sistemas de información deberá tener asignado una cuenta y una contraseña para su utilización, de acuerdo con los estándares que maneja la Oficina de Tecnologías de la Información y las Comunicaciones, previa solicitud de la Oficina de Talento Humano o del jefe Inmediato de cada dependencia.

La cuenta de usuario se protegerá mediante una contraseña o password. El uso de esta es responsabilidad de la persona a la que está asignada, es de carácter personal e intransferible.

En los sistemas de información, se debe establecer el cambio de contraseña, de acuerdo a periodos establecidos.

Las claves o contraseñas deben:

Tener mínimo ocho (8) caracteres alfanuméricos.

La contraseña debe cumplir con tres de los cuatro requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Base de 10 dígitos (0 a 9)
- Caracteres no alfabéticos (Ejemplo: ¡,$, %,&)

9.4.4 Uso de programas utilitarios privilegiados

No se permitirá la instalación y uso de programas utilitarios en los equipos a cargo de los funcionarios y/o contratistas de la CAR, sin previa autorización de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

9.4.5 Control de acceso a códigos fuente de los programas

El acceso al código fuente de las aplicaciones estará restringido solo al personal autorizado, con el fin de evitar el acceso no autorizado e impedir cambios involuntarios y mantener la confidencialidad de propiedad intelectual.

10 CRIPTOGRAFÍA

10.1 Controles criptográficos

10.1.1 Política sobre el uso de controles criptográficos

Implementar actividades para proteger activos de información clasificada y reservada, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.

La Oficina de Tecnologías de la Información y las Comunicaciones OTIC, es la encargada de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de la Entidad. Con base en el análisis de riesgos y considerando los criterios de confidencialidad, integridad y autenticidad de las comunicaciones o en el tratamiento de la información, se adoptan los controles de cifrado y firma digital de datos que reduzcan los riesgos de seguridad de la información. El uso de herramientas de cifrado será autorizado conforme a los roles o responsabilidades de los funcionarios y contratistas de la Entidad.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de cómputo de la Corporación

, sea por cualquier medio tecnológico existente, siempre deberá estar autenticado y sus conexiones deberán estar cifradas.

Con el fin de garantizar la confidencialidad e integridad de los documentos, la Corporación debe utilizar sistemas y técnicas criptográficas para la protección de la información.

En los sistemas de información se deben implementar mecanismos de protección de información que cumplan con la reglamentación, políticas, estándares y guías aplicables.

Proporcionar una protección adecuada a los equipos utilizados para generar, almacenar y archivar claves considerándolos críticos o de alto riesgo y proteger las claves evitando que sean copiadas o modificadas sin autorización.

La Corporación deberá velar porque la información de su custodia o propiedad que es catalogada como reservada o clasificada, se cifre al momento de almacenarse o transmitirse por cualquier medio.

10.1.2 Gestión de llaves

Los usuarios responsables autorizados deberán velar por la conservación de la disponibilidad, integridad y confidencialidad de las llaves criptográficas, así como de la información a la cual se le haya aplicado algún proceso de cifrado. De igual modo, la información cifrada o descifrada deberá ser tratada conforme a su nivel de clasificación y su eliminación deberá realizarse a través de borrado seguro.

Las llaves caducarán en un tiempo máximo de tres meses y deberán ser restablecidas por el usuario.

Las llaves serán deshabilitadas cuando estas tengan riesgo de divulgación o cuando los funcionarios, contratistas y terceros autorizados culminen la relación laboral o contractual con la Entidad.

Los responsables del sistema de cifrado y de las llaves criptográficas serán los encargados de establecer los controles para asegurar el sistema y las llaves, así como gestionar el acceso sólo a los funcionarios, contratistas y terceros autorizados.

Las actividades relacionadas con la administración y eliminación de las llaves criptográficas deberán ser registradas por la persona encargada.

11 SEGURIDAD FÍSICA Y DEL ENTORNO

11.1 Áreas seguras

11.1.1 Perímetro de Seguridad Física

Todas las áreas destinadas al procesamiento, almacenamiento de documentos o información, así como aquellas en las que se encuentren los equipos de cómputo y demás infraestructura de los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. Por tanto, contarán con medidas de control de acceso físico en el perímetro de tal forma que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información.

Identificar todas las salidas de emergencia en caso de escenarios catastróficos en la Corporación.

11.1.2 Controles de acceso físico

Implementar el procedimiento de control de acceso a los centros de datos para garantizar la seguridad física que permita fortalecer la confidencialidad, disponibilidad e integridad de la información.

