Manual de Políticas Complementarias de Seguridad de la Información

Diciembre de 2021

TABLA DE CONTENIDO

Introducción

Capital, ha querido 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 Capital convirtiéndose así en la base para la implementación de controles, procedimientos y estándares definidos.[1]

Teniendo en cuenta lo anterior, el presente Manual tiene como finalidad establecer los principios orientadores en seguridad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad y continuidad de la información de Capital, así como dar lineamientos para la aplicación de mecanismos que eviten 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.

1 Objetivo

Dar a conocer los lineamientos de seguridad para asegurar los activos de información y de la infraestructura tecnológica que soporta las operaciones de Capital, que sean accedidos solo por aquellas personas que tienen la necesidad legitima para el cumplimiento de sus funciones y/o obligaciones (confidencialidad), que este 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 ocurrencia de cualquier ataque a estos.

2 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 o presten sus servicios o tengan algún tipo de relación con la Entidad a través de la recolección, procesamiento, almacenamiento,

[1] https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

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.

3 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 que 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 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 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: Posibilidad de que ocurra un contra tiempo.

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: Limites 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.

4 Marco Legal

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 Capital se encuentra centralizado en el Normograma Institucional.

5 Documentos de Referencia

- Norma ISO7IEC 27001:2013
- Norma ISO/IEC 27002:2013
- Manual de Sistema de Gestión de Seguridad de la Información.
- Declaración de Aplicabilidad SoA Capital.
- Instrumento de Evaluación MSPI 2020.
- Política de Seguridad y Privacidad de la Información Capital

6. Política de Seguridad y Privacidad de la Información y Seguridad Digital

Asegurar y administrar la información y los recursos tecnológicos para que sean accedidos solo por aquellas personas que tienen la necesidad legitima para el cumplimiento de sus funciones (confidencialidad), que este 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 ocurrencia de cualquier ataque a esta.

Para asegurar la información el área de sistemas de Capital establece la articulación con la política de seguridad de la información y los objetivos de seguridad de la información así:

- Consolidar la seguridad de la información como una línea estratégica en 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 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.

7. Políticas Específicas de Seguridad y Privacidad de la Información

7.1 Política Organizacional de Seguridad de la Información

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

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

Normas Dirigidas a la Gerencia de 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 auditorias.
- Validar y monitorear la implantación de las Políticas Complementarias de la Seguridad de la Información.

Normas Dirigidas al Área de Sistemas

- 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 dar aviso 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 a Todos los Colaboradores, Contratistas y Terceros

- Cumplir con el presente Manual de Políticas Complementarias de Seguridad de la Información.

5.1.2 Política para el Uso de Dispositivos Móviles

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

5.1.2.1 Normas Generales para el Uso de Dispositivos Móviles

Normas Dirigidas al Área de Sistemas

- 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 la 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 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 el área de sistemas 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.

5.1.2.2 Normas Generales para el Uso de Dispositivos Móviles no Corporativos

Normas Dirigidas al Área de Sistemas

- Dar a conocer las Políticas de Seguridad de la Información de 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 Capital, en función de sus actividades laborales.
- Eliminar los datos propios de Capital del usuario cuando este no tenga ninguna vinculación con la entidad.

Normas Dirigidas a Todos los Colaboradores, Contratistas y Terceros

- Conocer y aceptar la normatividad dada por 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 Capital.
- Hacer únicamente uso de los recursos de red asignados por Capital.
- Abstenerse de instalar aplicaciones que pongan en riesgo la seguridad de la información al interior de Capital.
- Tener instalado, debidamente licenciado y actualizado un antivirus y que este realiza un análisis automático de todos los recursos del equipo de cómputo.
- Evitar en lo posible almacenar información sensible de propiedad de Capital.
- Al finalizar la vinculación con Capital, se obliga al colaborador 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.

5.2 Política de Seguridad de los Recursos Humanos

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.

5.2.1 Antes de asumir el Empleo

- El área de Recursos Humanos, debe contar con procedimientos para la vinculación de personal, de acuerdo a 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 Capital.

5.2.2 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.
- El área de sistemas 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.
- El área de sistemas en conjunto con el área de Comunicaciones debe diseñar y ejecutar un plan de Uso y apropiación de comunicaciones en apropiación del Sistema de Gestión de la Seguridad de la Información – SGSI.
- 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 el área de sistemas para tal fin.

