CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA - CVC

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Santiago de Cali, diciembre de 2019

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. OBJETIVO

1.1. OBJETIVO GENERAL

Establecer lineamientos y comportamientos de seguridad de la información que debe seguir todo el personal de la CVC (funcionarios, contratistas, visitantes y todos aquellos con acceso a la información), con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información y de los activos relacionados.

1.2. OBJETIVOS ESPECÍFICOS

a) Establecer un esquema de seguridad de la información claro, transparente y aplicable bajo la responsabilidad de la CVC para la gestión o administración de riesgos de seguridad de la información.

b) Comprometer a todo el personal de la CVC con el Sistema de Gestión de Seguridad de la Información, agilizando la aplicación de los controles de seguridad de la información con eficacia y eficiencia, generando una cultura de seguridad de la información.

c) Proteger los recursos de información y la tecnología utilizada por La CVC frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2. ALCANCE

El presente manual describe las políticas de seguridad de la información definidas por la CVC, teniendo en cuenta la estrategia de Gobierno en línea de MinTIC, algunos aspectos de la ley estatutaria de protección de datos personales (Ley 1581 de 2012), sus decretos reglamentarios, y demás legislación aplicable, además de la norma técnica NTC - ISO/IEC 27001:2013.

Estas políticas se aplican en todo el ámbito de la CVC, a sus recursos y a la totalidad de los procesos, ya sean internos o externos, vinculados a la Corporación.

Los jefes, funcionarios y contratistas sean cual fuere su nivel jerárquico son responsables de la implementación de estas políticas de seguridad de la información dentro de sus áreas de responsabilidad, así como del cumplimiento de los lineamientos aquí descritos.

Este manual de políticas de seguridad de la información es de carácter particularmente técnico, por lo cual, antes de ser aplicado a un asunto en concreto, previamente deberá ser avalado por el área jurídica de la CVC, o de un profesional del derecho experto en el tema y con la autoridad relevante.

3. DEFINICIONES

El presente documento utiliza las referencias, los términos y definiciones del documento Manual del Sistema de Gestión de Seguridad de la Información, SGSI, así como los términos y definiciones de la norma NTC-ISO/IEC 27001:2013. Entre los cuales se destacan los siguientes:

Activo de Información: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

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

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

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evento de seguridad de la información: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

Incidente de seguridad de la información: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Seguridad de la información: Entiéndase como la preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información. **"**Un Sistema de Gestión de la Seguridad de la Información (SGSI) consiste en las políticas, procedimientos, directrices y recursos y actividades asociados, gestionados colectivamente por una organización, con el fin de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos de negocio. Se basa en una evaluación de riesgos y en los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar los riesgos de forma eficaz. Analizar los requisitos para la protección de los activos de información y aplicar los controles apropiados para asegurar la protección de estos activos de información, según se requiera, contribuye a la implementación exitosa de un SGSI." - ISO/IEC 27000: 2014.

4. DESARROLLO

4.1. GENERALIDADES

El presente manual proporciona las directrices necesarias para el aseguramiento y/o protección de los activos de información, los datos e información corporativa pertenecientes o tratados por la CVC. Las presentes políticas están dirigidas a todos los funcionarios o colaboradores de la CVC, al personal temporal, a contratistas o terceros que prestan servicios (outsourcing) en modalidad in-house u out-house, a clientes, proveedores y toda persona natural o jurídica que de alguna manera realice transacciones, contrataciones y prestación de servicios con la CVC. Para los funcionarios o colaboradores de la CVC la responsabilidad de garantizar su cumplimiento no está solo en ellos, sino también en cada director o jefe de oficina o de Direcciones Ambientales donde deben contribuir a monitorear y gestionar el cumplimiento de las políticas de seguridad de la información.

4.2. MONITOREO, CONTROL Y AUDITORÍA

El monitoreo al cumplimiento de las políticas por parte de cada funcionario, contratista o tercero, corresponde al conocimiento que cada líder o responsable por la administración de un servicio tenga sobre el desempeño y cumplimiento de las obligaciones contraídas, realizando las

gestiones pertinentes para hacer cumplir las políticas e informar del incumplimiento de las mismas.

El Oficial de Seguridad de la Información, o quien haga sus veces, será quien gestione el cumplimiento de las políticas y/o controles técnicos y organizativos, las auditorías internas o externas, el cumplimiento de las presentes políticas por parte del personal de la CVC o involucrados, con el fin de mejorar la seguridad de la información. Las auditorías se definen en el documento general del SGSI (Manual del SGSI), en el numeral 4.4.5.2 “Auditoría Interna”

4.3. EXCEPCIONES

Si se requieren excepciones a alguna de las políticas aquí descritas estas deben ser solicitadas a través de los jefes inmediatos del funcionario con visto bueno de las autoridades competentes en relación a la seguridad de la información dentro de la CVC. Las excepciones deberán quedar documentadas y almacenadas como soporte. El jefe de cada área o proceso será el encargado de evaluar los riesgos de la solicitud, con apoyo del Oficial de Seguridad de la Información o quien hace sus veces, si así lo requiere. Si el encargado de autorizar considera que una excepción solicitada conlleva riesgos altos para la seguridad de la información puede no autorizarla, o escalarla a su superior según el organigrama de la CVC.

Las excepciones a políticas y privilegios serán revisadas regularmente. Su fecha de vencimiento tiene vigencia de seis (6) meses a partir de la aprobación, por lo tanto, si se encuentra vencida debe ser solicitada nuevamente con las autorizaciones respectivas.

4.4. INCUMPLIMIENTO A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El cumplimiento de las políticas de seguridad de la información es obligatorio para todo funcionario o colaborador, contratista, consultor, pasante o tercera parte relacionada con la CVC. En caso de presentarse un desacato, un incumplimiento o una potencial violación a las políticas aquí descritas por negligencia o intencionalmente, el colaborador que detectó la falta está en la obligación de informar el incumplimiento de la política mediante los canales de comunicación establecidos; éste a su vez informará a los procesos necesarios de acuerdo al incidente con el fin de tomar las medidas correctivas pertinentes según el caso y que surta el respectivo proceso según el código disciplinario vigente. Si el caso se presenta por parte de un tercero como un contratista, proveedor o un cliente, el mismo será analizado conjuntamente con las partes involucradas dentro de la CVC, quienes serán la instancia que tomarán las acciones necesarias para solucionar el inconveniente.

