Manual de Políticas Complementarias de Seguridad de la Información

2025

Tabla de contenido

1. Introducción

Canal Capital, requiere definir las responsabilidades y conductas que se deben mantener para conformar un ambiente seguro en la Entidad, las cuales se establecen a través de su Política de Seguridad y Privacidad de la Información, Manual de Políticas Complementarias de Seguridad de la Información y Manual del Sistema de Gestión de Seguridad de la Información para que soporten el manejo de la información y se constituyan como parte fundamental de Sistema de Gestión de Seguridad de la Información de Canal Capital convirtiéndose así en la base para la implementación de controles, procedimientos y estándares definidos.

Teniendo en cuenta lo anterior, el presente Manual tiene como finalidad establecer los principios orientadores en seguridad de la información que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad y continuidad de la información y recursos tecnológicos de Canal Capital, así como dar lineamientos para la aplicación de mecanismos que prevengan la vulneración de la seguridad y privacidad de la información, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información-SGSI.

2. Objetivo

Dar a conocer los lineamientos de seguridad para asegurar los activos de información y de los recursos tecnológicos que soportan las operaciones de Canal Capital, que sean accedidos solo por aquellas personas que tienen la necesidad legítima para el cumplimiento de sus funciones u obligaciones (confidencialidad), que esté y sea protegida contra las alteraciones no planeadas y realizadas con o sin intención (integridad) y que esté disponible cuando esta sea requerida (disponibilidad), adicionalmente debe disminuir con el impacto de riesgos, amenazas, vulnerabilidades y reducir las ocurrencia de cualquier ataque a estos.

3. Alcance

El Manual de Políticas Complementarias de Seguridad de la Información es aplicable para todas las funciones administrativas y de control que deben ser cumplidas por cada uno de los colaboradores, contratistas y terceros que laboren, presten sus servicios o tengan algún tipo de relación con la Entidad a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos.

4. Definiciones

Acción Correctiva: Medida orientada a eliminar la causa de cualquier amenaza, evento, riesgo o vulnerabilidad asociada a la seguridad de la información.
Acción Preventiva: Medida orientada a prevenir cualquier amenaza, evento, riesgo o vulnerabilidad asociada a la seguridad de la información.
Activo de Información: Datos o información que tienen un valor para una Entidad.
Amenaza: Circunstancia, suceso o persona con el potencial para dañar un sistema mediante la destrucción, divulgación, modificación de datos o negación de servicios.
Análisis de Riesgo: método cualitativo o cuantitativo para la evaluación del impacto de riesgo en la toma de decisiones.

Aplicaciones: Es todo software que se utiliza para la gestión o manejo de la información.
Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona en cualquiera de los sistemas de información de la entidad.
BackUp: Parámetros que determinan qué equipo o que información debe incluirse en una copia de respaldo dentro de la entidad.
Código malicioso: Es un código informático que crea brechas de seguridad para dañar un

sistema informático.

Confidencialidad: Mantener la información reservada oculta a individuos, entidades o procesos no autorizados.

Control: Procedimiento, procesos, políticas que permiten mantener el riesgo de la seguridad de la información por debajo del riesgo presente.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. Debe entonces entenderse el "dato personal" como una información relacionada con una persona natural (persona individualmente considerada).

Denegación de Servicio: Es una acción iniciada por un ataque a un sistema objetivo, que provoca la denegación a los usuarios legítimos forzando su cierre o conllevando a una inoperatividad.

Disponibilidad: Mantener la información accesible a quien la necesita en el momento que la necesite.

Dispositivo: Es un ordenador que se puede utilizar para acceder a los servicios de red, computador Tablet, Smartphone.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

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

Ingeniería Social: Método utilizado para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la divulgación de información.

Integridad: Prevenir la modificación no autorizada de la información.

Política: Medidas necesarias para garantizar la seguridad de las tecnologías de la información.

Riesgo: probabilidad de que ocurra un evento no deseado o un peligro que pueda causar daño, lesión o enfermedad contratiempo.

Seguridad de la Información: Según ISO 27002 es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguridad Informática: Encargada de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de gestión de seguridad de la información seguro y confiable.

Seguridad Física: Límites mínimos que se deben cumplir en cuanto a los perímetros de seguridad, de forma que se puedan establecer controles.

Seguridad Lógica: Integrar mecanismos y procedimientos que permitan monitorear el acceso a los activos de la información.

SGSI Sistema de Gestión de Seguridad de la Información: Es un mecanismo que permite preservar la confidencialidad, integridad y disponibilidad de la información.

Usuario: Cualquier persona que haga uso de los servicios de red proporcionados por la entidad tales como equipos de cómputo, sistemas de información y redes.
Virus: Es un tipo de software o aplicación que tiene como objetivo alterar el normal funcionamiento de los equipos tecnológicos, sin permiso o conocimiento de los usuarios.
Vulnerabilidad: Condición de un sistema que lo hace susceptible a una amenaza.

5. Marco legal

Canal Capital y los usuarios operaran siempre dentro del Marco Legal aplicable en Colombia, manteniendo siempre como objetivo asegurar la integridad, confidencialidad y disponibilidad de la Información en la Entidad, actuando de acuerdo con las políticas generales establecidas para las entidades oficiales y manteniendo siempre un comportamiento profesional, compromiso y calidad. El marco normativo de Canal Capital se encuentra centralizado en el Nomograma Institucional.

6. Documentos de referencia

- Norma IS071EC 27001:2022
- Norma ISO/IEC 27002:2013
- Manual de Sistema de Gestión de Seguridad de la Información.
- Declaración de Aplicabilidad SOA.
- Instrumento de Evaluación MSPI.
- Política de Seguridad y Privacidad de la Información.
- Política de Tratamiento de Datos Personales.

7. Política de seguridad, digital y privacidad de la información

Asegurar y administrar la información y los recursos tecnológicos para que sean accedidos solo por aquellas personas que tienen la necesidad legítima para el cumplimiento de sus funciones (confidencialidad), que esté y sea protegida contra las alteraciones no planeadas y realizadas con o sin intención (integridad) y que esté disponible cuando esta sea requerida (disponibilidad), adicionalmente debe disminuir con el impacto de riesgos, amenazas y vulnerabilidades y reducir las ocurrencias de cualquier ataque a esta.

Para asegurar la información y los recursos tecnológicos, la Oficina de Gestión de Tecnologías de la Información y Comunicaciones de Canal Capital establece la articulación

con la Política de Seguridad y Privacidad de la Información y los objetivos de seguridad de la información así:

- Consolidar la seguridad de la información como una línea estratégica en Canal Capital definiendo, comunicando y generando la cultura de buenas prácticas para el acceso, uso y manejo de la información y recursos tecnológicos, por parte de todos los funcionarios, contratistas y terceros relacionados con Canal Capital.
- Proteger los activos de información, y salvaguardar la plataforma tecnológica en aras de proteger la imagen, los intereses y el buen nombre de la Entidad, gestionando las amenazas y vulnerabilidades en la plataforma tecnológica para reducir los riesgos asociados con la seguridad de la información y dar cumplimiento a los lineamientos establecidos en la Política de Gobierno Digital y Seguridad Digital respecto a la Seguridad de la Información.

8. Políticas específicas de seguridad y privacidad de la información

8.1 Política Organizacional de Seguridad de la Información

Canal Capital establece un Manual del Sistema de Gestión de Seguridad de la Información, una Política de Seguridad y Privacidad de la Información, un Manual de Políticas Complementarias de Seguridad de la Información y un Manual del Sistema de Gestión de Seguridad de la Información, donde se definen roles y responsabilidades para la administración, operación y gestión de la Seguridad y Privacidad de la Información.

