Politica General de Seguridad de la Informacion

MANUAL: Políticas de Seguridad de la Información			
FECHA DE APLICACIÓN: 2024-05-07	**CÓDIGO:** MN.0720.02	**VERSIÓN:** 002	
ELABORADO POR: FABIAN EDUARDO ROJAS GALLEGO PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION CAROLA DUQUE JIMENEZ TECNICO ADMINISTRATIVO DE LA OFICINA DETECNOLOGIAS DE LA INFORMACION **JUAN CARLOSCAMACHO CASTILLO** PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	**REVISADO POR:** DIEGO ALEXANDER MILLAN LONDOÑO JEFE DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION EDWIN RUANO GAMBOA PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION **JINETH ALEXIAMURILLO SINISTERRA** PERSONAL DE APOYO GRUPOGESTIÓN AMBIENTAL Y DE CALIDAD	**APROBADO POR:** DIEGO ALEXANDER MILLAN LONDOÑO JEFE DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	

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 DE SEGURIDAD DE LA INFORMACIÓN

Realizar una adecuada gestión del riesgo con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, atreves de políticas y controles de seguridad de la información.

Capacitar y sensibilizar al personal en temas relacionados con la seguridad de la información, buscando un aumento progresivo en la cultura de seguridad al interior de la Corporación, reflejado en el nivel de cumplimiento de políticas y procedimientos y el reporte de eventos e incidentes de seguridad.

Gestionar de manera adecuada los incidentes de seguridad de la información generando, documentando y aplicando las lecciones aprendidas, con el fin de reducir la posibilidad o impacto de incidentes futuros.

Mejorar continuamente el desempeño del SGSI mediante la implementación de acciones correctivas eficaces, auditorías internas y las revisiones de seguridad de la información.

2. ALCANCE

El presente manual establece las políticas de seguridad de la información definidas por la CVC, teniendo en cuenta la estrategia de Gobierno Digital 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, sus recursos y la totalidad de los procesos internos o externos, vinculados a la Corporación.

3. DEFINICIONES

Las definiciones que aplican a este manual pueden ser consultadas en el siguiente enlaceGLOSARIO DE TÉRMINOS Y DEFINICIONES

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 cumplimiento de las Políticas de Seguridad de la Información estará a cargo de todos los funcionarios, contratistas y terceros que se vinculen con la CVC. Igualmente deberán informar a la Oficina de Tecnologías de la Información - OTI cuando se evidencie incumplimiento a algunas de las políticas, que ponga en riesgo la seguridad de la información.

La Oficina de Control Interno y el Oficial de Seguridad de la Información, o quien haga sus veces, velarán por el cumplimiento de las políticas a través de controles técnicos y organizativos, auditorías internas o externas, con el fin de mejorar la seguridad de la

Si se requieren excepciones a alguna de las políticas aquí descritas, deben ser solicitadas a través de los jefes inmediatos del funcionario. 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 negarla, o escalarla a su superior según el organigrama de la CVC.
Las excepciones a las políticas serán revisadas al menos una vez al año. Podrán concederse excepciones con plazos máximos de seis (6) meses, por lo tanto, si se encuentran vencidas deben ser solicitadas nuevamente con su respectiva autorización.

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, contratista, pasante o usuario relacionado con la CVC. En caso de presentarse un desacato, un incumplimiento o una violación a las políticas aquí descritas, de forma intencional o por negligencia, se deberá informar a la OTI mediante los canales de comunicación establecidos. La OTI vinculará a los procesos comprometidos en el incidente con el fin de tomar las medidas correctivas pertinentes y que se inicien las investigaciones disciplinarias o a las que haya lugar.

4.5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.5.1. Política general de seguridad de la información

La Política General de Seguridad de la Información representa la posición de la CVC con respecto a la protección de los activos de información, la implementación del Sistema de Gestión de Seguridad de la Información y a la articulación, actualización y publicación de sus políticas, procedimientos e instructivos.
La CVC para dar cumplimiento a su misión, visión y objetivos estratégicos, establece la política de seguridad de la información que alineada a los valores corporativos permite:

a. Minimizar el riesgo en las funciones misionales 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.