4.5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.5.1. Política general de seguridad de la información

La Política de Seguridad de la Información representa la posición de la CVC con respecto a la protección de los activos de información (los funcionarios, la información, los procesos, las tecnologías de información, incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

La CVC para el cumplimiento de su misión, visión, objetivos estratégicos y apegado a sus valores corporativos, establece la función de Seguridad de la Información en la entidad, con el objetivo de:

a) Minimizar el riesgo en las funciones más importantes y críticas de la entidad.
b) Cumplir con los principios de seguridad de la información.
c) Mantener la confianza de sus clientes, socios y empleados.
d) Apoyar la innovación tecnológica.
e) Implementar el sistema de gestión de seguridad de la información ajustado a las necesidades y dimensión de la CVC.
f) Proteger los activos tecnológicos y de información.
g) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
h) Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la CVC.
i) Garantizar la continuidad del negocio frente a incidentes de seguridad de la información.

Esta política aplica a toda la entidad, sus funcionarios, terceros, aprendices, practicantes, proveedores y clientes de la CVC y la ciudadanía en general relacionada.

4.5.2. Revisión de la política

La política general y el manual de políticas de seguridad de la información serán revisadas al menos una vez al año o cuando haya cambios relevantes en la CVC, con el fin de asegurar que sea adecuada a la estrategia y necesidades de la organización.

Las políticas serán revisadas y aprobadas por la Alta Dirección mediante acto administrativo.

4.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.6.1. Roles y responsabilidades

Todo aquel que tenga acceso a la información de la CVC es responsable de velar por la seguridad de la información a la que tiene acceso y de cumplir las políticas descritas en este documento; entre ellos están: jefes de oficinas y direcciones, líderes de procesos, funcionarios, contratistas, usuarios y ciudadanía en general relacionada con la CVC.

El profesional encargado de la seguridad de la información, Oficial de Seguridad de la Información, o quien haga sus veces, asumirá la responsabilidad por el desarrollo e implementación de la seguridad de la información, comprobará el cumplimiento de las políticas, en caso de requerirse prestará asesoría a todo aquel que maneje información de la organización, coordinará las actividades de la gestión de riesgos de la seguridad de la información, apoyará la identificación de controles y pondrá en contexto a la gerencia general (en adelante alta dirección).

En la documentación (manuales, procedimientos e instructivos) del SGSI están definidas las responsabilidades específicas de los funcionarios y contratistas que están directamente relacionados con la seguridad de la información.

4.6.2. Separación de deberes

Todo aquel que tenga acceso a la información de la CVC deberá tener claramente definidos sus deberes, los cuales se pueden apoyar en los procesos de la gestión humana de la organización, con el fin de reducir el uso no autorizado, indebido o accidental de los activos de información.

Todos los sistemas de información de la organización y aplicativos deberán implementar reglas de acceso, de tal forma que haya segregación de funciones entre quien administre, mantenga y audite o tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

4.6.3. Contacto con las autoridades

La CVC mantendrá contacto actualizado de las autoridades competentes para el cumplimiento de la ley, organismos de control y autoridades de supervisión correspondientes. Para ello, se definirá un listado de autoridades a contactar en caso de que se sospeche de la violación de la ley o se confirme una situación de amenaza para la organización.

4.6.4. Contactos con grupos de interés

La CVC mantendrá contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior con el fin de estar al día con la información relacionada con la seguridad de la información y recibir advertencias de actualizaciones, ataques, y vulnerabilidades del software y firmware utilizado.

4.6.5. Seguridad de la información en la gestión de proyectos

La seguridad de la información se debe integrar a las actividades en el desarrollo o la gestión de proyectos de la CVC, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Esto aplicará a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los coordinadores asegurar que se sigan las siguientes directrices:

a) Incluir objetivos o requisitos de seguridad de la información en los objetivos del proyecto.
b) Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del proyecto, para identificar los controles necesarios.
c) Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del proyecto.
d) Evaluar y medir el cumplimiento de la seguridad de la información respecto a sus objetivos o requisitos definidos.

4.6.6. Dispositivos móviles

Con el fin de minimizar los riesgos de seguridad de la información que implica el uso de dispositivos móviles se restringirá la conexión de dispositivos móviles tales como smartphones y tablets a la red corporativa, a excepción de los dispositivos que sean propiedad de la CVC. Se dispondrá de una red de invitados para la conexión de otros dispositivos; esta red permitirá la salida hacia internet, pero no permitirá la conexión con equipos de cómputo o servidores de la CVC.

Las estaciones de trabajo y equipos portátiles que son propiedad de la CVC cuentan con software licenciado y protección contra código malicioso.

El contratista que utilice equipos de cómputo de su propiedad para el desarrollo del objeto del contrato debe:

a) Tener y usar solo software legal instalado en su equipo.

b) Contar con software antivirus.
c) Adjuntar el listado del software que va a utilizar y evidencia de las licencias correspondientes (tanto para el sistema operativo como para las aplicaciones).
d) Indicar nombre del software, fabricante, versión licenciada y fecha de caducidad de la licencia.
e) Esta información debe remitirse al área de Tecnologías de la Información previo a la conexión de dichos dispositivos a la red corporativa y acceso a los servicios de TIC que presta la CVC.

La organización se reserva el derecho de revisar cuando se requiera el software instalado y utilizado en equipos de cómputo y servidores.

4.6.7. Teletrabajo

Cuando se requiera realizar labores de teletrabajo, el líder del área o proceso debe solicitar la creación de una conexión VPN, indicando el tiempo por el cual se requiere la conexión remota para el desarrollo del teletrabajo o si es conforme a la duración del contrato.

En los casos que el acceso y procesamiento de la información sea mediante la modalidad de teletrabajo, los responsables de estas actividades deberán dar cumplimiento a las condiciones y restricciones definidas entorno a la seguridad de la información, tales como:

a) Seguridad física y de comunicaciones.
b) Amenazas de accesos no autorizados a información o recursos.
c) Uso de equipos con software licenciado.

Cumplir con las políticas de seguridad de la información de la CVC para el uso, tratamiento y disposición de los activos e información de la organización.

4.7. SEGURIDAD DE LOS RECURSOS HUMANOS

4.7.1. Vinculación, desvinculación y cambio de empleo

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013, la Ley 909 de 2004, y demás legislación aplicable con relación a la contratación pública, la vinculación laboral, retiro laboral y el cambio de cargo, el área o procesos relacionados con la gestión humana deben hacer verificación de antecedentes de los candidatos al empleo, contratistas y terceros, en concordancia con las regulaciones, las leyes relevantes y la ética organizacional, siendo afín a los requerimientos de la CVC, además de la clasificación de la información a la cual se va a tener acceso y los tipos de riesgos percibidos, así como la

protección de la información de la privacidad, del tratamiento de los datos personales, la disponibilidad de referencias, verificación de la hoja de vida, confirmación de las calificaciones o certificados académicos y profesionales declarados.

Es importante también que se asegure que los candidatos tengan las competencias para desempeñar los cargos a los que aspiran, y si son cargos de importancia sean confiables para desempeñar el rol designado.

Como parte de la obligación contractual, empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la CVC para la seguridad de la información.