8.2 Normas que actúan en la Política Organizacional de Seguridad de la Información

Normas dirigidas a la Gerencia de Canal Capital

- Definir y establecer los roles y responsabilidades relacionados con la Seguridad de la Información en niveles administrativos y operativos.
- Revisar y aprobar las políticas y normas de seguridad de la información contenidas en el presente manual.
- Promover y facilitar activamente la divulgación del Manual de Políticas Complementarias de Seguridad de la Información a los colaboradores, contratistas y terceros de la entidad.
- Asignar los recursos, infraestructura tecnológica y personal idóneo para la gestión de la seguridad y privacidad de la información de la entidad.

Normas dirigidas a Control Interno

- Planear y ejecutar auditorías al Sistema de Gestión de Seguridad de la Información (SGSI) con el fin de determinar el cumplimiento del Manual de Políticas Complementarias de Seguridad de la Información.
- Informar al área correspondiente sobre los hallazgos y observaciones de las auditorías.
- Validar y monitorear la implantación de las Políticas Complementarias de la Seguridad de la Información.

Normas dirigidas la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Actualizar y presentar periódicamente las Políticas Complementarias de Seguridad de la Información, la metodología del análisis de riesgos según se considere.
- Analizar los incidentes de seguridad y avisar a las autoridades cuando sea necesario.
- Verificar el cumplimiento del Manual de Políticas Complementarias de Seguridad de la Información.
- Asignar roles y responsabilidades a los funcionarios para la administración y gestión de la Infraestructura Tecnológica.

Normas dirigidas al área de Recursos humanos

- Controlar y salvaguardar la información del personal de planta de la Entidad, según la normatividad vigente.
- Reportar oportunamente a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones las diferentes situaciones administrativas que se presenten, con el fin de gestionar el control de acceso a los diferentes sistemas de información y recursos tecnológicos de los colaboradores.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Implementar y custodiar los acuerdos de confidencialidad y de no divulgación de información en los actos administrativos de toma de posesión de cargos de los colaboradores y demás documentos equivalentes que así lo requieran.
- Tratar y salvaguardar la información de datos personales de los colaboradores de la Entidad, en concordancia con sus funciones y la normatividad vigente.

Normas dirigidas a Gestión Jurídica

- Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que

involucren actuaciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Representar a la Entidad en procesos judiciales y administrativos ante las autoridades competentes relacionados con la seguridad y privacidad de la información.
- Realizar el debido tratamiento y custodia de los datos personales, documentación e información que en desarrollo de sus funciones tenga bajo su cuidado o la que se requiera recolectar, así como impedir o evitar la sustracción, destrucción, ocultamiento o uso indebido de terceros no autorizados según la normatividad vigente.

Normas dirigidas a Gestión Contractual

- Asegurarse de que los contratos incluyan cláusulas sobre seguridad de la información y reportar oportunamente cualquier cambio relevante (vinculación, terminación, cesión, etc.) para gestionar el acceso a los sistemas de información.
- Verificar que los contratos o convenios contengan cláusulas de derechos de autor, confidencialidad y no divulgación de la información, según corresponda.
- Realizar el debido tratamiento y custodia de los datos personales, documentación e información que en desarrollo de sus obligaciones tenga bajo su cuidado o la que se requiera recolectar, así como impedir o evitar la sustracción, destrucción, ocultamiento o uso indebido de terceros no autorizados según la normatividad vigente.

Normas dirigidas a todos los Colaboradores, Contratistas y Terceros

- Dar cumplimiento a los manuales, procedimientos, lineamientos y políticas del Sistema de Gestión de Seguridad de la Información.
- Custodiar y cuidar la documentación e información que por razón de su empleo, cargo, obligaciones o funciones conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Reportar inmediatamente los eventos o incidentes de seguridad de la información al correo de Canal Capital tic@canalcapital.gov.co.
- Dar cumplimiento a la Política de protección de datos personales de la Entidad.
- Aceptar, firmar y cumplir los acuerdos de confidencialidad y de no divulgación de la información.
- Participar en las sensibilizaciones y capacitaciones programadas en el marco del Sistema de Gestión de Seguridad de la Información.
- Mantener la confidencialidad de la información con terceros y fuera de la Entidad.
- Incurrirá en sanciones disciplinarias al violar o incumplir las responsabilidades y lineamientos definidos en el Manual de políticas de seguridad de la información.

- Clasificar la información e implementar los controles pertinentes de acuerdo con el nivel de confidencialidad, integridad y disponibilidad que se requiera.
- Está totalmente prohibido instalar algún tipo de software en los equipos institucionales, sin la debida autorización y aprobación de la Oficina de Gestión de Tecnologías de la Información y Comunicaciones
- Las herramientas colaborativas, el correo electrónico y otros recursos provistos por la Entidad, están a disposición del personal para el cumplimiento adecuado de sus funciones, obligaciones y actividades contractuales. El uso indebido de estos recursos puede dar lugar a acciones disciplinarias o legales correspondientes.
- Tratar y salvaguardar la información de datos personales que, con motivo del ejercicio de sus funciones u obligaciones, requiera recolectar, almacenar, gestionar, según la normatividad vigente.

8.3 Política para el uso de dispositivos móviles y teletrabajo

Garantizar, monitorear, proteger y supervisar la conexión y uso de los dispositivos móviles de todos los colaboradores, contratistas y terceros, que usen las redes corporativas de la entidad.

8.3.1 Normas generales para el uso de dispositivos móviles propios

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Proveer un servicio de red inalámbrica que garantice la conectividad de los dispositivos móviles dentro de la entidad.
- Proveer un servicio de red inalámbrica con diferentes perfiles de usuario que garantice la confidencialidad, integridad y disponibilidad de la información.
- Garantizar que las conexiones a las redes móviles de la entidad solo cuenten con los servicios necesarios para el uso de los dispositivos móviles.
- Configurar la opción de borrado remoto de los dispositivos móviles propios de la entidad.
- Configurar los dispositivos móviles de la entidad para que estos se bloqueen automáticamente después de un tiempo de inactividad no mayor a 30 segundos.

Normas generales para el Teletrabajo

- Aplicar las pautas establecidas en la GUÍA PARA CONEXIONES REMOTAS de Canal Capital.
- La Entidad debe establecer procedimientos para la solicitud y autorización del Teletrabajo.
- La Oficina de Gestión de Tecnologías de la Información y Comunicaciones será la encargada de implementar los controles de seguridad lógicos y tecnológicos necesarios para proteger la confidencialidad, integridad y disponibilidad de la información en la modalidad de Teletrabajo.
- Las herramientas de chat, almacenamiento y reuniones aprobadas por La Entidad son las herramientas colaborativas licenciadas, las cuales todos los colaboradores deben mantener activas durante su horario laboral y responder con la debida diligencia, tal como si estuviesen realizando sus funciones y actividades en las instalaciones de la Entidad.

Normas dirigidas a todos los Colaboradores, Contratistas y Terceros

- Hacer buen uso de las redes inalámbricas de la entidad y usar estas únicamente para realizar actividades laborales y no personales que pongan en riesgo la seguridad de la información de la entidad.
- No modificar las configuraciones ni instalaciones previas realizadas por la Oficina de Gestión de Tecnologías de la Información y Comunicaciones de la entidad.
- No guardar información personal en los dispositivos móviles de la entidad.
- Evitar conectar los dispositivos móviles de la entidad a redes públicas o gratuitas.