4.5.2. Revisión y aprobación de la Política General y el Manual de Politicas de Seguridad de la Información

L a Política General de Seguridad de la Información 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.
La aprobación de la Política General de Seguridad de la Información estará a cargo de la Dirección General y la aprobación del Manual de Politicas de Seguridad de la Información estará a cargo del Jefe de la Oficina de Tecnologías de la Información.

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 o el 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 y prestará asesoría a todo aquel que manipule información de la organización. Además, coordinará las actividades de gestión de riesgos de seguridad de la información, apoyará la identificación de controles y pondrá en contexto a la Dirección General.
En la documentación (manuales, procedimientos e instructivos) del SGSI están definidas las responsabilidades específicas de los funcionarios, contratistas y demás actores, 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 definidas claramente sus responsabilidades y deberes de acuerdo al manual de funciones o contrato, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.
Todos los sistemas de información de la CVC y aplicativos deberán implementar reglas de acceso para 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 permanente con las autoridades 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 Corporación.

4.6.4. Contacto 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

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 equipos portátiles externos; 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 deben contar 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 instalado solo software legal en los equipos.

b. Contar con software antivirus licenciado y actualizado.

c. Listar el software que va a utilizar y evidenciar las licencias correspondientes tanto para el sistema operativo como para las aplicaciones.

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

4.6.7. Teletrabajo y Trabajo en casa.

Cuando se requiera realizar labores de teletrabajo o trabajo en casa, de acuerdo a lo establecido por la entidad y la normatividad vigente, el líder del área o proceso debe autorizar y solicitar la creación de una conexión VPN si es necesario, o solicitar acceso a herramientas corporativas publicadas en la web para acceso desde internet, indicando el tiempo por el cual se requiere la conexión remota para el desarrollo del teletrabajo o Trabajo en casa o si es por la duración del contrato.

De igual forma antes de poner en marcha la modalidad de Teletrabajo o Trabajo en casa, se evaluará en primer lugar si es posible y practico teniendo en cuenta las funciones del puesto de trabajo y la persona que lo ocupa, teniendo en cuenta:

a. Identificar las funciones y tareas que se pueden hacer fuera del lugar de trabajo habitual. Con este fin es posible que sea preciso apartarse de la norma general para encontrar soluciones innovadoras y creativas.

b. Evaluar los mecanismos de conectividad, como las llamadas periódicas de videoconferencia y otros medios.

c. Evaluar la infraestructura, las instalaciones y los instrumentos disponibles para el trabajo desde casa, como la conexión a Internet y la disponibilidad de un suministro de energía fiable.

d. Evaluar los requisitos legales, las obligaciones y la posible responsabilidad civil, teniendo en cuenta la situación del trabajador y sus funciones laborales, así como el equipo y las herramientas necesarias.

En los casos que el acceso y procesamiento de la información sea mediante la modalidad de teletrabajo o trabajo encasa, 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.

d. 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 privacidad de la información, 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.

Se deben establecer para la vinculación de personal, perfiles y competencias idóneas para desempeñar los cargos a los que aspiran de

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. Se deberá utilizar el formato de Acuerdo de Confidencialidad y No Divulgación de Información de la CVC u otro que contemple como minimo esos controles.

4.7.2. Compromiso de la dirección

La 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 Corporación.
La Dirección General debe apoyar el SGSI a través de acto administrativo para el cumplimiento del presente manual de políticas de seguridad de la información. Igualmente debe apoyar los programas educativos en materia de seguridad de la información para los funcionarios 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

La CVC a través de la oficina de Control Interno Disciplinario da cumplimiento a lo establecido en la Ley 734 de 2002 (Código Disciplinario Único), cuando se vean afectados los activos de información por algún funcionario, teniendo en cuenta los lineamientos de establecidos en las políticas de seguridad de la CVC.

4.7.5. Intercambio de información

La CVC firmará acuerdos de confidencialidad e incluirá cláusulas 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, junto a los responsables de los activos de información, creará y mantendrá actualizado el inventario de activos de información de acuerdo con los procedimientos de la CVC.