El Centro de Cómputo debe contener mecanismos de control de acceso, como puertas de seguridad, cerradura, sistemas de control con tarjetas inteligentes, sistema de alarmas o controles biométricos.

El ingreso al centro de cómputo debe estar debidamente registrado en la planilla establecida y debe estar acompañado por el personal autorizado de la Oficina de Tecnologías de la Información y las Comunicaciones- OTIC.

Está totalmente prohibido el acceso de personal no autorizado al centro de cómputo de la Sede Central y de las Direcciones regionales.

11.1.3 Seguridad de oficinas, recintos e instalaciones

La Corporación establecerá las medidas de control de acceso físico a las oficinas de nivel central y direcciones regionales, con el fin de controlar el acceso de personal no autorizado.

11.1.4 Protección contra amenazas externas y ambientales

Las Oficinas e instalaciones de la Corporación, donde se procesa y/o almacena la información, debe contar con sistemas de alarmas, sistema de detección y extinción automáticas de incendios.

Se debe tener aislados los equipos de amenazas potenciales, como fuego, explosivos, agua, polvo, interferencias y vandalismo, entre otros.

Los equipos del centro de cómputo y centros de cableado deben tener control de los niveles de temperatura y humedad.

No se permite el ingreso de comidas, bebidas y fumar dentro de las instalaciones de procesamiento de la información de la Corporación.

11.1.5 Trabajo en áreas seguras

El trabajo en áreas seguras, solo deben ser realizadas por el personal autorizado, y deberán estar vigilado o acompañado por personal responsable de dichas áreas.

11.1.6 Áreas de despacho y carga

Los suministros o materiales que ingresen o salgan de la Corporación, deberán ser revisados y registrados por cada uno de los responsables, para ser resguardados de cualquier amenaza.

11.2 Equipos

11.2.1 Ubicación y protección de los equipos

El centro de cómputo debe contar con la seguridad necesaria de tal forma que personal no autorizado no pueda ingresar, y estará controlado por la Oficina de Tecnología e Información y las Comunicaciones.

Una vez entregado al usuario final el equipo de cómputo, este será el responsable del cuidado del equipo asignado y será registrado en el aplicativo de mesa de ayuda.

La Oficina de las Tecnologías de la Información y las Comunicaciones, será la encargada de programar y autorizar el mantenimiento y/o reparación de los equipos de cómputo de la Corporación.

11.2.2 Servicios de Suministro

La Corporación, debe poseer la infraestructura necesaria, con el fin de actuar contra eventos que pongan en riesgo los equipos de cómputo. Se debe tener instalaciones eléctricas de corriente regulada.

Contar con un sistema de energía UPS y/o planta eléctrica, para asegurar el funcionamiento ininterrumpido de los equipos de cómputo de la Corporación, garantizando la continuidad de los servicios, mientras se restablecen las fallas de energía eléctrica.

11.2.3 Seguridad del Cableado

Asegurar la protección del cableado de energía eléctrica, de telecomunicaciones e infraestructura de red, para evitar el daño o interceptación de comunicaciones.

Los tableros de control y los centros de cableado deben estar protegidos contra acceso no autorizado.

En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

- Fumar dentro del Data Center.
- Introducir alimentos o bebidas al Data Center
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.

Los centros de cómputo deben mantener las condiciones físicas y ambientales óptimas recomendadas, y cuando sea posible controles automáticos para incendio, temperatura, monitoreo por Circuito Cerrado de Televisión.

11.2.4 Mantenimiento de Equipos

La oficina de Tecnologías de la Información y las Comunicaciones debe desarrollar un procedimiento o guía o lineamientos, para llevar a cabo el mantenimiento correctivo y preventivo de los equipos.

La Oficina de las Tecnologías de la Información y las Comunicaciones, es la responsable de autorizar el mantenimiento y/o reparación de los equipos de cómputo y redes de datos.

Los trabajos de mantenimiento de redes eléctricas, cableado de datos y voz, deben ser realizados por personas especializadas y debidamente autorizadas.

La mesa de servicios debe establecer un cronograma de mantenimiento preventivo, el cual debe ser comunicado a los usuarios.

11.2.5 Retiro de activos

En caso de retirar los equipos de la sede principal o de las regionales, se debe cumplir con el proceso de gestión de apoyo logístico y su respectivo diligenciamiento en el formato establecido para tal fin, con la previa autorización de los jefes o directores.