8.4 Normas generales para el uso de dispositivos móviles no corporativos

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Dar a conocer las Políticas de Seguridad de la Información de Canal Capital y asegurar que se cumpla esta normatividad.
- Asegurar las redes LAN e inalámbrica de la entidad con controles que eviten el acceso no autorizado a los recursos de red y tecnológicos de la entidad.
- Garantizar que las conexiones a las redes móviles de la entidad solo cuenten con los servicios necesarios para el uso de los dispositivos móviles no corporativos.
- Analizar y mitigar las vulnerabilidades y/o software malicioso que puedan presentar los dispositivos móviles no corporativos.
- Asegurarse que el software instalado en los dispositivos móviles no corporativos

cumpla con las normas de propiedad intelectual y su debida autenticidad.

- Realizar monitoreo y control de tráfico de datos de los dispositivos móviles no corporativos.
- Cumplir con los acuerdos de confidencialidad exigidos por Canal Capital, en función de sus actividades laborales.
- Eliminar los datos propios de Canal Capital del usuario cuando éste no tenga ninguna vinculación con la entidad.

Normas dirigidas a todos los Colaboradores, Contratistas y Terceros

- Conocer y aceptar la normatividad dada por Canal Capital para el uso de dispositivos móviles no corporativos.
- Asegurar que el software instalado en los dispositivos móviles no corporativos es legal y que no incumple con las normas establecidas por Canal Capital.
- Hacer únicamente uso de los recursos de red asignados por Canal Capital.
- Abstenerse de instalar aplicaciones que pongan en riesgo la seguridad de la información al interior de Canal Capital.
- Tener instalado, debidamente licenciado y actualizado un antivirus y que este realice un análisis automático de todos los recursos del equipo de cómputo.
- Evitar en lo posible almacenar información sensible de propiedad de Canal Capital.
- Al finalizar la vinculación con Canal Capital, se obliga al colaborador a permitir la revisión final del dispositivo móvil con el fin de borrar de forma segura los recursos de red y la información propia de la entidad.

8.5 Política de Seguridad de los Recursos Humanos

Canal Capital debe asegurar que todos los Colaboradores, Contratistas y Terceros, conozcan los derechos, deberes y responsabilidades dependiendo de su actividad dentro de la entidad, con el fin de minimizar los riesgos de fraude, fuga o cualquier uso inadecuado de la información.

8.5.1 Antes de asumir el empleo

- El área de Recursos Humanos, debe contar con procedimientos para la vinculación de personal, de acuerdo con la normatividad establecida para tal fin.
- Gestión Contractual, debe definir una lista de verificación que contenga los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con la normatividad vigente.
- El área de Recursos Humanos y Gestión Contractual, deben establecer mecanismos o controles necesarios para proteger la confidencialidad y privacidad

de la información contenida en las historias laborales y expedientes contractuales.

- Todo Colaborador o contratista, debe firmar un documento o cláusulas en las que se establezcan acuerdo de confidencialidad y no divulgación de la información reservada de Canal Capital.

8.5.2 Durante la ejecución del empleo

- Una vez formalizado el proceso de vinculación, el jefe inmediato, supervisor o el delegado del área para tal fin, debe solicitar a través de la mesa de ayuda la apertura del inventario y demás servicios que requiera el colaborador, contratista o tercero, para la ejecución de sus funciones u obligaciones contractuales.
- La Oficina de Gestión de Tecnologías de la Información y Comunicaciones y el personal de apoyo que se requiera debe diseñar y ejecutar de manera permanente, un plan de sensibilización en seguridad de la información, con el fin de apoyar la protección adecuada de la información.
- Es responsabilidad del colaborador, contratista o personal provisto por terceros, informar de los incidentes de seguridad de la información a través de los medios dispuestos por la Oficina de Gestión de Tecnologías de la Información y Comunicaciones para tal fin.

8.5.3 Terminación y cambio de empleo

- Es responsabilidad del Colaborador y Contratista realizar la entrega de la información propia de Canal Capital, que se encuentra en gestión por parte de estos, cuando existe una novedad de retiro, investigación, inhabilidades, o cambio de funciones.
- El supervisor del contrato o a quien éste delegue debe recoger y custodiar la información de Canal Capital bajo la responsabilidad del contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
- La Oficina de Gestión de Tecnologías de la Información y Comunicaciones debe parametrizar en el directorio activo, la inactivación automática de los accesos y credenciales a los diversos sistemas de información o aplicativos a contratistas, teniendo en cuenta la fecha de terminación del contrato. Para los funcionarios de planta se realiza conforme a la notificación del área de Recursos Humanos sobre la terminación de contrato.
- Se creará una copia de respaldo del buzón de correo electrónico, y se realizará la transferencia de la propiedad de los documentos de Drive y/o unidades compartidas al jefe inmediato o supervisor del contrato con la previa solicitud del mismo.
- Se debe realizarla devolución del carné en caso de que aplique, tarjeta de acceso o cualquier distintivo de autenticación (a la oficina de Recursos Humanos o Gestión

de Tecnologías de la Información y Comunicaciones), que lo acredite como colaborador, contratista o tercero de Canal Capital.

8.6 Política de teletrabajo y conexiones remotas

Canal Capital debe proteger la información y sus recursos tecnológicos a los cuales se tiene acceso y es procesada en las instalaciones donde se realicen conexiones remotas o teletrabajo, esto con el fin de mantener la confidencialidad e integridad de la información.

8.6.1 Normas generales para el teletrabajo y conexiones remotas

Normas dirigidas la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Implementar y mantener métodos y controles seguros para establecer conexiones remotas hacia la infraestructura tecnológica de la entidad.
- Autorizar y asignar los permisos necesarios a la información requerida cuando sea necesario, esto por un determinado tiempo.
- Verificar que las conexiones remotas se realicen desde equipos identificados y con las credenciales de acceso asignadas.
- Llevar una bitácora donde se evidencie las conexiones remotas autorizadas y el motivo por el cual se realizó.
- La Oficina de Gestión de Tecnologías de la Información y Comunicaciones establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones u obligaciones contractuales de los colaboradores y contratistas, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.

Normas dirigidas a todos los Colaboradores, Contratistas y Terceros

- Mantener la confidencialidad de la información.
- Toda información gestionada por Canal Capital, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.
- Verificar que todas las conexiones sean cerradas de forma adecuada de servidores o recursos informáticos utilizados.
- Las conexiones se deben establecer por medio de VPN seguras y con doble factor de autenticación expedidas por la Oficina de Gestión de Tecnologías de la Información y Comunicaciones de la entidad.
- Por ningún motivo se pueden realizar conexiones remotas o sesiones de teletrabajo

sin la previa autorización de la Oficina de Gestión de Tecnologías de la Información y Comunicaciones de la entidad y el jefe o coordinador de contrato.

8.7 Política de control de acceso

Canal Capital debe implementar controles que garanticen la seguridad del acceso de la información e instalaciones de la entidad dando los permisos necesarios para el cumplimiento de las actividades laborales.