Asimismo, el área o los procesos relacionados a la gestión humana deberán hacer firmar a todos los empleados y contratistas a los que se brinde acceso a información confidencial, acuerdos de confidencialidad y no divulgación, antes de asumir el cargo o roles establecidos.

4.7.2. Compromiso de la dirección

La alta dirección o dirección general, a través de las áreas de gestión de talento humano, los responsables de la seguridad de la información y otros procesos; exigirá que los empleados, contratistas, usuarios y terceras partes apliquen la seguridad de la información según las políticas y los procedimientos establecidos por la organización. Esto se realizará mediante la contratación legal y los acuerdos de confidencialidad.

La alta dirección se compromete en apoyar al SGSI a través de Acto Administrativo para el cumplimiento del presente manual de políticas de seguridad de la información. Se compromete en apoyar los programas educativos en materia de seguridad de la información para los funcionarios tales como seminarios, conferencias, espacios de charlas y difusión a través de los diversos canales de comunicación.

4.7.3. Toma de conciencia, capacitación y entrenamiento en seguridad de la información

La CVC debe asegurar que todos los funcionarios, contratistas, visitantes y todos aquellos con acceso a la información y que tengan definidas responsabilidades de seguridad de la información sean competentes (en cuanto a capacitación formal y no formal) para desempeñar sus funciones. Para ello, el área o proceso responsable de la gestión del talento humano revisa anual o semestralmente un Plan de Capacitación en relación a la seguridad de la información.

4.7.4. Procesos disciplinarios

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013, la Ley 734 de 2002 (Código Único Disciplinario), y demás legislación aplicable con relación a los procesos disciplinarios, la CVC sigue los lineamientos de los procedimientos Disciplinario Ordinario, Disciplinario Verbal y Segunda Instancia, a través de la oficina de Control Interno Disciplinario.

4.7.5. Intercambio de información

La CVC firmará acuerdos de confidencialidad con los funcionarios e incluirá una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información restringida o confidencial. En este acuerdo quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se firmarán antes de permitir el acceso o uso de dicha información.

Cuando se realicen acuerdos entre organizaciones para el intercambio de información física o digital, se especificará el grado de sensibilidad de la información de la CVC y las consideraciones de seguridad sobre la misma, así como los controles a implementar.

4.8. GESTIÓN DE ACTIVOS

4.8.1. Inventario de activos

El Oficial de Seguridad de la Información, o quien haga sus veces, creará y mantendrá actualizado el inventario de activos de seguridad de la información, de acuerdo con las directrices o metodología de gestión de riesgos de seguridad de la información.

4.8.2. Uso aceptable de los activos

La información, archivos físicos, sistemas, servicios, y los equipos (ej. estaciones de trabajo, portátiles, impresoras, redes, internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de la CVC, son activos de la organización y se proporcionan a los funcionarios, contratistas y terceros autorizados para cumplir con los propósitos del negocio.

Todos los funcionarios y contratistas deben etiquetar la información y darle un manejo adecuado según su clasificación, siguiendo las directrices de inventario o levantamiento de

activos de información acorde con la metodología de gestión de riesgos de seguridad de la información y lo establecido en el procedimiento Gestión de activos.

Los funcionarios y contratistas de la CVC deben reportar los eventos de seguridad de la información identificados, de acuerdo con el procedimiento Gestión de incidentes.

4.8.3. Uso de equipos de cómputo

Está prohibido que personal ajeno a la Oficina de Tecnologías de la Información (OTI) manipule los equipos de cómputo de la CVC.

El ingreso de equipos de contratistas o visitantes será registrado por parte del personal de seguridad física o recepción.

La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad de la OTI y, por tanto, se debe solicitar soporte para la realización de estas labores.

Los equipos de cómputo no podrán ser trasladados del sitio asignado inicialmente, ni cambiar el colaborador al que le fue asignado, sin previo aviso a la OTI.

Debe respetarse y no modificarse la configuración de hardware y software establecido.

Se restringirá el uso de medios extraíbles para almacenamiento de información (USB, celulares, memory card etc.) en las estaciones de trabajo de la Corporación, con excepción para aquellos funcionarios que por sus funciones y actividades, sean autorizados por los jefes directos o la Dirección General.

Toda actividad informática (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) no autorizada que afecte tanto las redes corporativas como los sistemas de información de la CVC, está prohibida y dará lugar a los procesos disciplinarios y/o legales correspondientes.

Durante la permanencia en las instalaciones de la CVC los equipos de cómputo externos deben estar conectados únicamente a la red de datos corporativos configurada por la OTI, de acuerdo al nivel de acceso correspondiente.

Todas las estaciones de trabajo deben apagarse o hibernarse al finalizar la jornada laboral.

Los equipos de cómputo (CPU y monitor), servidores, teléfonos IP y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados.

La conexión eléctrica de equipos personales debe hacerse a través de los puntos eléctricos no regulados. La corporación no se responsabiliza por daños que puedan sufrir estos dispositivos.

La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones de la CVC y que no son propiedad de la corporación, serán responsabilidad única y exclusiva de sus propietarios. La corporación no será responsable por estos equipos en ningún caso.

4.8.4. Uso de internet

Está prohibido manipular conexiones de red o dispositivos módems o celulares para acceder a internet dentro de la red de la organización por parte de personal no autorizado.

Queda prohibido a todos los funcionarios y contratistas acceder a cualquier página o dirección que contenga material pornográfico en cualquiera de sus variantes, o bien páginas que promuevan cualquier tipo de ideas que puedan ser consideradas ofensivas para las normas de la organización, como: violencia, terrorismo, grupos al margen de la ley, discriminación, y apuestas, entre otras.

Con el propósito de minimizar la probabilidad de saturación, interrupción, alteraciones no autorizadas y errores en la red de la organización, no se permite el envío o descarga de información masiva como música, videos y software no autorizado.

Todo usuario es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta de acceso.

Todas las actividades realizadas en los sistemas de información de la organización y aplicaciones con conexión a internet podrán ser monitoreadas con el fin de preservar la seguridad informática de la organización.

Ningún usuario está autorizado para asignar claves de administrador sobre los computadores de la organización. Esto es competencia de la OTI.
Los usuarios no deben intentar burlar los sistemas de seguridad y de control de acceso; acciones de esta naturaleza se consideran violatorias de las políticas de la organización.

Queda prohibido utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o autorizados por la OTI.

Queda prohibido acceder a sitios de contenido multimedia (videos, música, emisoras online, etc.) debido al alto consumo de canal de internet.

Queda prohibido descargar, instalar y configurar navegadores distintos a los permitidos por la OTI.