La Entidad establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por la Corporación, velando por la disponibilidad y confidencialidad de la información.

11.2.6 Seguridad de equipos y activos fuera de las instalaciones

El servidor público que está autorizado para retirar un equipo de cómputo debe asumir el control de protección del equipo y de la información fuera de las instalaciones de la Corporación.

En caso de pérdida o robo de un equipo de la Corporación, el responsable debe colocar la denuncia ante la autoridad competente e informar al jefe inmediato para que se inicie el trámite interno correspondiente.

11.2.7 Disposición segura o reutilización de equipos

Establecer un procedimiento, o lineamientos para la reutilización de los equipos de cómputo de la Corporación.

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información, y realizar el borrado seguro de acuerdo con lo establecido en los lineamientos, o procedimiento, o guía determinado para ello.

11.2.8 Equipos de usuario desatendido

Los equipos de cómputo de la Corporación deben ser bloqueados y/o apagados tras abandonar el puesto de trabajo o al terminar la jornada laboral.

Se deben establecer políticas en el servidor de dominio para bloquear las pantallas de los equipos en un determinado tiempo de inactividad.

11.2.9 Política de escritorio limpio y pantalla limpia

Los funcionarios, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con la Corporación, deben conservar su escritorio limpio (pantallas, tableros, etc.) libre de información, propia de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD, USB, unidades de disco externas, etc.

Al imprimir documentos con información pública reservada y/o pública clasificada, deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

12 SEGURIDAD DE LAS OPERACIONES

12.1 Procedimientos operacionales y responsabilidades

12.1.1 Procedimientos de operación documentados

Definir las reglas para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de la Corporación, con el fin de robustecer la continuidad de los sistemas de TIC.

Se definirán procedimientos, registros e instructivos de trabajo debidamente documentados, los cuales serán progresivamente implementados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica.

Cada procedimiento tendrá un responsable para su definición, mantenimiento e implementación.

12.1.2 Gestión de Cambios

Al realizar cambios en los sistemas de información, se debe llevar un control de cambios que garantice la actualización realizada.

En caso de realizar cambios de emergencia, al hacerlo se debe reportar y evaluar la pertinencia del cambio.

Todo procedimiento, formato, guía, etc, que se actualice, o modifique dentro de la Oficina de Tecnologías de la Información y las Comunicaciones, deberá tener su respectivo control de cambios, y deberá ser publicado en el Sistema de Gestión Pública – SIGESPU.

12.1.3 Gestión de capacidad

La Corporación, a través de la Oficina de Tecnologías de la Información y las comunicaciones deberá implementar el plan de gestión de la capacidad acuerdo con los lineamientos establecidos.

12.1.4 Separación de los ambientes de desarrollo, prueba, y operación

Para la gestión de las operaciones de la infraestructura de procesamiento de información en la Corporación, la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC, con el apoyo de las áreas, establecerá mecanismos que permitan segregar las funciones de administración (sistemas operativos, bases de datos y aplicaciones), monitoreo y operación, separando entre estos los diferentes ambientes de desarrollo, pruebas y producción.

12.2 Protección contra códigos maliciosos

12.2.1 Controles contra códigos maliciosos

La Corporación debe tener actualizada las licencias de antivirus para evitar la descarga de código malicioso en los equipos institucionales, así mismo, controlar el acceso a la información contenida en las plataformas de almacenamiento.

Los servidores públicos de la Corporación, no deben descargar archivos que puedan ser nocivos para los sistemas como virus, software espía, programas maliciosos capaces de alojarse en computadores permitiendo el acceso a usuarios externos y atacantes que pongan en riesgo la seguridad de la información, así mismo, no deben acceder a sitios desconocidos o de baja confianza, ni aceptar los mensajes sobre instalación de software que ofrezcan las diferentes páginas sin la debida autorización de la Oficina de Tecnologías de la Información y las Comunicaciones

12.3 Copias de respaldo

12.3.1 Respaldo de la información

La Corporación debe establecer un procedimiento, o lineamientos para la Administración de Backup; y proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando

que la información y la infraestructura de software crítica de la Entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos establecida por la Entidad.

Semanalmente los administradores de la plataforma de backups de la Corporación verificarán la correcta ejecución de los procesos de backups, suministrarán las cintas requeridas para cada trabajo y controlarán la vida útil de cada cinta o medio empleado.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

El administrador de la plataforma de backups de la Entidad, deben generar tareas de restauración aleatorias de la información y deben ser documentadas.