8.7.1 Normas para el control de acceso

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Los sistemas de información, equipos de procesamiento y comunicaciones administrados por la Oficina de Gestión de Tecnologías de la Información y Comunicaciones, deben contar con el procedimiento de control de acceso a los mismos.
- Las asignaciones de perfiles de usuarios con privilegios para los diferentes sistemas de información deben ser definidos por la Oficina de Gestión de Tecnologías de la Información y Comunicaciones.
- Los equipos de contratistas y terceros que requieran el acceso a la red LAN y WLAN deberán ser autorizados por la respectiva área donde laboran y por la Oficina de Gestión de Tecnologías de la Información y Comunicaciones.
- Asegurar las redes LAN e inalámbrica de la entidad con controles que eviten el acceso no autorizado a los recursos de red y tecnológicos de la entidad.
- Asegurar la asignación, bloqueo y eliminación de accesos otorgados sobre los recursos tecnológicos y de red de la entidad, en el momento de vincular, desvincular, por periodo de vacaciones, cambios de cargo y licencias de trabajo.

Normas dirigidas a Servicios Administrativos

- Garantizar la entrega de tarjetas de control de acceso para colaboradores y/o contratistas. Para el caso de visitantes se debe asignar carné digital de identificación como visitante, el cual deberá ser solicitado a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones.

Normas dirigidas a Control Interno

- Verificar periódicamente los permisos asignados sobre los recursos tecnológicos y

de red de la entidad.

Normas dirigidas a todos los Colaboradores, Contratistas y Terceros

- Hacerse responsable de las actividades y acciones realizadas sobre los recursos compartidos y la infraestructura tecnológica, de igual manera sobre los usuarios y claves de acceso asignadas.
- Por ningún motivo se deben compartir las cuentas de usuario a los recursos de red, infraestructura tecnológica, firma digital y correo electrónico asignados para el cumplimiento de las actividades laborales.
- Cumplir con las políticas y normas concebidas en el presente manual.
- Los carnés de identificación propios de la entidad son de uso personal e intransferible.

8.8 Política de uso de controles criptográficos

Canal Capital velará porque la información contenida en sus bases de datos, aplicaciones y copias de seguridad mantenga la confidencialidad e integridad de la información.

Se deben usar controles seguros en las siguientes actividades:

- Transferencias bancarias.
- Copias de seguridad.
- Transporte de información digital.

8.8.1 Normas para el uso de controles criptográficos

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- La Oficina de Gestión de Tecnologías de la Información y Comunicaciones debe asegurar que las copias de seguridad realizadas a los servidores de la entidad estén cifradas y mantengan su integridad.
- Definir estándares para la aplicación de controles criptográficos.
- Configurar la red inalámbrica con el estándar de cifrado más seguro, en la actualidad WPA2.
- Velar por el correcto uso y funcionamiento de los certificados digitales implementados en la entidad y los servicios que dependen de esto.
- Definir un inventario de certificados digitales, que uso específico tienen y que funcionarios o servicios hacen uso de estos.

Normas dirigidas a los Administradores de Token para transacciones bancarias)

- Definir inventario de token de seguridad, que uso específico tiene y cuales usuarios tienen acceso a ellos.
- Dar aviso a las entidades correspondientes en caso de pérdida o hurto de los token de seguridad.

- Velar por el buen funcionamiento de los token, en caso contrario realizar el cambio de estos.
- Los token son de uso personal e intransferible.
- Resguardar los token en sitios seguros manteniéndolos fuera del alcance de personas no autorizadas.

8.9 Política de escritorio y pantalla limpia

Reducir el acceso no autorizado, daño, pérdida, alteración o copia de información no autorizada durante horarios laborales o fuera de ellos por parte de terceros o funcionarios de la entidad que no estén a cargo del activo en mención.

8.9.1 Normas generales para el mantenimiento del escritorio y pantalla limpia

Normas dirigidas a todos los Funcionarios, Proveedores, Socios de Negocio y Terceros

- Cuando se realicen impresiones de documentos confidenciales, estas deben ser retiradas de forma inmediata de las impresoras y no deben permanecer sin custodia.
- No ingerir bebidas o comida en los puestos de trabajo.
- Los escritorios y oficinas deben permanecer despejados y libres de elementos que impidan el confort y el libre movimiento.
- Los Colaboradores, Contratistas y Terceros que tengan a cargo estaciones de trabajo o equipos tecnológicos de propiedad de Canal Capital deben bloquear estos en el momento de abandonar el puesto de trabajo con el fin de proteger el acceso indebido a la información en estos almacenada.
- Los documentos en desuso deben ser archivados o destruidos mediante los medios establecidos (por ejemplo, trituradora de papel).
- Se debe cerrar sesión en aplicaciones que contengan información confidencial.
- Evitar dejar unidades USB, discos duros externos u otros dispositivos de almacenamiento conectados sin supervisión.
- Todos los materiales deben estar almacenados adecuadamente en cajones, archivadores u otros espacios asignados.
- Por ningún motivo se deben poner, pegar (sticker, afiches) y/o alterar las partes

físicas de las estaciones de trabajo.

- Está estrictamente prohibido anotar contraseñas en hojas, post-its o cualquier medio físico visible (como debajo del teclado, en monitores o dentro de cajones).

8.10 Política para la transferencia de información

Canal Capital debe garantizar que el uso del correo electrónico institucional y la transferencia de información sean exclusivamente para el intercambio de información corporativa entre Colaboradores, Contratistas y Terceros, además de garantizar la confidencialidad y privacidad de la información contenida.

8.10.1 Normas generales para el uso de correo electrónico

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Garantizar que el acceso a las cuentas de correo sea exclusivamente por las plataformas designadas por la entidad.
- No permitir el uso de clientes de correo tales como Outlook, Thunderbird o Mail, solo se permitirá este uso por autorización de la dirección.
- Las firmas de correo electrónico deben estar estandarizadas y no deben ser modificadas por ningún motivo.
- La foto de perfil del correo electrónico debe ser corporativa y permitir la identificación clara de la persona responsable de la cuenta.
- Controlar la asignación de cuentas de correo y contraseñas de acceso, cambios de contraseñas, desbloqueo de cuentas e informes de uso.
- Generar campañas para concienciar con respecto a las precauciones de uso que se deben tener sobre el correo electrónico.

Normas dirigidas a todos los Colaboradores, Contratistas y Terceros

- Las cuentas de correo asignadas son de uso personal e intransferible, por ningún motivo se debe usar una cuenta de correo que no sea la del Colaborador.
- La información y mensajes deben ser exclusivamente relacionados con las actividades propias de la entidad, no para actividades personales.
- Los buzones de correo y la información allí contenida son de propiedad de Canal Capital.
- Abstenerse de realizar envío de correos electrónicos con archivos adjuntos con extensiones .exe (ejecutables), esto con el fin de evitar la propagación de códigos maliciosos.

- En periodo de vacaciones se debe informar al área de sistemas para que esta proceda a re-dirigir los correos a la cuenta de correo del funcionario que durante este periodo de tiempo sea asignado para el desarrollo de las actividades encomendadas.
- Cerrar la sesión de correo electrónico cada vez que se retire del puesto de trabajo o al finalizar la jornada laboral.
- No se deben descargar archivos adjuntos de los correos electrónicos sin tomar las medidas de seguridad correspondiente, esto con el fin de evitar el acceso y propagación de código malicioso en la red de la entidad.
- No enviar cadenas políticas, religiosas, publicitarias o material que no sea estrictamente laboral, esto se cataloga como correo spam.