4.8.2. Uso aceptable de los activos

La activos de información como información, archivos físicos, sistemas, servicios y los equipos de propiedad de la CVC, se proporcionan a los funcionarios, contratistas y terceros autorizados para cumplir con los propósitos del negocio.
Todos los activos de información deben ser etiquetados y se debe dar un manejo adecuado según su clasificación, siguiendo las directrices de inventario de activos de información y los procedimientos establecidos para ello.
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 de Seguridad de la Información PT.0720.29.

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.
Está prohibido utilizar los equipos de cómputo, software y/o periféricos, para realizar actividades diferentes a las estrictamente laborales.
El ingreso y salida 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, tarjetas de memoria, etc.) en las estaciones de trabajo de la Corporación, con excepción para aquellos equipos que reciben información de forma automática desde algún dispositivo especial por medio de puertos USB. De igual forma, se habilitarán temporalmente los puertos para descargue de información, previa autorización de los jefes directos o la Dirección General.
Toda actividad informática (escaneo 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 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.

Las impresoras láser y equipos que no hacen parte de la infraestructura informática, no deben ser conectados a la red energía regulada. 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.
No se debe consumir alimentos, ni bebidas cerca de los equipos de cómputo y sus periféricos.

4.8.4. Uso de internet

Está prohibido manipular conexiones de red o dispositivos 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, reproducción 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.
No se debe utilizar en los equipos de la CVC, software o servicios de mensajería instantánea y redes sociales no instalados o autorizados por la OTI.
No es permitido acceder a sitios de contenido multimedia (videos, música, emisoras online, etc.) para fines diferentes a los laborales, 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, de acuerdo a las capacidades contratadas.
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 o el grupo de Comunicaciones, a través de los canales autorizados.
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, los cuales deben ser usados de forma responsable para el desarrollo de las actividades exclusivamente laborales.
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 al correo itmesaintegral.principal@cvc.gov.co. El correo no debe ser abierto, ni reenviado a ningún usuario y deberá ser marcado como Spam o no deseado.

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

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 de prevención de perdida de datos (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 de almacenamiento removibles en los que se almacene información clasificada o crítica de la CVC, 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

La OTI proveerá un servicio de conectividad (Cableado o Wi-Fi) a todos los funcionarios y a los

contratistas autorizados de la Corporación para la navegación en internet. Dicho acceso se controla con usuarios y contraseñas bajo protocolos de seguridad 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 un 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 y el procedimiento de Gestión de Usuarios PT.0720.24.

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.

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.
e. Las contraseñas se deben establecer teniendo en cuenta los siguientes parámetros: Deben contener mayúsculas, minúsculas, números y mínimo ocho (8) caracteres.
f. 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 o cambiar la clave de acceso, el usuario deberá realizar la solicitud a la OTI mediante los canales autorizados que permitan la trazabilidad de la misma.
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 PT.0720.24.
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 CVC deberá permitir implementar mecanismos de doble autenticación, los cuales serán de uso obligatorio para las cuentas de administración y las cuentas de correo electrónico clasificadas como criticidad alta. Para las demás cuentas de usuarios, su uso será opcional.
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.
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.

custodia.

4.11.2. Ubicación y protección de los equipos

El data center está ubicado en un sitio estratégico y cuenta con un sistema de control de accesos biométrico gestionado por la OTI, que controla el ingreso de personal autorizado

Todos los servidores y equipos de comunicaciones de voz y datos deben estar localizados en lugares seguros para prevenir el uso o acceso no autorizado. De igual forma, deberá contarse con protecciones físicas y ambientales para los activos críticos, incluyendo perímetros de seguridad, controles de acceso físicos, seguridad en el suministro eléctrico, cableado, sistemas de detección y extinción de incendios.

Se debe prevenir el daño de los equipos por interferencia eléctrica o magnética, riesgo de contaminación por alimentos, bebidas o golpes con objetos que perjudiquen o pongan en riesgo el funcionamiento de los mismos o deterioren la información almacenada en ellos.

Se debe evitar colocar encima o cerca de los computadores ganchos, clips, bebidas y comidas que se pueden caer accidentalmente y afectar el funcionamiento del equipo.