La información previamente definida y contenida en los servidores de la Corporación, se respaldará de forma periódica, determinada según el procedimiento " Administración de Backups " y los medios que se consideren necesarios se almacenarán en una custodia externa que cuente con mecanismos de protección ambiental como detección de humo, incendio, humedad y mecanismos de control de acceso físico. Adicionalmente, se realizarán pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad.

Todos los usuarios son responsables de realizar copias de respaldo del original de la información de valor, confidencial o crítica a su cargo. Estas copias deben ser efectuadas con la periodicidad requerida de acuerdo con los cambios que se presenten en la información.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

12.4 Registro y seguimiento

12.4.1 Registro de eventos

La Corporación debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC será la encargada de realizar la investigación y seguimiento a los eventos e incidentes de seguridad reportados.

12.4.2 Protección de la información de registro

La Oficina de Tecnología de la Información y las Comunicaciones, debe implementar mecanismos con el fin de proteger la información de acceso no autorizado.

12.4.3 Registros del administrador y del operador

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 al cual solo debe tener acceso el personal autorizado de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

Los administradores de los sistemas de información de la Corporación deben establecer mecanismos para la protección de los registros de información.

12.4.4 Sincronización de relojes

La Corporación debe sincronizar los relojes de todos los sistemas de tratamiento de información con una única fuente de tiempo acordada.

12.5 Control de software operacional

12.5.1 Instalación de software en sistemas operativos

La Corporación debe establecer un procedimiento, o lineamientos para la instalación de software en los sistemas operativos

Todo software nuevo y actualizaciones debe estar completamente soportados y documentado, no debe ser puesto en el ambiente de producción sin contar con la debida documentación.

12.6 Gestión de la vulnerabilidad técnica

12.6.1 Gestión de las vulnerabilidades técnicas

Identificar las vulnerabilidades técnicas potenciales, la Corporación, identificará los riesgos asociados y los controles de seguridad a ser tenidos en cuenta (esta acción puede implicar la actualización de sistemas vulnerables y/o aplicación de las medidas de acción necesarias).

La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas

Una vez se lleve a cabo el análisis de vulnerabilidades y/o Hacking Ético, se realizará un informe detallado y se establecerá un plan para establecer las correcciones necesarias de acuerdo con la identificación de dichas vulnerabilidades.

12.6.2 Restricciones sobre la instalación de software

Está prohibido la instalación de software no licenciado, a excepción de software libre que deberá ser autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

La instalación de software solo estará habilitada por los usuarios administradores. Si un usuario necesita instalar software en equipos de la entidad para el cumplimento de sus deberes, debe ser solicitado a la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC para su evaluación y viabilidad.

Ningún usuario podrá desinstalar software previamente instalado en los equipos de cómputo de la Corporación. Esta actividad será solicitada por cada dependencia a la Oficina de tecnologías de la información y la Comunicaciones - OTIC.

Está prohibida la transferencia de software desarrollado por la Corporación a usuarios particulares.

La transferencia de software desarrollado por la Corporación a otras entidades del estado deberá estar autorizado por la dirección de la Corporación.

Los responsables de la administración de las plataformas de producción estarán obligados a controlar el acceso y uso de los programas fuente, el acceso a los archivos de los sistemas y/o a las aplicaciones que operan en ellas, así como a la programación de las actualizaciones necesarias a realizar.

No se permitirá el uso de versiones de software en los sistemas de producción que no sean soportadas por los fabricantes, ni versiones de prueba que no hayan sido liberadas al mercado (Beta), a menos que sea autorizado la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

No se permitirá la instalación de herramientas de desarrollo ni programas fuente en los sistemas de producción, a menos que sea autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC.

12.7 Consideraciones sobre auditorias de sistemas de información

12.7.1 Controles de auditorías de sistemas de información

Los accesos a sistemas de información para auditorias deben acordarse con el jefe de la Oficina de la Tecnologías de la Información y las Comunicaciones.

Los accesos a los sistemas de información para auditorias deben tener permisos de solo lectura.

Todos los archivos de auditorías deben proporcionar suficiente información para apoyar el monitoreo, control y seguimiento que se requiera y preservarse por períodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

13 SEGURIDAD DE LAS COMUNICACIONES

13.1 Gestión de la seguridad de las redes

13.1.1 Controles de redes

La Corporación debe implementar procedimiento, lineamientos y mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento de la Corporación.

Se debe realizar monitoreo y registro de eventos a las redes y canales de comunicación que permitan detectar acciones que puedan afectar la continuidad del servicio y la seguridad de la información.