8.11 Política de relaciones con los proveedores

Canal Capital debe controlar que toda relación con los proveedores, especialmente los que tienen acceso a la información sensible de la entidad, se comprometan a través de Acuerdos de Confidencialidad a mantener la Integridad, Confidencialidad y Disponibilidad de la Información, asegurando así que los productos y servicios adquiridos cumplen con los requerimientos exigidos por la entidad al momento de la contratación y posterior ejecución de las actividades encomendadas.

8.11.1 Normas para las relaciones con los proveedores

Normas dirigidas a todos los Funcionarios

- Establecer los requerimientos mínimos de seguridad con los que deben cumplir los proveedores de la entidad.
- Elaborar cláusulas en las que se asegure el tratamiento de la seguridad de la información y los recursos tecnológicos.
- Exigir certificaciones que avalen la calidad de los servicios o bienes adquiridos en el momento de la contratación.
- Realizar supervisión a las actividades de los servicios o bienes contratados.

8.12 Política uso de estaciones de trabajo

Canal Capital, para mitigar la pérdida y mal uso de los recursos tecnológicos, proveerá los recursos, controles y procedimientos que garanticen el mínimo de exposición al riesgo de las estaciones de trabajo.

8.12.1 Normas para el Uso de Estaciones de Trabajo

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Proveer los mecanismos necesarios para mantener la Confidencialidad, Integridad y Disponibilidad de la Información y la Infraestructura Tecnológica dentro y fuera de la entidad.
- Realizar periódicamente mantenimientos preventivos y correctivos de la Infraestructura Tecnológica.
- Establecer procesos de configuración seguros para las Estaciones de Trabajo que usen los funcionarios de la entidad.
- Establecer las condiciones que deben cumplir los equipos de cómputo personal, Smartphone, Tablet de terceros que requieran conectarse a la red LAN o WLAN de la entidad
- Aislar los equipos sensibles y críticos (servidores, firewall, switch, etc.) del acceso a personas que no estén autorizadas para su uso.
- Generar y aplicar lineamientos para la disposición segura de las estaciones de trabajo u otro elemento tecnológico ya sea cuando este sea dado de baja o cambie de usuario.

Normas dirigidas a Control Interno

- Incluir dentro del plan anual de auditorías la verificación aleatoria de estaciones de trabajo ubicadas en las diferentes áreas de Canal Capital y velar por el cumplimiento de las políticas complementarias de seguridad de la información que aplique a estas.

Normas dirigidas a todos los Funcionarios, Proveedores, Socios de Negocio y Terceros

- La oficina de Gestión de Tecnologías de la Información y Comunicaciones de Canal Capital es la única autorizada para realizar traslados, movimientos y asignaciones de estaciones de trabajo.
- Las fallas de software, hardware y configuración de las Estaciones de Trabajo e Infraestructura Tecnológica se deben informar a través de la mesa de ayuda de Canal Capital donde se atenderá la solicitud y se realizará la reparación que dé a lugar.
- Los Funcionarios, proveedores, socios de negocio y terceros que tengan a cargo Estaciones de Trabajo o equipos tecnológicos de propiedad de Canal Capital deben bloquear estos en el momento de abandonar el puesto de trabajo con el fin de

proteger el acceso indebido a la información en estos almacenada.

- Los Funcionarios, proveedores, socios de negocio y terceros que tengan a cargo Estaciones de Trabajo o equipos tecnológicos de propiedad de Canal Capital no deben usar estos para actividades diferentes a las estrictamente laborales.
- Reportar a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones cualquier anomalía que se presente en la alteración del software o hardware instalados en los equipos propios de Canal Capital, así como la pérdida o robo de estos a través de la mesa de servicios, como canal oficial de recepción de incidentes y requisitos de OFITIC.
- Asegurar que las estaciones de trabajo, equipos electrónicos e Infraestructura Tecnológica no crítica sean apagadas de forma correcta y total al finalizar la jornada laboral.

Normas dirigidas a Servicios Administrativos

- Velar por que las estaciones de trabajo e Infraestructura Tecnológica de propiedad de Canal Capital posean pólizas de seguro vigentes.

8.13 Política de recursos compartidos en la red y acceso a redes de datos

- Canal Capital es responsable de las redes de datos y los recursos compartidos en la red, además de propender porque estas sean protegidas de accesos no autorizados con los controles de acceso necesarios.
- Está prohibido compartir información sensible o confidencial sin los controles de seguridad adecuados.
- Los recursos compartidos en la red deben ser utilizados exclusivamente para fines laborales autorizados, quedando prohibido su uso para actividades personales o que comprometan la seguridad de la red.

8.13.1 Normas de acceso a los recursos compartidos en la red y acceso a redes de datos

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Asegurar que las redes inalámbricas de Canal Capital (SSID) tengan métodos de autenticación y contraseñas seguras que no permitan el acceso a personal no autorizado.
- Asegurar que las redes LAN de Canal Capital tengan métodos de autenticación y contraseñas seguras que no permitan el acceso a personal no autorizado.

- Almacenar la información de la entidad en las unidades de red compartidas asignadas para esta función.
- La Oficina de Gestión de Tecnologías de la Información y Comunicaciones no audita el contenido de la información almacenada por los usuarios, ya que esta es responsabilidad exclusiva de cada funcionario, colaborador y contratista (propietarios y custodios de los activos de información).
- Velar por que las estaciones de trabajo propias de Canal Capital que se conectan a las unidades de red compartidas, cumplan con los requerimientos y controles de autenticación y que únicamente puedan acceder a los recursos asignados y autorizados.
- Está prohibida la instalación o el uso de software no autorizado o de dispositivos que puedan comprometer la seguridad de los recursos compartidos o de la red.

Normas dirigidas a todos los Colaboradores, Contratistas y Terceros

- Deben contar con un usuario y una contraseña autorizadas y provistas por la Oficina de Gestión de Tecnologías de la Información y Comunicaciones de Canal Capital.
- No se permite almacenar información personal en las unidades de red compartida (música, vídeos, fotos personales, entre otros).

8.14 Política de seguridad del centro de datos y cableado

Canal Capital debe asegurar la protección de la información en las redes de datos y la infraestructura tecnológica.

8.14.1 Normas para la mantener la seguridad del centro de datos y cableado

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- El ingreso a los centros de datos y cableado se limita únicamente a los usuarios autorizados, adicional se debe registrar el acceso en una bitácora de acceso.
- No ingerir bebidas o alimentos dentro de los centros de datos y cableado.
- Supervisar las actividades de mantenimiento preventivo y correctivo que se lleven a cabo dentro de los centros de datos y cableado.
- El Data Center debe contar con control de acceso biométrico, tarjeta de proximidad, además debe contar con una cámara de seguridad que egrabe todas las actividades que se desarrollen en este.
- Los centros de cableado deben estar identificados y con acceso restringido solo para personal autorizado.

Normas dirigidas a Servicios Administrativos

- Señalizar de forma adecuada los elementos de seguridad física que se encuentren al interior de los centros de datos y cableado.
- Proveer y velar por el correcto funcionamiento de extintores de incendio probados y verificados mínimo 3 veces en el año.
- Mantener en buen funcionamiento los controles de acceso instalados en el ingreso y salida de los centros de datos y cableado de Canal Capital
- Velar por el correcto funcionamiento de las cámaras de seguridad instaladas en los centros de datos y cableado.

8.15 Política de asignación de usuarios y protección de claves de acceso

Canal Capital debe garantizar el control de acceso a las estaciones de trabajo, servidores, recursos de red, redes de datos, correo electrónico, aplicaciones y servicios en general de la entidad.