Cualquier cambio que se realice en el data center o centros de cableado, y que potencialmente afecte los sistemas de información de la Entidad, debe estar previamente autorizado y debe registrarse en una bitácora de ingreso.

Toda persona que ingrese al data center debe estar autorizada y acompañada por un funcionario(a) y/o contratista de la Oficina de Tecnologías de la Información - OTI. Los administradores del centro de cómputo mantendrán un registro de todas las visitas autorizadas a esta área, en el que se identifique nombre del visitante, documento de identificación, fecha, hora de entrada y salida de las instalaciones, actividad por la cual ingresaron y la persona que autorizó su ingreso. A su vez, todo equipo informático ingresado al centro de cómputo deberá ser registrado.

Constituyen áreas de acceso restringido el centro de cómputo, los cuartos de potencia (Plantas eléctricas, unidades de poder ininterrumpida UPS y cuartos de electricidad) y centros de cableado, por lo que solo el personal autorizado por la Oficina de Tecnologías de la Información – OTI puede acceder a él. Este personal debe portar el carnet de la Entidad que lo acredita como funcionario(a) y/o contratista del área en mención

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.

El suministro de energía eléctrica deberá estar regulado bajo la norma RETIE vigente para Colombia, con sistema de polo a tierra, salvo especificación diferente del fabricante o proveedor de los equipos y se debe contar con sistema de energía ininterrumpida (UPS) y/o planta eléctrica para asegurar el apagado controlado y sistemático o la ejecución continua del parque tecnológico que soporta las operaciones críticas de la CVC.

Los equipos críticos y estaciones de trabajo deben conectarse al sistema de corriente regulado, a diferencia de equipos como impresoras las cuales pueden afectar el normal funcionamiento del sistema regulado.

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.

La instalación de cableado de red, puntos de red y cableado eléctrico regulado, deberá ser supervisado por personal autorizado por la Oficina de Tecnologías de la Información - OTI.

No pueden conectarse computadores, servidores, dispositivos de comunicaciones como concentradores, switches, enrutadores o cualquier otro hardware a la red, sin la participación y/o supervisión de personal autorizado por la Oficina de Tecnologías de la Información - 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 activos de información de la CVC es controlada mediante el formato Ingreso / salida de activos informáticos.

Los equipos portátiles y medios removibles que son retirados de las instalaciones de la CVC deben estar 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 desatendidos en lugares públicos, o dejar a la vista en 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 que allí se encuentre almacenada (en caso de ser necesario). Posteriormente, el equipo deberá ser sometido a

4.11.8. Política de 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 equipos de cómputo conectados a la red corporativa cerraran su sesión de forma automática al pasar como mínimo 8 minutos de inactividad.

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.

4.11.9. Política de equipo desatendido

Los equipos de cómputo que no son de propiedad de CVC, y requieran conexión a recursos de red corporativa, deberán ser revisados por el grupo de MSI (Mesa de Servicio Integral), donde se validarán parámetros de seguridad como antivirus y software licenciado, adicionalmente los equipos deben ser registrados en una base de datos para el control de activos en la Red.

4.11.10. Cambio y/o reposición de equipos de cómputo

La vida útil de un equipo de cómputo está determinada en muchas ocasiones por el manejo y cuidado del mismo, también por la periodicidad del mantenimiento preventivo y por la duración de sus componentes electrónicos.

En la CVC se ha determinado que la vida útil de un equipo de cómputo es de 6 años, si este no ha presentado fallas electrónicas.

El control del tiempo de funcionamiento del equipo debe ser registrado desde que se ingresa al inventario, hasta que se da de baja.

La Oficina de Tecnologías de la Información - OTI, deberá mantener actualizado el inventario de equipos de cómputo, con el fin de identificar equipos obsoletos, los cuales deberán ser dados de baja, para minimizar la materialización de riesgos de seguridad de la información.

Los equipos obsoletos deberán ser procesados de acuerdo al numeral 4.11.7 de la presente política y deberá ser dados de baja.