13.1.2 Seguridad de los servicios de red

La Oficina de Tecnologías de la Información y las Comunicaciones, establecerá los acuerdos de servicio de red y canales de comunicación, con el fin de garantizar los acuerdos de niveles de servicio y requisitos de gestión.

La Entidad permite el acceso al servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

Los usuarios de los activos de información de la Corporación tienen restringido el acceso a redes sociales, sistemas de mensajería instantánea y acceso a sistemas de almacenamiento en la nube. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud al jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC, para que sea autorizado.

13.1.3 Separación en las redes

La infraestructura tecnológica de la Corporación, que soporta aplicaciones debe estar separada en segmentos de red físicos y Lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La separación de estos segmentos debe ser realizada por medio de elementos de conectividad perimetrales e internos de enrutamiento y de seguridad.

13.2 Transferencia de información

13.2.1 Políticas y procedimientos de transferencia de información

La Corporación debe establecer mecanismos para proteger la información transferida de interceptación, copia, modificación, errores de enrutamiento y destrucción.

13.2.2 Acuerdos sobre transferencia de información

La Corporación debe generar acuerdos entre las partes cuando se requiera intercambio de la información para asegurar el manejo de la información y el nivel de protección de esta.

Las partes relacionadas en los acuerdos de intercambio de la información deben establecer la responsabilidad de las partes en el manejo, tratamiento y divulgación de la información, deben determinar la trazabilidad de la información, el cumplimiento de las normas técnicas y legales, y establecer las responsabilidades en la cadena de custodia, de acuerdo con lo establecido por la ley.

13.2.3 Mensajería electrónica

El sistema generador de documentos electrónicos de la Corporación es el Sistema de Información Documental de la CAR – SIDCAR.

Para garantizar la integridad y autenticidad de los documentos generados en el sistema de gestión documental SIDCAR, se utilizará el estampado electrónico y la firma digital Corporativa, servicios que serán contratados con firmas autorizadas y certificadas.

Los documentos generados o cargados al Sistema de Gestión Documental deben incorporar condiciones de seguridad mediante la utilización del formato PDF/A.

Los documentos generados electrónicamente deben tener un número consecutivo de radicado generado automáticamente por el Sistema de Gestión de Documentos Electrónicos.

Las firmas digitales adquiridas por la CAR y asignadas a los directores, jefes y/o autorizados, son personales e intransferibles y sólo se pueden utilizar para firma de documentos pertinentes a la Corporación.

Una vez terminado el vínculo laboral del director, jefe o autorizado, la firma electrónica será cancelada.

Todas las comunicaciones externas que se envíen por correo electrónico deberán ser enviadas a través de correo electrónico certificado institucional a través de SIDCAR.

El sistema debe contar con metadatos que garanticen las búsquedas, roles, controles, recuperación, acceso y administración de la información y documentación electrónica generada.

Los cambios, adiciones y/o modificaciones que se requiera hacer al Sistema De Gestión Documental SIDCAR, serán aprobados y solicitados por el área de Gestión Documental de la Dirección Administrativa y Financiera.

Establecer estrategias de preservación digital para garantizar que la información almacenada pueda permanecer en el futuro, pese a los cambios tecnológicos u otras

causas que puedan alterar la información que contiene, manteniendo su confidencialidad, integridad y disponibilidad.

Los lineamientos y directrices para la conformación de expedientes híbridos y digitalización de documentos se establecerán en el Manual de Gestión Documental de la entidad.

Los Manuales, instructivos, procesos y procedimientos se verificarán y ajustarán de manera periódica, con el fin de garantizar la preservación digital de los documentos

Se prohíbe enviar o reenviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y/o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

La cuenta de correo electrónico deberá ser usada para el desempeño de las funciones asignadas dentro de la Corporación.

Los mensajes y la información contenida en los buzones de correo son de propiedad de la Corporación. El usuario podrá crear un histórico de su correo siempre y cuando sea almacenado en el disco duro del usuario y bajo su propia responsabilidad.

La Corporación, define las pautas generales para asegurar una adecuada protección de la información, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la Corporación, que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instagram, etc., se considera fuera del alcance de las políticas establecidas y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales que sea originada por la Entidad debe ser autorizada por los directores o jefes de área para ser socializadas y con un vocabulario institucional.

El nombre de la entidad en las redes sociales no puede ser utilizado para difamar o afectar la imagen y reputación de las personas que no están de acuerdo o estén en contra de la CAR por información publicada.