8.15.1 Normas para la asignación de usuarios y protección de claves de acceso

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Asignar un nombre único de usuario y contraseña a cada colaborador y contratista de la entidad.
- La contraseña inicial emitida a un nuevo usuario debe ser válida únicamente para el primer inicio de sesión.
- Notificar credenciales de acceso mediante el uso de correo en modo confidencial.
- Las cuentas de usuarios de los colaboradores y contratistas de la entidad se deben mantener vigente exclusivamente por el periodo de contratación.
- Limitar el número de intentos de inicio de sesión a tres (3); después del tercer intento fallido la cuenta involucrada debe ser bloqueada.
- Velar y controlar que ningún funcionario tenga más de una cuenta de usuario para acceso a los recursos de red y aplicaciones.
- Las contraseñas deben ser robustas y cumplir, como mínimo, con los siguientes requisitos:
  - Longitud mínima: Contar con al menos 12 caracteres (o preferiblemente más para mayor seguridad).
  - Combinación de caracteres: Incluir una mezcla de letras (mayúsculas y minúsculas), números y al menos un carácter especial (por ejemplo: @, #, $, %, &, *).

- No contener datos personales: Evitar el uso de información fácilmente asociable al usuario, como nombres, fechas de nacimiento o números de identificación.
- Rotación periódica: Cambiar las contraseñas regularmente (por ejemplo, cada 90 días) o inmediatamente después de un incidente de seguridad.
- Evitar patrones predecibles: No utilizar secuencias comunes (1234, abcdef) o palabras simples.

- Concienciar sobre las buenas prácticas de seguridad en la selección y uso de claves, las cuales son el medio de validación de la identidad y credenciales de los funcionarios.

Normas dirigidas a todos los Colaboradores, Contratista y Terceros

- Los usuarios y contraseñas deben ser únicas e intransferibles.
- Los usuarios y contraseñas por ningún motivo deben ser anotadas en papel, medios digitales a menos que puedan ser almacenadas de forma segura.
- Crear contraseñas seguras, para ello debe cumplir las requisitos mencionados en el ítem anterior: “Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones”
- Se debe informar a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones de la entidad si se detecta alguna anomalía en las cuentas de usuario para que se proceda a bloquearlas mientras se reasignan nuevas credenciales de acceso, validando que se haya mitigado el riesgo generado.

8.16 Política de uso de activos de información y tecnológicos

Canal Capital se encarga de velar y mantener la protección adecuada de cada uno de los activos de información y tecnológicos, esto mediante la asignación de estos a los colaboradores y contratistas de la entidad y propender por el correcto uso de acuerdo a sus funciones u obligaciones contractuales y roles asignados.

8.16.1 Normas generales para el uso de activos de información y tecnológicos

Normas dirigidas a la Dirección de Canal Capital

- Informar y concientizar a los colaboradores, contratistas y proveedores, socios de negocio y terceros pertenecen a Canal Capital y deben ser usados exclusivamente para fines laborales y no personales.

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Asegurar la apropiada operación y administración de los activos de información y tecnológicos.
- Todos los procesos de Canal Capital deben contar con un inventario y clasificación de sus activos de información y se debe evidenciar a través de los instrumentos dispuestos desde la Oficina de Gestión de Tecnologías de la Información y Comunicaciones.
- Monitorear semestralmente la validez de los usuarios y perfiles de acceso a la información.
- Asegurar el correcto funcionamiento a través de una configuración adecuada de estos certificando la seguridad de la información y el adecuado uso de estos.

Normas dirigidas a todos los Colaboradores, Contratistas y Terceros

- Usar los activos de información y tecnológicos asignados de manera ética y dando cumplimiento de las políticas complementarias y normas de seguridad de la información descritas en el presente manual.
- Por ningún motivo se debe instalar y/o usar software que no esté debidamente licenciado, autorizado o no sea de propiedad de la entidad.
- En el momento de desvinculación de la entidad, realizar la entrega de los activos de información y tecnológicos suministrados en el momento de su vinculación.

8.16.2 Clasificación de la Información

- Canal Capital define los niveles más adecuados para clasificar su información, de acuerdo con su sensibilidad. La clasificación de la información se realiza en el formato "ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA" de acuerdo a la información de cada proceso de la entidad.
- Las Tablas de Retención Documental (TRD) deben indicar el tipo de clasificación de las series, subseries y documentos en ella contenidas.
- Cada propietario del activo de Información debe velar por el cumplimiento de su clasificación de acuerdo con lo establecido en lineamientos para la administración de los archivos y activos de Información.

8.17 Política de adquisición de software y hardware

Canal Capital debe velar porque se cumplan los procesos de contratación expuestos en el Manual de Contratación de la Entidad.

8.17.1 Normas generales para la adquisición de software y hardware

Normas dirigidas a las oficinas que adquieran Software y Hardware

- Asegurar y verificar que el software y hardware que se adquiere para la entidad cumpla con todos los requerimientos solicitados en el momento de la contratación.
- Por ningún motivo las claves de licencias, medios de instalación y/o códigos fuente pueden ser copiados o suministrados a terceros.
- Incluir en todos los procesos de adquisición de hardware y software que estos soporten el protocolo de comunicaciones IPv6.
- Verificar que el software y hardware adquirido sea original, adicional se deben solicitar los manuales de instalación y soporte correspondiente.
- Todos los equipos tecnológicos adquiridos (computadores, impresoras, monitores, equipos de streaming, networking, equipos de televisión, etc.) deberán cumplir con estándares reconocidos de eficiencia energética, tales como la certificación ENERGY STAR u otras equivalentes, que incorporen materiales biodegradables, reciclables o reutilizables, contribuyendo a la reducción del impacto ambiental.
- Los proveedores deberán garantizar el uso de empaques sostenibles, minimizando el uso de plásticos de un solo uso y favoreciendo materiales reciclables o de origen responsable.

Normas dirigidas a Gestión Contractual

- Velar porque todos los requerimientos legales y condiciones contractuales establecidos por la entidad para la adquisición de software y hardware sean cumplidos por parte de los proveedores.

8.18 Política de desarrollo de software interno o externo (Escritorio y Web)

La Oficina de Gestión de Tecnologías de la Información y Comunicaciones es la responsable de liderar, planificar, controlar, desarrollar y ejecutar las actividades relacionadas con el desarrollo de software, así como efectuar las actualizaciones e instalaciones de software. Además, este grupo lidera y ejecuta la planificación de pruebas funcionales y de seguridad de los sistemas nuevos o modificados, situación que se presenta antes de ejecutar la instalación en los servidores de producción.