Los equipos catalogados como obsoletos deberán ser reemplazados por equipos nuevos, previo informe de diagnóstico técnico generado por la OTI.

4.12. SEGURIDAD DE LAS OPERACIONES

4.12.1. Documentación técnica

Cuando se realice alguna actividad de tipo técnico sobre los activos de información críticos se deben tener en cuenta los manuales técnicos o de usuario generados por el fabricante o proveedor autorizado.

La Oficina de Tecnologías de la Información - OTI, deberá proveer a su personal los documentos técnicos necesarios para gestionar los recursos y servicios tecnológicos.

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 los lineamientos del procedimiento Gestión de Cambios Tecnológicos PT.0720.28 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 de Gestión de Cambios Tecnológicos PT.0720.28 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 los lineamientos del procedimiento de Gestión de la Capacidad Tecnológica PT.0720.26.

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 ambientes en sistemas de información

Para la gestión de los sistemas de información corporativos, se debe contar con ambientes independientes para las fases de desarrollo, pruebas y producción.

Los ambientes de desarrollo, pruebas y producción contarán con control de acceso según los perfiles autorizados por la OTI.

4.12.5. Protección contra códigos maliciosos

Se deben proteger contra códigos maliciosos las estaciones de trabajo, equipos portátiles, servidores y demás equipos computacionales que se conecten a la red de la CVC.

Los contratistas que hagan uso de sus equipos portátiles personales deben contar con un software antivirus licenciado y actualizado en su base de conocimiento.

El servicio de antivirus corporativo no requiere de solicitud o autorización por parte de los usuarios para su operación. Todos los equipos de propiedad de la CVC deben tener el antivirus instalado y activo.

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.
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, de acuerdo al procedimiento de Gestión de Copias de Seguridad PT.0720.27.
La OTI establecerá las políticas y reglas de copias de seguridad a aplicar para los sistemas de información y bases de datos.
Los administradores de las bases de datos, aplicaciones y servicios, deben cumplir con las por la políticas de copias de seguridad establecidas OTI.
Las copias de seguridad de los activos de información críticos se deben almacenar en un área adecuada y con control de acceso, aplicando los controles para la protección de los medios de respaldo.
Las copias de seguridad se guardarán con el objetivo de restablecer los sistemas o servicios cuando se presenten situaciones como: borrado de datos, incidentes de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores, computadores o por requerimientos legales que soliciten recuperar una copia de seguridad específica.
Las copias de seguridad deberán ser validadas por responsable del activo de información para comprobar su integridad.
Es responsabilidad de cada funcionario y contratista, realizar periódicamente copia de seguridad de la información que está bajo su custodia de forma local y/o en nube. Para ello debe solicitar a la OTI los recursos necesarios, los cuales serán asignados de acuerdo a la capacidad.
La información que se almacena en los equipos asignados a los funcionarios o contratistas es de propiedad de la CVC, 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.

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 tener habilitado el registro de eventos (logs) con el fin de realizar seguimiento y control.
Los sistemas de información que sean desarrollados o adquiridos para la CVC, deben contar con un módulo de registro de transacciones que permita la auditoría.

4.12.7.2. Protección de la información de registro

La OTI con el fin de proteger la información de registro de eventos, implementará mecanismos de copiado de logs a un medio externo aplicando control de acceso.

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 con el controlador de dominio.

4.13. CONTROL DE SOFTWARE OPERACIONAL

4.13.1. Instalación de software

El proceso de instalación y desinstalación de software debe ser realizado exclusivamente por el personal de la OTI.
Para la instalación de software se deben seguir los siguientes lineamientos:

a. El software propietario debe contar con su respectiva licencia y en el caso del software libre debe estar permitido el uso comercial.
b. Se deben utilizar instaladores suministrados directamente por el fabricante y verificar la integridad por medio del código hash.
c. Debe dejarse evidencia de la instalación del software autorizado.

Se debe capacitar a los usuarios y al personal técnico en la operación y funcionalidad de los sistemas de información, sus actualizaciones o mejoras.
Todos los sistemas de información deben contar con manuales de instalación actualizados.