4.8.5. Uso del correo institucional

La organización proveerá a todos los funcionarios y contratistas que lo requieran un correo electrónico institucional en el dominio ***cvc.gov.co***

El estándar para la creación de buzón del correo es “primer nombre + punto (.) + Primer apellido”, ej.: luisa.caviedes. También se acepta “Primer nombre + guion (-) + Segundo nombre + punto (.) + Primer apellido”, ej. juan-sebastian.vallejo.

La cuenta de correo electrónico institucional es personal e intransferible, los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y el buzón asociado a la corporación.

El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de la corporación; esto es para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo desempeñadas.

El correo electrónico institucional es una herramienta para el intercambio de información necesaria que permita el cumplimiento de las funciones propias de cada cargo, no es una herramienta de difusión masiva de información y no debe ser utilizada como servicio personal de mensajes o cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, programas piratas, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso.

El envío de información masiva a los clientes debe realizarse exclusivamente por parte de la OTI.

El servidor de correo bloqueará archivos adjuntos o información nociva como archivos .exe, .apk, .msi, .bat o de ejecución de comandos.

Bajo ningún motivo se debe abrir o ejecutar un correo de origen desconocido, debido a que podría contener código malicioso malware (virus, troyanos, keyloggers, gusanos, ransomware etc.), lo cual podría atentar contra los sistemas, programas e información de la organización.

Cada cuenta de correo electrónico tiene asociado un conjunto de recursos de almacenamiento mínimo que es limitado (15GB).

No está permitido abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario como si fuera propia.

El usuario deberá notificar cualquier recibo de correo electrónico sospechoso, a la cuenta helpdesk@cvc.gov.co. El correo sospechoso no debe ser abierto ni reenviado a ningún usuario.

4.8.6. Clasificación de la información

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013, la Ley 1712 de 2014 y sus decretos reglamentarios, la CVC clasifica, etiqueta y maneja la información y sus activos asociados de acuerdo con los procedimientos de clasificación definidos por los procesos responsables.

4.8.7. Gestión de medios removibles

La CVC promoverá el uso de carpetas compartidas en lugar de medios removibles para el intercambio de información al interior de la corporación.

Las unidades de medios removibles de las estaciones de trabajo, equipos portátiles y servidores se bloquearán y quien requiera hacer uso de éstas deberá solicitar la activación a la Oficina de Tecnologías de la Información (OTI) con previa autorización del jefe inmediato, indicando el tiempo por el cual se requiere la activación. Las personas que requieran los medios removibles habilitados de forma permanente deberán tener una autorización firmada por el jefe inmediato y la Oficina de Tecnologías de la Información (OTI).

Se debe hacer seguimiento a la transferencia de información en la red mediante el uso de herramientas DLP u otra herramienta que permita realizar la trazabilidad de la información transmitida en los equipos de cómputo de funcionarios que se hayan definido de acuerdo con las necesidades y la gestión de riesgos.

Se controlará el ingreso y salida de los equipos de cómputo y medios extraíbles de almacenamiento de información de las instalaciones de la CVC mediante mecanismos definidos por la OTI y los encargados de la seguridad física.

Los medios removibles en los que se almacene información clasificada o crítica deben estar cifrados.

Si ya no se requiere el contenido de cualquier medio reusable que se vaya a retirar de la organización se deberá remover de forma que no sea recuperable, es decir de forma segura.

4.8.8. Disposición de los medios

Los medios que contienen información confidencial se deben disponer en forma segura, mediante incineración, destrucción o el borrado de datos antes de ser reutilizados o dados de baja.

La información almacenada en medios removibles debe ser transferida a medios nuevos antes de que se vuelvan ilegibles, de acuerdo con el tiempo de vida útil de los mismos.

Se deben guardar varias copias de datos valiosos para la CVC en medios separados, con el fin de evitar la pérdida de información por daño, pérdida o robo de los medios removibles.

4.8.9. Transferencia de medios físicos

Los medios físicos de almacenamiento como CD/DVD, discos duros, discos extraíbles, memorias, documentación y otros, que contienen información de tipo Confidencial deberán ser protegidos contra acceso no autorizado, uso indebido o corrupción durante el transporte o transferencia de cualquier forma entre partes interesadas.

Para la transferencia o envío de medios de información física deberá ser protegida previamente contra el acceso no autorizado utilizando métodos de embalaje de correspondencia por medio de sobres sellados y enviado por medio de mensajería certificada donde se verifique el recibo de la misma por parte del receptor.

4.9. CONTROL DE ACCESO

4.9.1. Política de control de acceso

La Oficina de Tecnologías de la Información controlará el acceso mediante el enfoque basado en roles, aplicando los siguientes principios:

a) Lo que necesita conocer: solamente se concede acceso a la información que la persona necesita para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber y, en consecuencia, diferentes perfiles de acceso).
b) Lo que necesita usar: solamente se concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, áreas) que la persona necesita para la realización de su tarea/trabajo/rol.

4.9.2. Acceso a redes y a servicios en red

El acceso a redes Wi-Fi se controla con autenticación por contraseña utilizando el protocolo WPA2-PSK.

La OTI proveerá un servicio de conectividad a todos los funcionarios y contratistas de la organización para la navegación en internet, dicho acceso se controla por usuario mediante la autorización previa de los jefes o dirección general. La activación será por nombre de usuario y los accesos están delimitados de acuerdo con los siguientes niveles:

a) Nivel Restringido: Acceso restringido a internet. Este nivel será utilizado únicamente por los visitantes a la organización.
b) Nivel Básico: Acceso a internet y a los recursos o servicios de la organización, ya sean internos o externos y a servicios autorizados para su rol.
c) Nivel Avanzado: Acceso ilimitado, a excepción de páginas con contenido adulto e inmoral y software no deseado.

Para los usuarios con niveles de acceso a internet restringido y básico, que requieran contar con servicios especiales de mensajería instantánea, páginas de encuentro o descargas, deberán ser autorizados por escrito por el jefe inmediato dirigiéndose a la OTI, justificando la necesidad del acceso.

La conexión remota a la red de área local de la CVC debe ser realizada a través de una conexión VPN segura, suministrada por la OTI, la cual debe ser aprobada por los jefes de las

dependencias o la Dirección Administrativa y del Talento Humano por escrito y dirigido a la Oficina de Tecnologías de la Información (OTI).

La conexión a servicios en red se controla mediante el portal cautivo, a excepción del control de acceso físico a la organización donde se utilizará mecanismos biométricos.

4.9.3. Gestión de acceso de usuarios

El registro y cancelación de usuarios; el suministro de acceso a usuarios; la gestión de derechos de acceso privilegiado; la gestión de información de autenticación secreta; y la revisión, retiro o ajuste de los derechos de acceso se realizan de acuerdo con la política de control de acceso, establecida en el numeral 4.9.1 del presente manual.