8.18.1 Normas generales para el desarrollo de software interno o externo

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Establecer controles para garantizar que la seguridad de la información sea un requisito para el desarrollo de nuevos sistemas o la mejora de los existentes.
- En caso de que el desarrollo sea llevado a cabo por el personal de la Entidad, deben incluirse los requisitos de seguridad de la información en los nuevos sistemas de información o la mejora de los actuales.
- Estos requisitos deben ser identificados mediante herramientas como: obtención de requisitos de cumplimiento a partir de políticas y reglamentación, revisiones de incidentes e identificación de vulnerabilidades.
- Esta identificación debe ser documentada y revisada por las partes interesadas. En caso de que estos desarrollos sean producidos por terceros, debe seguirse un proceso formal de adquisición, que incluya los requisitos de seguridad de la información de la Entidad.
- De igual manera, el nivel de protección de la información que se encuentra en un ambiente de protección no puede ser disminuido utilizándolo en procesos de desarrollo y pruebas.
- Debe evitarse que los datos de producción sean utilizados para el desarrollo, y en caso de ser necesarios, estos datos deben permanecer en estos ambientes tan poco como sea posible y estar bajo monitoreo permanente.
- La Oficina de Gestión de Tecnologías de la Información y Comunicaciones debe implementar los controles necesarios para asegurar que las migraciones entre ambientes de desarrollo, pruebas y producción sean aprobadas de acuerdo al procedimiento de control de cambios.
- También, debe certificar que cualquier tipo de desarrollo que vaya a ser pasado a producción cumple con los requerimientos de seguridad establecidos antes de realizar este proceso.
- Si las aplicaciones Web son alojadas en un servidor de la Entidad, el personal de OFITIC debe dar soporte sobre el mismo garantizando la conectividad; además de instalar certificados SSL y utilizar procedimientos de aseguramiento de la información alojada allí.
- Todo desarrollo, que haya sido creado interna o externamente, debe contar con un proceso de soporte. En caso de ser creado de manera interna, el (los) desarrollador(es) deben proporcionar un nivel adecuado de soporte y de documentación, en caso de no ser posible proveer el primero.
- De manera externa, debe exigirse durante la contratación que se cuente con un proceso de soporte para los errores que puedan presentar las aplicaciones. Respecto a las aplicaciones, los desarrolladores, internos o externos, deben asegurar que:
- Antes de la puesta en producción, todas las características que no sean estrictamente esenciales deben ser removidas de la aplicación.
- Las conexiones a la base de datos son cerradas desde las aplicaciones tan pronto no sean requeridas.

- No se debe poder ejecutar comandos en el sistema operativo del servidor que las aloja.
- Debe prevenirse revelar la estructura de directorios de los sistemas de información de la Institución.
- Los valores para conexión a base de datos no deben estar insertados en el código sino en archivos independientes que permanecen por fuera del control de cambios, y que, de ser posible, se encuentren cifrados.

Normas dirigidas a todos los Colaboradores, Contratistas y Terceros

- Los colaboradores de la entidad son responsables de la información almacenada en la base de datos por medio del software desarrollado y deben velar por los lineamientos descritos en la presente política para el desarrollo, instalación y actualización de software.
- Se deberá estandarizar el ciclo de vida, criterios de seguridad y de calidad en el desarrollo de software, por medio de marcos para la gestión de proyectos ágiles como SCRUM, KANBAN, Crystal, entre otros.
- Toda modificación de software crítico realizado por el personal y/o desarrollador, bien sea por actualizaciones o modificaciones, debe ser analizada en ambientes independientes de prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación de manera que no afecte el ambiente de producción.
- Se debe realizar una planeación en detalle de todas las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y post-instalación, y criterios de aceptación del cambio.

Normas dirigidas para la gestión de Vulnerabilidades

- Se establecerá una gestión centralizada de vulnerabilidades la cual se debe orientar a analizar los problemas de seguridad que surgen en el desarrollo y de los productos de software.
- Se deberá establecer un plan de actualización para el software que es desarrollado o se utiliza en la Entidad, asegurando que las últimas versiones y parches sean instalados lo antes posible, con el fin de evitar que alguna vulnerabilidad sea explotada, esta gestión iniciar se debe realizar en un ambiente controlado de pruebas de manera que no afecte el software en producción.
- Se deben establecer monitoreos en los sistemas de información que contemple, entre otras, las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios entre otros.

- Integración Continua y Entrega Continua (CI/CD):
  - Implementar pipelines de CI/CD para asegurar que cada cambio en el código pase por una serie de pruebas automatizadas antes de ser desplegado en producción. Esto incluye pruebas unitarias, de integración, de regresión y de seguridad.
- Políticas de Respuesta a Incidentes:
  - Definir procedimientos claros para la gestión de incidentes de seguridad relacionados con el software, incluyendo la identificación, contención, erradicación y recuperación.
  - Establecer un equipo de respuesta a incidentes que esté preparado para manejar brechas de seguridad y vulnerabilidades explotadas.
- Protección contra Amenazas Avanzadas.
  - Implementar técnicas avanzadas de protección como la detección y respuesta de amenazas (Threat Detection and Response, TDR), que incluyen el monitoreo de comportamiento anómalo en las aplicaciones y servidores.
  - Asegurar que todas las aplicaciones críticas estén protegidas contra amenazas avanzadas persistentes (APT) utilizando firewalls de aplicaciones web (WAF) y sistemas de prevención de intrusiones (IPS).
- Control de Acceso Basado en Roles (RBAC):
  - Refinar y revisar periódicamente las políticas de control de acceso basado en roles para asegurar que los permisos y privilegios estén alineados con las responsabilidades actuales de los usuarios.
  - Implementar la revisión periódica de permisos y accesos para asegurar la minimización de privilegios y reducir el riesgo de accesos no autorizados.

Normas dirigidas para la documentación del software.

- El diccionario de datos, o repositorio de metadatos, deberá mantener una descripción actualizada de las definiciones de datos.
- Todo sistema desarrollado por el personal/desarrollador en la entidad, debe tener implícito el protocolo de las condiciones de autenticación a través de controles de acceso fuerte que incluyan contraseñas robustas para el acceso a las aplicaciones, el cual deberá ser revisado y aprobado por el personal designado por el Grupo de Recursos Informáticos.
- Como buena práctica toda documentación de desarrollo debe tener:
  - Crearse durante el desarrollo del software y no postergarse hasta el final.
  - Actualizarse cuando en razón al desarrollo de software se presenten cambios.
  - Almacenarse en un sitio destinado para guardar la documentación autorizado por el grupo de recursos informáticos.
  -

Normas dirigidas para la codificación y pruebas.

- Al momento de realizar las pruebas es importante incluir: instalación, stress, carga, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores.
- Se deben tener las siguientes consideraciones con relación a los datos de entrada y salida de los sistemas de información:
  - Validar la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como tipos de datos, rangos válidos y longitud, entre otros.
  - Validar las entradas de datos con una lista “blanca” que contenga un directorio de caracteres aceptados.
  - Validar el intento de ingreso de bytes nulos, caracteres de nueva línea o caracteres de alteración de rutas.
  - Limpiar las salidas de datos no confiables hacia consultas SQL, XML y LDAP o hacia comandos del sistema operativo.
  - Validar que estén deshabilitados los métodos HTTP peligrosos como put, delete, trace y tenga restricción la administración remota
  - Validar que se protege la integridad del código, mediante: (i) la validación exhaustiva de: inputs, variables post y get (no enviar parámetros sensibles a través del método get), Cookies (habilitar atributos de seguridad como Secure y HttpOnly), y, cabeceras HTTP; (ii) verificación estándar de las Políticas de Origen de las cabeceras.