4.13.2. Gestión de la vulnerabilidad técnica

La OTI, es responsable de verificar de manera periódica la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los activos 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 los lineamientos del procedimiento de Gestión de Cambios Tecnológicos PT.0720.28.

4.13.3. Consideraciones sobre auditorías 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 deben acordar con los jefes de la(s) dependencia(s) involucradas.
b. El alcance de las pruebas técnicas de auditoría se deben concertar con la OTI.

d. La información recolectada como evidencia dentro del proceso de auditoría debe ser tratada con los principios de confidencialidad e integridad.

4.14. SEGURIDAD DE LAS COMUNICACIONES

4.14.1. Seguridad en las redes de comunicaciones

La OTI debe implementar mecanismos de segmentación y control de tráfico en las redes para mejorar el desempeño, proteger la confidencialidad y preservar la integridad y disponibilidad de la información.

El acceso a la red corporativa estará controlado por la OTI

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.

Cuando se detecte un comportamiento anormal en la red de datos corporativa, se deberán aplicar medidas restrictivas para mitigar los riesgos y preservar la disponibilidad y desempeño de la red.

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 deGestión de Activos de Información PT.0720.25 (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 contratados externamente o desarrollados en la CVC. Para ello, debe tener en cuenta:

a. Principio de autenticación:

Los sistemas de información deben contar con herramientas de autenticación segura, por ejemplo, la implementación de segundos factores de autenticación y un sistema de gestión de contraseñas que exija grados de complejidad, el cambio periódico de las mismas y que guarde un historial para evitar su reúso.

b. Principio de confidencialidad:

Los sistemas de información deben contar con control de acceso basado en roles y se deben asignar permisos de acuerdo con las funciones y responsabilidades de los usuarios.

Se debe controlar el acceso a nivel de datos limitando el acceso a información específica, según la autorización del usuario.

Las contraseñas se deben almacenar cifradas y restringir el acceso a las mismas a los usuarios.

El acceso a las bases de datos de los sistemas de información se permitirá únicamente a los administradores (DBA) de las mismas.

Los sistemas de información deberán implantar protocolos seguros para la transferencia de información.

c. Principio de integridad:

Los sistemas de información deben contar con mecanismos para detectar el acceso, inserción, actualización y eliminación de información realizada por los usuarios (registro de eventos).

Se debe aplicar la transaccionalidad en las operaciones realizadas en los SI para garantizar la integridad de la información.

Se deben aplicar controles a nivel de interfaz que validen la integridad de los datos registrados.

d. La gestión de usuarios en los sistemas de información se debe realizar de acuerdo a los lineamientos del procedimiento de Gestión de Usuarios PT.0720.24.

4.15.2. Seguridad en los procesos de desarrollo y soporte

4.15.2.1. Política de desarrollo seguro

Los sistemas de información deben ser desarrollados de acuerdo a las etapas establecidas en las metodologías de desarrollo de software aplicando métodos para la protección de la información.

Se deben desarrollar funcionalidades que permitan mitigar los riesgos de seguridad en cuanto a la integridad, disponibilidad y confidencialidad de la información.

Se deben emplear motores de base de datos que cumplan con las propiedades de atomicidad, consistencia, aislamiento y durabilidad (ACID).

Los sistemas de información deben contar con acuerdos de nivel de servicio y soporte vigente.

La contratación del desarrollo o adquisición de software debe ser apoyada por la OTI,con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.

Los sistemas de información deben contar con la documentación legal, técnica, funcional y comercial.

Se debe incentivar el uso de software libre con autorización en ambiente empresarial y comercial.