13.2.4 Acuerdos de confidencialidad o de no divulgación

Todo servidor público y/o terceros que utilice los recursos tecnológicos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como publica clasificada o publica reservada.

Los funcionarios, contratista, pasantes y proveedores deben firmar acuerdos o compromisos de confidencialidad, para el manejo de la información que conozca durante su vinculación laboral o contractual.

14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

14.1 Requisitos de seguridad de los sistemas de información

14.1.1 Análisis y especificación de requisitos de seguridad de la información

Establecer un procedimiento, o lineamientos para el aseguramiento de la calidad en el desarrollo de proyectos de Software, el cual debe ser aplicado a toda solicitud, requerimiento, desarrollo, adquisición de software que serán revisados, validados y liderados por la Oficina de las Tecnologías de la Información y las Comunicaciones – OTIC.

El desarrollo de tecnologías informáticas se debe orientar sobre herramientas basadas en tecnologías de última generación, que permitan la portabilidad y escalabilidad de las aplicaciones.

La supervisión y seguimiento a proyectos de infraestructura informática deben incorporar como un elemento básico de la supervisión, el cumplimiento de la aplicación de políticas de seguridad tanto en el desarrollo de la solución como en el producto final que será entregado a la Entidad.

Los desarrollos de software deben involucrar la correspondiente documentación interna y externa que permitan identificar su seguimiento hasta el nivel de rutinas y procedimientos

Todos los desarrollos de software, adquisición de sistemas de información y adquisición de equipos de cómputo, deberán ser aprobados por la Oficina de las Tecnologías de la Información y las Comunicaciones - OTIC.

14.1.2 Seguridad de servicios de las aplicaciones en redes públicas

La Corporación debe garantizar la seguridad de la información de los diferentes aplicativos disponibles a través de redes públicas, con el fin de evitar vulnerabilidades de seguridad amenazas, modificación y acceso no autorizado.

14.1.3 Protección de transacciones de los servicios de las aplicaciones

Toda la información transmitida debe estar cifrada garantizando la confidencialidad de la misma, evitando la alteración, divulgación o duplicación no autorizada.

14.2 Seguridad en los procesos de desarrollo y de soporte

14.2.1 Política de desarrollo seguro

La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC define los procedimientos y reglas básicas para tener en cuenta en el desarrollo seguro de software dentro de la Corporación, estableciendo lineamientos para realizar una programación segura en los nuevos desarrollos y actualizaciones de software, acorde a la necesidad de las partes interesadas.

14.2.2 Procedimiento de control de cambios en sistemas

La Corporación debe establecer e implementar procedimientos para el control de cambios, para requerimientos de actualización, modificación o nuevas funcionalidades a los sistemas de información en producción.

Para el control de cambio se debe tener en cuenta:

- Establecer un proceso técnico documentado para llevar o realizar los cambios
- Realizar las diferentes pruebas de calidad sobre los cambios establecidos.
- Realizar la correspondiente evaluación de riesgos antes de realizar los cambios
- Verificar los requisitos de seguridad a los diferentes sistemas al implementar los cambios
- Aprobación de los cambios realizados a los sistemas de información
- Determinar controles y restricciones de acceso a los sistemas de información.

14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

Al realizar cambios en las plataformas de operación se debe garantizar la continuidad y funcionamiento de las aplicaciones o sistemas de información, mediante la realización de pruebas a los mismos.

14.2.4 Restricciones en los cambios a los paquetes de software

Toda solicitud de cambio, actualización a los aplicativos o sistemas de información debe ser analizada y evaluada por el grupo de desarrollo para establecer la viabilidad del requerimiento.

14.2.5 Principios de construcción de los sistemas seguros

La Corporación debe establecer un procedimiento, o lineamientos para el aseguramiento de la calidad en el desarrollo de proyectos de software para la construcción de sistemas seguros.

14.2.6 Ambiente de desarrollo seguro

La Corporación debe desarrollar e implementar una guía, o lineamientos de políticas de desarrollo seguro, donde se establezca ambientes de prueba y producción.

Definir una metodología ágil para el desarrollo de software en la Corporación, con el fin de asegurar el éxito de los proyectos de software emprendidos, mediante el procedimiento establecido.

14.2.7 Desarrollo contratado externamente

La Oficina de Tecnologías de la Información y las Comunicaciones, será quien define y/o aprueba los requerimientos de desarrollos tercerizados.

La Oficina de Tecnologías de la Información y las Comunicaciones apoyará la supervisión de los desarrollos contratados externamente.