4.9.4. Uso de información de autenticación secreta (responsabilidades de los usuarios)

Cada usuario es responsable exclusivo de mantener a salvo la contraseña de ingreso al equipo asignado y del portal cautivo. Los usuarios autorizados a acceder a los sistemas de información de la CVC son responsables de la seguridad de las contraseñas y cuentas de usuario. Las contraseñas son únicas e intransferibles.

No se podrá guardar o escribir las contraseñas en papeles o superficies, así como dejar constancia de ellas.

La contraseña escogida para el acceso a cada uno de los sistemas de información de la CVC debe:

a) Ser diferente para cada aplicación o sistema de información.
b) No deberá contener características personales o de los parientes tales como nombres, apellidos, fechas de cumpleaños o alguna otra fecha importante.
c) No debe contener palabras de diccionario. Las palabras en idioma inglés y español son las primeras utilizadas por los atacantes.
d) Las contraseñas se deben establecer teniendo en cuenta los siguientes parámetros: Deben contener mayúsculas, minúsculas, números y mínimo ocho (8) caracteres.

Las contraseñas deben ser cambiadas cada tres (3) meses.

Está prohibido facilitar o proporcionar acceso a las aplicaciones e información a usuarios o a terceros no autorizados.

Para desbloquear la clave de acceso, el usuario deberá realizar la solicitud a la OTI; dicho desbloqueo se debe realizar posterior a la validación de la solicitud.

4.9.5. Control de acceso a sistemas y aplicaciones

El control de acceso a sistemas y aplicaciones se rige por la política de control de acceso y el procedimiento de Gestión de usuarios.

Las aplicaciones críticas de la organización deben forzar la autenticación mediante el protocolo HTTPS.

Las aplicaciones críticas de la organización deben tener implementados mecanismos de protección contra intentos de ingreso mediante fuerza bruta, tales como recaptcha y/o bloqueo de cuentas por un tiempo determinado después de múltiples intentos.

El sistema de correo electrónico de la organización deberá implementar mecanismos de doble autenticación tan pronto como sea posible o en el momento que se considere necesario.

Con el fin de controlar el acceso no autorizado a sistemas y aplicaciones, las contraseñas de cuentas de administración genéricas (root, SYS, SYSADMIN, cuenta de administrador de Windows, entre otras) deben ser cambiadas anualmente o cada vez que expire el tiempo de acceso concedido a un colaborador, excolaborador, contratista y/o proveedor.

La OTI debe cambiar las credenciales por defecto de las aplicaciones y servicios utilizados.

El uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones no está permitido para fines diferentes a las actividades propias de la OTI.

La organización controlará el uso de programas utilitarios privilegiados.

Para acceder a los códigos fuente de programas y elementos asociados se debe contar con autorización de la oficina o dirección encargada y la OTI. Lo anterior con el fin de evitar la introducción de funcionalidades no autorizadas, evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual valiosa.

4.10. CONTROLES CRIPTOGRÁFICOS

La OTI debe determinar los algoritmos criptográficos y protocolos autorizados para su uso en la organización y configurar los sistemas para permitir únicamente aquellos seleccionados, teniendo en cuenta la información de los grupos de interés con el fin de descartar algoritmos de cifradas débiles tales como DES, RC3, RC4 y protocolos débiles tales como SSLv2 y SSLv3. Se debería considerar en su lugar el uso de algoritmos tales como AES (cifrado simétrico), RSA (cifrado asimétrico) y los protocolos SSL/TLS 1.1 o 1.2 y tamaños de cifrado de 168 o 256 bits (cifrado simétrico) y 2048 bits (cifrado asimétrico) preferiblemente o en su defecto 128 bits (cifrado simétrico) y 1280 o 1536 bits (cifrado asimétrico).

Las llaves criptográficas serán cambiadas anualmente o cada vez que se sospeche que han perdido su confidencialidad.

La administración de llaves criptográficas y certificados digitales estará a cargo de la OTI. Sin embargo, la administración de tokens y firmas digitales estarán a cargo de cada uno de los funcionarios o contratistas a quienes les fueron asignados para el desempeño de sus labores.

El sistema de cifrado del almacenamiento de los equipos de cómputo final utilizado por el personal colaborador de la CVC es obligatorio.

4.11. SEGURIDAD FÍSICA Y DEL ENTORNO

4.11.1. Áreas seguras

La CVC en sus instalaciones tiene implementado un sistema de control de acceso biométrico a la entrada de la organización. Adicionalmente, se cuenta con una recepción donde se controla el ingreso y salida de terceros, y el ingreso y salida de elementos, tanto de funcionarios como de terceros.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

El data center debe contar con mecanismos que permitan garantizar que se cumplen los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que alberga.

La CVC cuenta con un Sistema de Seguridad CCTV, para otorgar la mayor seguridad posible tanto a los ciudadanos como a los funcionarios que ingresan a sus instalaciones. El acceso al centro de monitoreo es de carácter restringido. Las únicas personas que tienen permiso de acceder son aquellos funcionarios que autorice la OTI, los responsables de la seguridad física y Dirección General.

a) Todo colaborador está en la obligación de informar cualquier evento o incidente que se presente en las zonas de monitoreo.
b) Está prohibido generar una copia de video sin previa autorización de la OTI.
c) Toda solicitud de copias de video debe hacerse por escrito a la OTI.
d) Todas las grabaciones tienen una duración de 10 días y después se reescribe.
e) Está prohibido dar información de especificaciones técnicas y ubicaciones de cámaras.
f) Toda copia de video generada deberá ser entregada mediante oficio o mediante cadena de custodia.

La CVC cuenta con un plan de emergencias que es probado anualmente, con el fin de brindar protección contra amenazas externas.

4.11.2. Ubicación y protección de los equipos

El data center está ubicado de forma tal que personas no autorizadas no puedan ver la información durante su uso y el acceso físico es controlado por la OTI.

Se hace seguimiento a las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) que pueden llegar a afectar adversamente el data center.

4.11.3. Servicios de suministro

La CVC cuenta con aire acondicionado, un sistema de alimentación no interrumpida (UPS) que asegura el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de energía, un enlace de red redundante y un sistema de monitoreo de las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) del data center.

4.11.4. Seguridad del cableado

El cableado de la CVC debe cumplir con la normatividad de cableado estructurado, el cual debe estar certificado. Esta es una responsabilidad de la OTI.

4.11.5. Mantenimiento de equipos

La OTI establece y ejecuta planes de mantenimiento de la infraestructura tecnológica de la organización.

4.11.6. Seguridad de equipos y activos fuera de las instalaciones

La salida de elementos de la CVC es controlada mediante el formato Ingreso / salida de activos informáticos (equipos de cómputo).

Los equipos y medios removibles que son retirados de las instalaciones de la CVC están debidamente cifrados.