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

Los cambios en sistemas deben realizarse de acuerdo con el procedimiento deGestión de Cambios Tecnológicos PT.0720.28.

del ciclo de vida de desarrollo del software y se debe tener en cuenta los siguientes principios:
Principio de Menor Privilegio: Otorgar a los usuarios y componentes del sistema solamente los privilegios mínimos necesarios para realizar sus funciones específicas. Esto ayuda a limitar el daño potencial que puede causarse en caso de una brecha de seguridad.
Defensa en Profundidad: Aplicar múltiples capas de seguridad en diferentes niveles del sistema para que, si una capa falla, las demás puedan proporcionar protección adicional. Esto incluye medidas como firewalls, monitoreo de intrusiones y cifrado de datos.
Principio de Seguridad por Diseño: Integrar la seguridad desde el inicio del proceso de diseño y desarrollo, en lugar de intentar parchear problemas de seguridad una vez que el software esté completo. Esto implica considerar las amenazas potenciales desde el principio y diseñar contramedidas adecuadas.
Mínima Superficie de Ataque: Reducir la exposición y el número de puntos de entrada posibles para los atacantes. Esto implica eliminar componentes innecesarios, deshabilitar servicios no utilizados y minimizar la superficie de ataque general.
Validación y Sanitización de Entradas: Validar y limpiar adecuadamente todas las entradas de usuario y datos externos para prevenir inyecciones de código malicioso, como ataques de SQL o XSS (Cross-Site Scripting).
Actualizaciones y Parches: Mantener el software actualizado con los últimos parches y actualizaciones de seguridad para abordar las vulnerabilidades conocidas. Esto se aplica tanto al software de terceros utilizado en su aplicación como a sus propias implementaciones.
Principio de Separación de Responsabilidades: Dividir el sistema en componentes separados y asignar responsabilidades específicas a cada uno. Esto ayuda a evitar que una falla en un componente comprometa la seguridad de todo el sistema.
Auditoría y Monitorización: Implementar mecanismos de auditoría y monitoreo para rastrear actividades sospechosas y detectar posibles brechas de seguridad en tiempo real.
Cifrado: Utilizar el cifrado para proteger los datos en reposo y en tránsito. Esto garantiza que incluso si los datos son comprometidos, no sean útiles para los atacantes sin la clave de descifrado.
Pruebas de Seguridad: Realizar pruebas de seguridad regulares, como pruebas de penetración y análisis de vulnerabilidades, para identificar y abordar posibles debilidades en el sistema.
Educación y Concienciación: Capacitar al equipo de desarrollo y a los usuarios finales en prácticas de seguridad y concienciarlos sobre las posibles amenazas y mejores prácticas de seguridad.
Gestión de Vulnerabilidades: Establecer un proceso para gestionar las vulnerabilidades descubiertas, priorizarlas y aplicar soluciones en función de su gravedad.
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 seguro de desarrollo de software
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 de desarrollo y de 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 de Gestión de Cambios Tecnológicos PT.0720.28.
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 de software 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.
Cuando se contraten desarrollos a la medida para la CVC, se debe acordar con el contratista la transferencia de los derechos de autor y hacer entrega del código fuente.
La CVC debe exigir la evidencia de realización de pruebas de seguridad en el desarrollo de software por parte de terceros.
Los principios de desarrollo seguro se deben aplicar a desarrollos contratados con terceros.
La OTI debe apoyar a las dependencias que contraten desarrollos externos para asegurar que se realicen pruebas de aceptación del software, con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.
Se debe incluir en los acuerdos contractuales, el cumplimiento de la normatividad relacionada con la seguridad y protección de la información, tanto en la etapa de desarrollo, como en el producto final.
Se debe incluir en los acuerdos contractuales, el derecho de la CVC a realizar auditorías durante cualquiera de las etapas del desarrollo del software.
En los contratos se deben establecer acuerdos de niveles de servicio (ANS)
Se debe incluir en los acuerdos contractuales la entrega de documentos técnicos y funcionales, que describan la estructura interna del sistema, diccionario de datos, librerías, componentes, manuales y demás documentos relacionados con el software.
4.15.2.6. Pruebas de seguridad de software
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.
Se deben realizar pruebas al software, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de

Las pruebas de seguridad se deben llevar a cabo en el ambiente de pruebas, para asegurar que el sistema no incluya vulnerabilidades y que sea confiable.
No se deber recibir a satisfacción un software que no cumpla con la totalidad de los requisitos de seguridad, documentando los riesgos que puedan atentar con la confidencialidad, integridad y disponibilidad de la información
4.15.3. Datos de prueba
Los datos que se utilicen para realizar pruebas no deberán revelar información sensible o confidencial de la CVC y se deberán utilizar métodos que permitan enmascarar y cifrar la información, dando 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 comunicará 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, los siguientes requisitos de seguridad de la información:
a. Cláusula de confidencialidad.