14.2.8 Pruebas de seguridad de sistemas

Todos los desarrollos de software deben surtir una fase de pruebas de funcionalidad en la cual se evidencien los controles establecidos en relación con la integridad de la información que será ingresada una vez se lleve a cabo su implementación

No deberán realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información. Así mismo, en los ambientes de desarrollo y calidad si se llegaran a utilizar datos reales del ambiente de producción, se debe definir el protocolo de seguridad que permita salvaguardar la integridad de la información

14.2.9 Pruebas de aceptación de sistemas

La actualización e incorporación de nuevos sistemas o nuevo software debe estar sujeto a un proceso de pruebas funcionales y de seguridad, con el fin de establecer el cumplimiento y aceptación de lo requerido.

14.3 Datos de prueba

14.3.1 Protección de datos de prueba

La Oficina de Tecnologías de la Información y las Comunicaciones debe establecer los lineamientos de selección y control para la utilización de datos de prueba.

15 RELACIÓN CON LOS PROVEEDORES

15.1 Seguridad de la información en las relaciones con los proveedores

15.1.1 Política de seguridad de la información para las relaciones con proveedores

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la Entidad.

Se deben establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de la Corporación, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a la Corporación. El resultado del análisis de riesgos será la base para el establecimiento de los controles en la matriz de riesgo, que se definirá en el proyecto de pliegos del contrato.

15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores

La Corporación acordará con los proveedores el acceso y gestión de la información estableciendo los requisitos de la seguridad de la información.

Los proveedores y/o contratistas solo podrán tener acceso a los activos de información necesarios para el desarrollo de sus obligaciones contractuales.

El acceso de proveedores y/o contratistas a los sistemas de información estará definido por usuario y contraseña el cual tendrá el nivel de acceso requerido para el desarrollo de sus obligaciones contractuales.

Los proveedores y/o contratistas al dejar de prestar sus servicios a la Corporación, deben entregar toda información del producto del trabajo realizado y hacer entrega de los equipos y recursos tecnológicos en perfecto estado, de acuerdo con las condiciones establecidas en el contrato o convenio. Una vez terminada la relación contractual, debe comprometerse a no utilizar, comercializar o divulgar la información generada o conocida durante la gestión en la Corporación, directamente o a través de terceros.

15.1.3 Cadena de suministro de tecnología de información y comunicación

En los procesos contractuales se deben incluir los requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios tecnología de la información y comunicación.

15.2 Gestión de la prestación de servicios de proveedores

15.2.1 Seguimiento y revisión de los servicios de los proveedores

Los funcionarios de la Corporación, que ejercen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

15.2.2 Gestión de cambios en los servicios de los proveedores

Tramitar los diferentes cambios en el suministro de los servicios por parte de los proveedores, (mantenimiento, procedimientos y controles de la seguridad de la información), de acuerdo con la necesidad y criticidad de la información y sistemas de información de la Corporación.

Realizar seguimiento y actualización de los riesgos respecto a la seguridad de la información.

Se debe tener en cuenta:

- Cambios o mejoras de los servicios en las aplicaciones ofrecidos por el proveedor
- Uso de nuevas herramientas
- Modificaciones o actualizaciones en las políticas de seguridad de la información de la Corporación.
- Implementación de controles para resolver incidentes de seguridad de la información.

16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1 Gestión de incidentes y mejoras en la seguridad de la información

16.1.1 Responsabilidades y procedimientos

Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de ejecutar oportunamente las acciones correctivas.

Realizar capacitaciones de sensibilización periódicas a todos los servidores públicos de la Corporación para que conozcan las rutas de atención a incidentes en la seguridad de la información.

16.1.2 Reporte de eventos de seguridad de la información

Todo incidente de seguridad que se observe debe ser reportado mediante la mesa de ayuda de TI, para hacer el respectivo seguimiento por parte del La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC. El resultado del seguimiento será informado al usuario, especificando las causas, consecuencias, responsabilidades, solución y acciones para evitar que se presenten nuevamente.

16.1.3 Reporte de debilidades de seguridad de la información

Los funcionarios y contratistas de la Corporación deberán informar inmediatamente a la Oficina de las Tecnologías de la Información y las Comunicaciones – OTIC, cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.