Los funcionarios y contratistas que retiren equipos o medios removibles de las instalaciones deben seguir las siguientes directrices:

a) Bajo ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.
b) Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
c) En caso de pérdida o robo de un equipo de cómputo de la CVC, se deberá poner la denuncia ante la autoridad competente e informar inmediatamente al jefe inmediato y a la Oficina de Tecnologías de la Información (OTI) para que se inicie el trámite interno correspondiente.

4.11.7. Disposición segura o reutilización de equipos

Cuando una estación de trabajo, equipo portátil o medio removible vaya a ser reasignado o dado de baja, se deberá realizar una copia de respaldo de la información de la CVC que allí se encuentre almacenada (en caso de ser necesario). Posteriormente, el equipo deberá ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobre-escritura de los medios que contienen información) con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma.

4.11.8. Política de equipo desatendido, escritorio limpio y pantalla limpia

Los funcionarios de la CVC deberán conservar su escritorio libre de información propia de la organización, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento, cada vez que se vayan a retirar de sus puestos de trabajo.

Al imprimir documentos de carácter confidencial (información clasificada e información reservada), éstos deben ser retirados de la impresora inmediatamente.

Los computadores cargarán por defecto el fondo de pantalla de la CVC; este no podrá ser modificado y deberá permanecer activo.

Los funcionarios de la organización deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo.

Los usuarios son responsables y asumen las consecuencias por la pérdida de información que esté bajo su custodia.

Se prohíbe el almacenamiento de información personal en los computadores de la organización.

4.12. SEGURIDAD DE LAS OPERACIONES

4.12.1. Documentación de procedimientos operativos

Se debe contar con procedimientos de trabajo debidamente documentados para las actividades operativas asociadas con las instalaciones de procesamiento y comunicación.

4.12.2. Control de cambios

Los cambios en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información se realizan de acuerdo con las directrices del procedimiento Gestión de cambios.

Los cambios que se lleven a cabo deben ser evaluados y probados de forma integral y se debe contar con una participación de los administradores de los diferentes componentes de la solución.

El procedimiento Gestión de cambios debe considerar los niveles de servicio, acuerdos de seguridad en los servicios y las necesidades del negocio. Así mismo, debe incluir la identificación de los riesgos asociados al cambio y las acciones del tratamiento correspondiente.

4.12.3. Gestión de capacidad

La CVC gestiona la capacidad de su plataforma tecnológica (hardware y software) de acuerdo con las indicaciones del procedimiento Gestión de capacidad.

La OTI realiza seguimiento al uso de los recursos de la plataforma tecnológica y sistemas, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido de los sistemas.

4.12.4. Separación de los ambientes

La CVC cuenta con ambientes de desarrollo y producción separados por máquinas físicas y máquinas virtuales.

La CVC controla el acceso al ambiente de desarrollo de la misma forma que controla el acceso al ambiente de producción.

4.12.5. Protección contra códigos maliciosos

Se deben proteger las estaciones de trabajo, equipos portátiles y servidores de la CVC contra códigos maliciosos.

Los contratistas que hagan uso de sus equipos portátiles personales deben contar con un software antivirus licenciado.

El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos conectados a la red deben tener el antivirus instalado y activo.

El único servicio de antivirus autorizado en la CVC es el asignado directamente por la OTI, el cual cumple con todos los requisitos técnicos y de seguridad. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura.

El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados por virus o códigos maliciosos o sean sospechosos de estar infectados.

El usuario no debe instalar o emplear programas no autorizados para manejo de antivirus.

Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa de antivirus y que han sido establecidos por la OTI.

El programa de antivirus debe ser instalado única y exclusivamente por la OTI en los servidores y estaciones de trabajo.

4.12.6. Copias de respaldo

La CVC debe realizar copias de respaldo de la información y pruebas periódicas a las mismas. Para ello la OTI definirá y ejecutará las actividades requeridas en el procedimiento Gestión de backups.

La OTI establecerá las políticas y estándares de copias de seguridad para los sistemas de información y bases de datos.

Todos los administradores de base de datos, aplicaciones y servicios deben cumplir con las políticas de backup establecidas por la OTI.

Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso, y aplicar los controles para la protección de los medios de respaldo.

Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema cuando por situaciones como: borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o computadores o por requerimientos legales sea necesario recuperarla.

Las copias de respaldo o backup serán verificadas periódicamente por la OTI con el fin de certificar su validez y correcto funcionamiento.

Los funcionarios son responsables de salvaguardar la información local de sus equipos.

Toda la información institucional que se almacena en los equipos asignados a los funcionarios o contratistas es de propiedad de la organización, motivo por el cual no debe ser divulgada a terceros, salvo autorización expresa de la CVC. El incumplimiento de estas disposiciones acarrea sanciones de tipo legal que serán de total responsabilidad del colaborador o contratista.

4.12.7. Registro y supervisión

4.12.7.1. Registro de eventos

Los sistemas operativos, servicios y sistemas de información que hacen parte de la infraestructura para el procesamiento de información y comunicaciones de la CVC, deben generar archivos de registro de eventos (logs) definidos en conjunto por los responsables de su administración.

4.12.7.2. Protección de la información de registro

La OTI con el fin de proteger la información de registro de modificación no autorizada por parte de usuarios no autorizados, administradores u operadores de los sistemas de información implementará mecanismos de copiado de logs en “tiempo real” a un sistema por fuera del control de administradores y operadores de los sistemas.

4.12.7.3. Sincronización de relojes

Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por la CVC, deben estar sincronizados.

4.13. CONTROL DE SOFTWARE OPERACIONAL

4.13.1. Instalación de software en sistemas operativos

El proceso de instalación y desinstalación de software está autorizado exclusivamente al personal de la Oficina de Tecnologías de la Información (OTI). Por lo tanto, a cualquier otro servidor público o contratista no le es permitido realizar esta labor salvo autorización escrita.

Para la instalación de software se deben seguir las siguientes directrices:

a) El software propietario debe contar con su respectiva licencia y en el caso del software libre debe estar permitido el uso comercial.
b) El instalador debe ser descargado de la página oficial del fabricante.
c) Debe verificarse la integridad del archivo por medio de la comprobación de códigos hash.
d) Debe dejarse evidencia documentada de que las directrices anteriores fueron seguidas a cabalidad.

Se debe proporcionar capacitación adecuada a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de los nuevos sistemas de información o mejoras a sistemas de información existentes, antes de su puesta en marcha.

Todos los sistemas nuevos y mejorados deben estar completamente soportados por una documentación suficientemente amplia y actualizada, y no deben ser puestos en el ambiente de producción sin contar con la documentación disponible.