b. Cláusula de responsabilidades en seguridad posteriores a la ejecución de los contratos (Ejemplo, confidencialidad durante 5 años, después del vencimiento del plazo contractual).
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 de Gestión de Incidentes de Seguridad de la Información PT.0720.29.
e. Etiquetado y manejo de la información de acuerdo con las directrices del procedimiento de Gestión de Activos de Información PT.0720.25.
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.
g. Se debe suscribir acuerdos de confidencialidad y no divulgación de información. Para ello se deberá utilizar el formato Acuerdo de Confiedncialidad y No Divulgación de la CVC u otro que contemple como mínimo esos controles.
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 de Gestión de Incidentes de Seguridad de la Información PT.0720.29.
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: itmesaintegral.principal@cvc.gov.co – Edwin.ruano@cvc.gov.co
b. Extensión: 55555 – 1286
d. Software de gestión de incidentes: ARQ-Security
Asimismo, se deberán notificar situaciones tales como: personas ajenas en oficinas y centros de cómputo, correos maliciosos o sospechosos, reinicio inesperado 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 EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO
4.18.1. Continuidad de la seguridad de la información
La CVC debe planificar e implementar un plan de continuidad del negocio que integre los requisitos de la seguridad de la información, en situaciones de crisis o ante desastres.
La CVC debe realizar pruebas de los controles de seguridad de continuidad del negocio anualmente, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
4.18.2. Redundancias
La CVC debe establecer e implementar 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 debe realizar pruebas al DRP anualmente, 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

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 que todo software que se ejecute en la CVC, cuente con una licencia de uso.

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. La reproducción no autorizada es una violación a ley de propiedad intelectual.

Los supervisores de contratos deben asegurarse de cumplimiento de las cláusulas de propiedad intelectual y derechos de autor en los contratos.

4.19.1.3. Protección de registros

La CVC se obliga a proteger todos los registros que evidencien el cumplimiento de los requisitos normativos, legales o regulatorios contra la pérdida de confidencialidad, disponibilidad e integridad.

4.19.1.4. Privacidad y protección de información de datos personales

La CVC es responsable del tratamiento de los datos personales, tal y como se define en la Ley 1581 de 2012 y la política de protección de datos de la CVC.

La CVC debe implementar los controles necesarios para su protección y en ningún momento divulgará esta información si la debida autorización.

4.19.2. Revisiones de seguridad de la información

4.19.2.1. Revisión independiente de la seguridad de la información

Para evaluar el desempeño del SGSI se pueden realizar auditorías internas al menos una vez al año, que permitan evaluar la eficacia de los controles aplicados a los riesgos de seguridad identificados en la CVC.

4.19.2.2. Cumplimiento con las políticas y normas de seguridad

Los Directores, Jefes oficina, funcionarios y contratistas, deben promover el cumplimiento de las políticas y procedimientos de seguridad de la información en la CVC.

4.19.2.3. Revisión del cumplimiento técnico

El jefe de la Oficina de Tecnologías de la Información (OTI) debe coordinar la revisión una vez al año de los sistemas de información, para determinar el cumplimiento con las políticas y procedimientos de seguridad de la información.

5. ANEXOS

Anexo 1: MN.0720.01 Sistema de Gestión de la Seguridad de la Información Anexo 2: PT.0720.24 Gestión de Usuarios
Anexo 3: PT.0720.25 Gestión de Activos de Información Anexo 4: PT.0720.26 Gestión de la Capacidad Tecnológica Anexo 5: PT.0720.27 Gestión de Copias de Seguridad Anexo 6: PT.0720.28 Gestión de Cambios Tecnológicos
Anexo 7: PT.0720.29 Gestión de Incidentes de Seguridad de la Información
Anexo 8: Formato Acuerdo de Confidencialidad y No Divulgación de Información de la CVC

EDWIN RUANO GAMBOA @ 2024-12-06, 9:59:40