- Validar que los sistemas de información desarrollados restrinjan el uso de login contra ataques de fuerza bruta, implementando, entre otros: mecanismos de captcha accesibles o auto detectable, y/o limitar la tasa de intentos de login.
- Se deberán establecer los siguientes controles para la autenticación en los sistemas de información:
  - Realizar los controles de autenticación en un sistema confiable.
  - Validar que el almacenamiento de credenciales, guarden únicamente el hash de las contraseñas.
  - Validar los datos de autenticación, luego de haber completado todos los datos de entrada.
  - Controlar el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web.
- Se deberá realizar una gestión de las sesiones, que tenga en cuenta los siguientes aspectos:
  - Se debe garantizar la existencia de opciones de desconexión o cierre de sesión de los aplicativos (logout) que permita terminar completamente con la conexión

asociada.
    - No exponer los identificadores de sesión en URL, mensajes de error ni logs, y no transmitirlos como parámetros.
    - Asegurar que la sesión expire después de cierto tiempo.
- Validar que los mensajes de error generados por los sistemas de información, no revelen información sensible como: tecnología usada, excepciones o parámetros que dispararon el error específico, entre otros. El mensaje de error debe ser genérico.
- Se deberán desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y garantizar que dichos archivos sólo tengan privilegios de lectura.
- Garantizar conexiones seguras a través del uso de certificados, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales, para evitar la manipulación de parámetros en las peticiones.
- Se deben implementar acciones de seguridad con el fin de que los controles en los servidores (hardware o software) implemente acciones para la protección de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros.
- No se deberá permitir que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

Normas dirigidas para la Implementación

- Se deberá velar por la implementación de los controles de seguridad al mismo tiempo que la implementación de los componentes, funciones o módulos a los cuales controla.
- Las aplicaciones deberán contar con manejo de diferentes roles con permisos de acceso y operaciones asociados a estos.

8.19 Política gestión de incidentes de seguridad

La Oficina de Gestión de Tecnologías de la Información y Comunicaciones en conjunto con el agente de seguridad informática debe definir un documento oficial para la gestión de incidentes de seguridad de la información.

- La Oficina de Gestión de Tecnologías de la Información y Comunicaciones debe definir los canales para que los colaboradores, contratistas y terceros de Canal Capital puedan reportar los incidentes de Seguridad de la Información.
- La Oficina de Gestión de Tecnologías de la Información y Comunicaciones es la

encargada de la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos.

- La Oficina de Gestión de Tecnologías de la Información y Comunicaciones es la encargada para la recolección de evidencias de los incidentes de seguridad de la información.

8.20 Política de protección y análisis de software malicioso

Canal Capital proporcionará los recursos necesarios que mantengan y protejan la información e infraestructura tecnológica que mitigue o ponga en riesgo la confidencialidad, disponibilidad e integridad de esta.

8.20.1 Normas generales para la Protección y Análisis de Software Malicioso

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Asegurar la adquisición de herramientas tales como antivirus y antispyware que permitan proteger y asegurar la seguridad de las estaciones de trabajo y servidores donde está almacenada información de la entidad.
- Verificar que las herramientas de protección cuentan con una licencia debida de uso que permita la actualización constante de parches de seguridad para así mitigar en parte el riesgo de los activos de información y tecnológicos.
- Velar por que la información almacenada en las estaciones de trabajo y servidores de la entidad, sea escaneada de forma constante por el software de antivirus permitiendo así el análisis y mitigación de las posibles amenazas a las que esta se ve expuesta.
- Debe contar con equipo de seguridad perimetral Firewall, que cree una barrera que permita o bloquee intentos para acceder a la información de los equipos o servidores, bloquear aplicaciones y usuarios no autorizados, visualizar y advertir intentos de conexión que puedan generar riesgo y monitoreo del tráfico de datos entrante y saliente.

Normas dirigidas a todos los Colaboradores, Contratistas y Terceros

- Por ningún motivo se debe modificar, eliminar y/o alterar el software de antivirus instalado en las estaciones de trabajo de la entidad.
- Realizar un análisis de riesgos y vulnerabilidades con el software de antivirus a dispositivos de almacenamiento externos como USB, Discos, CD.
- Realizar un análisis de riesgos y vulnerabilidades con el software de antivirus a los

archivos descargados de Internet. (Imágenes, documentos, videos, etc.).

- Informar a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones de la entidad sobre cualquier hecho o acto que ponga en riesgo la seguridad de la información.

8.21 Política de backup y restauración de información

Proteger y garantizar la seguridad de la información para que se mantengan asegurados, respaldados y sean de fácil recuperación en el menor tiempo posible al momento de ser solicitados.

8.21.1 Normas generales para el backup y restauración de la información

Normas dirigidas a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones

- Establecer los lineamientos que defina la operación para la generación, seguimiento y almacenamiento de las copias de respaldo, en concordancia con la operación, las necesidades y los requisitos normativos de la entidad.
- Realizar copias de seguridad a las bases de datos, documentos, servidores, correo y demás servicios conforme al procedimiento de copias de seguridad (AGRI-SI-PD-014 COPIAS DE SEGURIDAD..pdf)
- Revisar los reportes diarios generados por la herramienta de gestión de copias de seguridad para validar el estado de las tareas programadas y ejecutadas. Este proceso permite identificar posibles fallos, verificar la integridad de las copias realizadas y garantizar la disponibilidad de los datos respaldados, asegurando así un seguimiento efectivo y una pronta respuesta ante cualquier incidencia.
- Realizar pruebas de restauración de información cuando se requiera.

Normas dirigidas a todos los Colaboradores, Contratistas y Terceros

- Los colaboradores de la entidad son responsables de la información almacenada en las estaciones de trabajo y deben velar por que esta mantenga la integridad, confidencialidad y disponibilidad.

8.22 Realizar periódicamente mantenimientos preventivos y correctivos de la Infraestructura Tecnológica.

- Establecer procesos de configuración seguros para las Estaciones de Trabajo que usen los funcionarios de la entidad.
- Establecer las condiciones que deben cumplir los equipos de cómputo personal,

Smartphone, Tablet de terceros que requieran conectarse a la red LAN o WLAN de la entidad

- Aislar los equipos sensibles y críticos (servidores, firewall, switch, etc.) del acceso a personas que no estén autorizadas para su uso.
- Generar y aplicar lineamientos para la disposición segura de las estaciones de trabajo u otro elemento tecnológico ya sea cuando este sea dado de baja o cambie de usuario.

Normas dirigidas a todos los Funcionarios, Proveedores, Socios de Negocio y Terceros

- La Oficina de Gestión de Tecnologías de la Información y Comunicaciones de Canal Capital es la única autorizada para realizar traslados, movimientos y asignaciones de estaciones de trabajo.
- Las fallas de software, hardware y configuración de las Estaciones de Trabajo e Infraestructura Tecnológica se deben informar a través de la mesa de ayuda de Canal Capital donde se atenderá la solicitud y se realizará la reparación que dé a lugar.
- Los Funcionarios, proveedores, socios de negocio y terceros que tengan a cargo Estaciones de Trabajo o equipos tecnológicos de propiedad de Canal Capital deben bloquear estos en el momento de abandonar el puesto de trabajo con el fin de proteger el acceso indebido a la información en estos almacenada.
- Los Funcionarios, proveedores, socios de negocio y terceros que tengan a cargo Estaciones de Trabajo o equipos tecnológicos de propiedad de Canal Capital no deben usar estos para actividades diferentes a las estrictamente laborales.
- Reportar a la Oficina de Gestión de Tecnologías de la Información y Comunicaciones cualquier anomalía que se presente en la alteración del software o hardware instalados en los equipos propios de Canal Capital, así como la pérdida o robo de estos.
- Asegurar que las estaciones de trabajo, equipos electrónicos e Infraestructura Tecnológica no crítica sean apagados de forma correcta y total al finalizar la jornada laboral.

Normas dirigidas a Servicios Administrativos

- Velar porque todas las estaciones de trabajo e Infraestructura Tecnológica de propiedad, planta y equipo de Canal Capital poseen pólizas de seguro vigentes.