4.13.2. Gestión de la vulnerabilidad técnica

4.13.2.1. Gestión de las vulnerabilidades técnicas

La OTI, es responsable de verificar de manera periódica (al menos mensual) la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la organización.
Se debe generar y ejecutar por lo menos una vez al año el plan de análisis de vulnerabilidades y/o hacking ético para las plataformas críticas de la organización, cuya viabilidad técnica y de administración lo permita.

Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad de la OTI, siguiendo las directrices del procedimiento Gestión de cambios.

4.13.3. Consideraciones sobre auditorías de sistemas de información

4.13.3.1. Controles sobre auditorias de sistemas de información

Para la ejecución de auditorías a los sistemas de información se deben tener en cuenta las siguientes consideraciones:

a) Los requisitos de auditoría para acceso a sistemas y a datos se deberían acordar con los jefes de la(s) dependencia(s) involucradas.
b) El alcance de las pruebas técnicas de auditoría se debería acordar y controlar.
c) Las pruebas de auditoría (incluidas las pruebas de análisis de vulnerabilidades y/o hacking ético) que puedan afectar la disponibilidad del sistema se deberían realizar fuera de horas laborales.
d) Se debería hacer seguimiento de todos los accesos y logs para producir un rastro de referencia.

4.14. SEGURIDAD DE LAS COMUNICACIONES

4.14.1. Gestión de la seguridad en las redes

La OTI debe definir e implementar los mecanismos de control que considere apropiados para proteger la confidencialidad, integridad y disponibilidad de las redes, los servicios en red y la información por allí transmitida.

La OTI define e implementa los mecanismos de separación de las redes de la CVC con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de computador de escritorio, dominio de servidor), por dependencias (por ejemplo, oficina de talento humano, oficina de servicios administrativos, oficina de gestión financiera, oficina de TIC) o alguna combinación (por ejemplo, un dominio de servidor que se conecta a múltiples dependencias).

La OTI debe mantener separadas la red de datos y la red de voz, con el fin de minimizar el impacto de interceptación de alguna de las dos redes.

El acceso remoto a las redes de la organización se controla mediante conexiones VPN.

4.14.2. Transferencia de información

La CVC firmará acuerdos de confidencialidad con los funcionarios e incluirá una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información restringida o confidencial. En este acuerdo quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se firmarán antes de permitir el acceso o uso de dicha información.

Cuando se realicen acuerdos entre organizaciones para el intercambio de información física o digital, se especificará el grado de sensibilidad de la información de la CVC y las consideraciones de seguridad sobre la misma, así como, los controles a implementar.

Los funcionarios y contratistas deben seguir las indicaciones del procedimiento Gestión de activos (clasificación, etiquetado y manejo de la Información), para la transferencia de información de acuerdo con su clasificación.

4.15. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

4.15.1. Requisitos de seguridad de los sistemas de información

La OTI debe definir los requisitos de seguridad de la información para sistemas de información nuevos o mejoras a los sistemas de información existentes, contratados externamente o desarrollados en la organización. Para ello, debe tener en cuenta:

a) El nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario. Por ejemplo, la implementación de segundos factores de autenticación y un sistema de gestión de contraseñas que exija el uso de contraseñas fuertes, el cambio periódico de contraseñas y que guarde un historial de contraseñas para evitar su reúso.
b) Los procesos de suministro de acceso y de autorización para usuarios, al igual que para usuarios privilegiados o técnicos. Por ejemplo, el suministro de datos de acceso por correo electrónico.
c) Las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad e integridad. Por ejemplo, cifrado de información almacenada, el envío de información por canales cifrados.
d) Los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso, seguimiento, y no repudio. formularios de autenticación mediante HTTPS, cifrado de contraseñas almacenadas, uso de firmas digitales.
e) Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.
f) La necesidad de exigir la implementación de metodologías de desarrollo seguro.

Las dependencias que contraten el desarrollo de software o adquieran software de terceros, deben apoyarse en la OTI para definir los requisitos de seguridad de la información de los mismos.

4.15.2. Seguridad en los procesos de desarrollo y soporte

4.15.2.1. Política de desarrollo seguro

La CVC velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requisitos de seguridad esperados, así como con pruebas de aceptación y seguridad al software desarrollado. Además, la CVC asegurará que todo software desarrollado o adquirido, interna o externamente cuente con el nivel de soporte requerido por la organización.

4.15.2.2. Cambios en sistemas, plataforma tecnológica o paquetes de software

Los cambios en sistemas deben realizarse de acuerdo con el procedimiento Gestión de cambios.

4.15.2.3. Principios de desarrollo seguro

La OTI debe definir e implementar principios de desarrollo seguro en actividades de construcción de sistemas de información internos.

Los principios de desarrollo establecidos se deben revisar con regularidad (al menos anualmente) para asegurar que están contribuyendo a mejorar los estándares de seguridad dentro del proceso de construcción. También se deben revisar regularmente para asegurar que permanezcan actualizados en términos de combatir nuevas amenazas potenciales y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

4.15.2.4. Ambiente de desarrollo seguro

La OTI aplicará los mismos controles aplicados al ambiente de producción en el ambiente de desarrollo, tales como, control de acceso, copias de respaldo, registro de eventos y separación de ambientes (desarrollo y producción).

La OTI debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y producción han sido aprobadas, de acuerdo con el procedimiento Gestión de cambios.

La OTI debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la CVC.

4.15.2.5. Desarrollo contratado externamente

La CVC debe asegurarse que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.

La CVC debe exigir el suministro de evidencia de que se realizaron pruebas de seguridad al software desarrollado por terceros.

Los principios de desarrollo seguro se deben aplicar, en donde sea pertinente, a desarrollos contratados externamente.

Las dependencias que contraten desarrollos externos deben asegurar que se realicen pruebas de aceptación del software, con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.

Las dependencias deben tener en cuenta e incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes aplicables.

Las dependencias deben incluir en acuerdos contractuales, en donde sea posible, el derecho de la CVC a realizar auditorías durante el desarrollo del contrato.

Cuando se contrata desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por la CVC. Adicionalmente, se debe acordar la entrega de manuales técnicos, que describan la estructura interna del sistema, así como el diccionario de datos, librerías y archivos que lo conforman; y manuales funcionales, que describan las funcionalidades de cada una de las opciones del menú de la aplicación.

4.15.2.6. Pruebas de seguridad de sistemas

Se debe exigir tanto para desarrollos internos como externos la ejecución de pruebas funcionales que incluyan la evaluación de los requisitos de seguridad de la información y la protección contra vulnerabilidades conocidas.

4.15.2.7. Pruebas de aceptación de sistemas

Se deben realizar pruebas de aceptación del software, independientemente de que sea un desarrollo interno o un desarrollo contratado externamente, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de desarrollo de sistemas seguros (en donde sea aplicable). En estas pruebas se puede hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y se debería verificar que se han corregido los defectos relacionados con la seguridad.