16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos

Los eventos e incidentes de seguridad de la información presentados deben ser evaluados de acuerdo con el procedimiento establecido para la Gestión de Incidentes de Seguridad de la Información, con el fin de clasificar e identificar los incidentes que no correspondan a la seguridad de la información,

16.1.5 Respuesta a incidentes de seguridad de la información.

Se debe dar respuesta a todo evento catalogado como incidente de seguridad, incluyendo el tratamiento a las debilidades o causas que generaron el incidente o evento de seguridad de la información, con su respectiva solución y acciones para evitar que se presenten nuevamente.

16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información

Se debe documentar el manejo y solución dado a los incidentes de seguridad de la información, creando una base de conocimiento que se pueda utilizar para el tratamiento de nuevos incidentes.

16.1.7 Recolección de evidencia

Aplicar el procedimiento establecido para la gestión de incidentes de seguridad de la información, de manera que se pueda evidenciar el manejo de los incidentes, los cuales deben permanecer en un repositorio.

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

17.1 Continuidad de seguridad de la información

17.1.1 Planificación de la continuidad de la seguridad de la información

La Oficina de Tecnologías de la Información y las Comunicaciones debe establecer el análisis de los requisitos de seguridad de la información, incluyendo las necesidades de la seguridad de la información en las situaciones de emergencia o desastres.

17.1.2 Implementación de la continuidad de la seguridad de la información.

Se debe desarrollar e implantar un plan de continuidad para asegurar que los procesos misionales de TI de la Corporación podrán ser restaurados dentro de escalas de tiempo razonables.

La Corporación, deberá tener definido un plan que permita mantener la continuidad de servicios de TI teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de TI de la Corporación, de acuerdo con su impacto en el cumplimiento de la misión de la Entidad.
- Documentación del plan de recuperación de TI de acuerdo con la estrategia definida anteriormente.
- Realizar las pruebas de recuperación.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

La Oficina de Tecnologías de la Información y las comunicaciones debe revisar periódicamente los documentos correspondientes al plan de continuidad (controles, tareas de recuperación, etc) y realizar las pruebas de recuperación para verificar su validez y su eficacia.

17.2 Redundancias

17.2.1 Disponibilidad de instalaciones de procesamiento de información

La Corporación, debe asegurar que la información y los sistemas de información se encuentren respaldados y almacenados en diferentes sitios, con el fin de garantizar pérdida o daño de los datos.

18 CUMPLIMIENTO

18.1 Cumplimiento de los requisitos legales y contractuales

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Se debe identificar y aplicar la normatividad vigente, para cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales.

18.1.2 Derechos de propiedad intelectual

La Corporación, respeta y acata las normas legales existentes relacionadas con protección de derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, garantizará que todo el software que se ejecute en los activos de información de la Corporación esté protegido por derechos de autor y requiera licencia de uso o sea software de libre distribución y uso.

18.1.3 Protección de registros

Realizar y conservar un análisis de los registros (bases de datos, registros de auditoría, registros documentales, y todos los registros generados por la entidad), para proteger y evitar la pérdida, destrucción, adulteración, y acceso no autorizado, de acuerdo con los requisitos contractuales y legales, y los contemplados por la Corporación.

La Corporación se obliga a proteger todos los registros que revelen la evidencia del cumplimiento de los requisitos contractuales y legales contra la pérdida de Confidencialidad, Integridad y Disponibilidad, siguiendo los lineamientos del manual de Gestión de Activos.

18.1.4 . Privacidad y protección de información de datos personales

La Corporación realizará el tratamiento de datos personales de acuerdo con la Ley 1581 de 2012 y la Resolución CAR No. 3294 de 2019 “Por la cual se adopta la política de protección de datos personales en la Corporación”.

***18.1.5** . Reglamentación de controles criptográficos*

Se debe establecer procedimientos, lineamientos y/o protocolos, para dar cumplimiento con respecto a los controles criptográficos.

18.2 Revisiones de seguridad de la información

18.2.1 *Revisión independiente de la seguridad de la información*

Se debe realizar la revisión y/o actualización periódica del sistema de gestión de seguridad, con el fin de mantener los controles y asegurar la eficacia en la seguridad de la información.

18.2.2 Cumplimiento con las políticas y normas de seguridad

Se debe establecer mecanismos para que dentro de las áreas de la Corporación, se revisen con regularidad el cumplimiento de las políticas y normas de seguridad de la información, de acuerdo a los documentos establecidos por la Corporación.

18.2.3 Revisión del cumplimiento técnico

La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, debe establecer mecanismos para revisar periódicamente los sistemas de información con herramientas automáticas y especialistas técnicos.

19 ANEXOS

TIC-MN-04-FR-03 Compromiso de Confidencialidad