De ser posible, las pruebas se deberían llevar a cabo en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades y que las pruebas son confiables.

En donde la funcionalidad de la seguridad no satisface el requisito especificado, antes de comprar el software se deberían reconsiderar el riesgo introducido y los controles asociados.

4.15.3. Datos de prueba

La OTI debe certificar que la información a ser entregada a los desarrolladores (tanto internos como externos) para sus pruebas será enmascarada o que los datos sensibles serán eliminados con el fin de no revelar información confidencial de los ambientes de producción y por ende, dar cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública).

4.16. RELACIÓN CON LOS PROVEEDORES

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

4.16.1.1. Política de seguridad de la información para las relaciones con proveedores

La CVC establecerá mecanismos de control en sus relaciones con proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas y procedimientos de seguridad de la información de la organización.

4.16.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores

La dirección general se asegurará de comunicar las políticas y procedimientos de seguridad de la información a los proveedores y/o contratistas.

Se deben incluir en los acuerdos con proveedores y/o contratistas, como mínimo, los siguientes requisitos de seguridad de la información:

a) Cláusula de confidencialidad.
b) Cláusula que defina las responsabilidades que continúan después de terminado el contrato (por ejemplo, confidencialidad durante 5 años después de terminado el contrato).

c) Cumplimiento de las políticas de seguridad de la información de la CVC.
d) Reporte de eventos de seguridad de la información a través de los canales definidos en el procedimiento Gestión de incidentes.
e) Etiquetado y manejo de la información de acuerdo con las directrices del procedimiento Gestión de activos.
f) Cláusula de seguimiento y revisión de los servicios de los proveedores y/o contratistas para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, en los acuerdos contractuales correspondientes (Evaluación del proveedor).

La dirección general debe administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad de la información establecidos con ellos y monitoreando la aparición de nuevos riesgos.

Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal, por escrito, al proceso Gestión de tecnologías de información.

4.17. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La CVC gestiona los riesgos de seguridad de la información de acuerdo con las directrices del procedimiento Gestión de incidentes.

4.17.1. Notificación de incidentes de seguridad de la información

Toda violación de estas políticas se deberá notificar inmediatamente a la Oficina de Tecnologías de la Información (OTI) a través de los siguientes canales:

a) E-mail: helpdesck@cvc.gov.co
b) Extensión: 55555 – 1286
c) Intranet: helpdesck@cvc.gov.co – Edwin.ruano@cvc.gov.co
d) Software de gestión de incidentes: Ito

Asimismo, se deberán notificar situaciones tales como: personas ajenas en oficinas y centros de cómputo correos maliciosos o sospechosos; reinicio de los equipos de cómputo o enrutadores; mala utilización de recursos; uso de software ilegal; divulgación, alteración y robo de información.

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

4.18.1. Continuidad de la seguridad de la información

La CVC planificará e implementará la continuidad del negocio teniendo en cuenta no sólo los recursos tecnológicos, sino también los demás activos de información y los procesos críticos de la continuidad de la seguridad de la información.

La CVC realizará pruebas periódicas (al menos anualmente) a los controles de continuidad del negocio y de continuidad de la seguridad de la información implementada, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

4.18.2. Redundancias

La CVC establecerá e implementará un Plan de Recuperación de Desastres (DRP) con el fin de asegurar la redundancia y continuidad de las instalaciones de procesamiento de información.

La CVC realizará pruebas periódicas (al menos anualmente) al DRP, con el fin de asegurar que los controles tecnológicos implementados son válidos y eficaces durante situaciones adversas.

4.19. CUMPLIMIENTO

4.19.1. Cumplimiento de requisitos legales y contractuales

4.19.1.1. Identificación de la legislación aplicable y de los requisitos contractuales

La Oficina Asesora Jurídica y el Oficial de Seguridad o quien haga sus veces deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables y relacionados con seguridad de la información. Para ello, se pueden apoyar en los jefes de dependencias que manejan los temas de talento humano y gestión documental corporativa.

4.19.1.2. Derechos de propiedad intelectual

La OTI debe asegurarse de que todo el software que se ejecute en la CVC esté protegido por derechos de autor y requiera licencia de uso, o en su lugar, sea software de libre distribución y uso.

Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos portátiles suministrados para el desarrollo de sus actividades.

Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

Los supervisores de contratos deben asegurarse de incluir cláusulas de propiedad intelectual y derechos de autor en contratos con terceros.

4.19.1.3. Protección de registros

La CVC se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requisitos normativos, legales o regulatorios contra la pérdida de confidencialidad, disponibilidad e integridad, siguiendo las directrices del procedimiento Gestión de activos.

4.19.1.4. Privacidad y protección de información de datos personales

La CVC será responsable del tratamiento de los datos personales, tal y como se define en la Ley 1581 de 2012: respetar la privacidad de cada uno de los terceros que le suministren sus datos personales a través de los diferentes puntos de recolección y captura de dicha información. Por lo tanto, implementarán los controles necesarios para su protección y en ningún momento divulgará esta información a terceras partes a menos que cuente con la autorización formal de los mismos o en los casos en que la ley lo permita.

4.19.1.5. Reglamentación de controles criptográficos

La reglamentación se regirá por la Ley 527 de 1999 *por 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) y sus decretos reglamentarios, según aplique.

4.19.2. Revisiones de seguridad de la información

4.19.2.1. Revisión independiente de la seguridad de la información

Al evaluar el desempeño del SGSI se realizarán auditorías internas de revisión independiente al menos anualmente. Esta revisión independiente es necesaria para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque de la organización para gestionar la seguridad de la información. Esta revisión debe incluir la valoración de las oportunidades de mejora y la necesidad de efectuar cambios en el enfoque hacia la seguridad, incluyendo la política y los objetivos de control.

4.19.2.2. Cumplimiento con las políticas y normas de seguridad

Los jefes de dependencia deben revisar con regularidad (al menos semestralmente) el cumplimiento de las políticas y procedimientos de seguridad de la información dentro de su área de responsabilidad.

4.19.2.3. Revisión del cumplimiento técnico

El jefe de la Oficina de Tecnologías de la Información (OTI) debe coordinar la revisión periódica (al menos semestralmente) de los sistemas de información para determinar el cumplimiento con las políticas y procedimientos de seguridad de la información. Para ello, se debe determinar a qué sistemas de información se hará revisión cada vez.

4.20. OTROS DOCUMENTOS RELACIONADOS

- Política General SGSI.
- MN.0720.01 Sistema de Gestión de la Seguridad de la Información.
- FT.0720.03 Ingreso / salida de activos informáticos (equipos de cómputo).
- Procedimiento Gestión de cambios.
- Procedimiento Gestión de capacidad.
- Procedimiento Gestión de backups.
- Procedimiento Gestión de activos.
- Procedimiento Gestión de incidentes.