5.2.3 Terminación y Cambio de Empleo

- Es responsabilidad del Colaborador y Contratista realizar la entrega de la información propia de Capital, que se encuentra en gestión por parte de los mismos, cuando existe una novedad de retiro, investigación, inhabilidades, o cambio de funciones.
- El supervisor del contrato o a quien este delegue debe recoger y custodiar la información de Capital bajo la responsabilidad del contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
- El área de Sistemas debe parametrizar en el directorio activo, la inactivación automática de los contratistas, teniendo en cuenta la fecha de terminación del contrato; la inactivación de los usuarios de los sistemas de información que no se autentican con el directorio activo, se debe hacer de forma manual.
- Se creará una copia de respaldo del buzón de correo electrónico, por solicitud del jefe inmediato o supervisor del contrato.
- Se debe solicitar la devolución del carné, tarjeta de acceso o cualquier distintivo de autenticación, que lo acredita como colaborador, contratista o tercero de Capital.

5.3 Política de Teletrabajo y Conexiones Remotas

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.

5.3.1 Normas Generales para el Teletrabajo y Conexiones Remotas

Normas Dirigidas al Área de Sistemas

- 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.
- El área de sistemas establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones 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 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 el área de sistemas de la entidad.
- Por ningún motivo se pueden realizar conexiones remotas o sesiones de teletrabajo sin la previa autorización del área de sistemas de la entidad y el jefe o coordinador de contrato.

5.4 Política de Control de Acceso

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

5.4.1 Normas para el Control de Acceso

Normas Dirigidas al Área de Sistemas

- Los sistemas de información, equipos de procesamiento y comunicaciones administrados por la oficina de sistemas, 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 sistemas.
- Los equipos de contratistas y terceros que requieran el acceso a la red LAN y WLAN deberán ser autorizados por la respectiva área donde laboraran y por la oficina de sistemas.
- 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 asignación de escarapelas de identificación a todos los Colaboradores, Contratistas y Terceros para el desplazamiento por las instalaciones de la entidad.

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 y correo electrónico asignados para el cumplimiento de las actividades laborales.
- Cumplir con las políticas y normas concebidas en el presente manual.
- Los carnets de identificación propios de la entidad son de uso personal e intransferible.

5.5 Política de Uso de Controles Criptográficos

Capital velará porque la información contenida en sus bases de datos, aplicaciones y copias de seguridad mantengan 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.

5.5.1 Normas para el Uso de Controles Criptográficos

Normas Dirigidas al Área de Sistemas

- El área de sistemas 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.

Normas Dirigidas a los Administradores de Token

- Definir inventario de token de seguridad, que uso específico tiene y que 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 sitio seguros manteniéndolos fuera del alcance de personas no autorizadas.

Normas Dirigidas a los Administradores de Certificados Digitales

- 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.

5.6 Política de Escritorio y Pantalla Limpia

Reducir el acceso no autorizado, daño, perdida, filtración 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.

5.6.1 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 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.
- Por ningún motivo se deben poner, pegar (sticker, afiches) y/o alterar las partes físicas de las estaciones de trabajo.

5.7 Política para la Transferencia de Información

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

5.7.1 Normas Generales para el Uso de Correo Electrónico

Normas Dirigidas al Área de Sistemas

- 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.
- Controlar la asignación de cuentas de correo y contraseñas de acceso, cambios de contraseñas, desbloqueo de cuentas e informes de uso.
- Generar campañas para concientizar 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 se la del Colabroador.
- 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 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.
- Realizar cambio de contraseña de acceso al buzón de correo electrónico como mínimo cada 30 días.
- 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.

5.8 Política de Relaciones con los Proveedores

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.

5.8.1 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.

5.9 Política Uso de Estaciones de Trabajo

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.

5.9.1 Normas para el Uso de Estaciones de Trabajo

Normas Dirigidas al Área de Sistemas

- 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

- El área de sistemas de 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 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 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 Capital no deben usar estos para actividades diferentes a las estrictamente laborales.
- Reportar al área de sistemas cualquier anomalía que se presente en la alteración del software o hardware instalados en los equipos propios de Capital, así como la pérdida o robo e estos.
- Asegurar que las estaciones de trabajo, equipos electrónicos e Infraestructura Tecnológica no crítica, sea apagada 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 Capital posean pólizas de seguro vigentes.

5.10 Política de Recursos Compartidos en la Red y Acceso a Redes de Datos

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.

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

Normas Dirigidas al Área de Sistemas

- Asegurar que las redes inalámbricas de Capital (SSID) tengan métodos de autenticación y contraseñas seguras que no permitan el acceso a personal no autorizado.
- Asegurar que las redes LAN de 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.
- Auditar la información almacenada en las unidades de red compartidas de la entidad con el fin de controlar y no permitir el almacenamiento de información que no sea estrictamente laboral.
- Velar por que las estaciones de trabajo propias de 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.

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 Capital y velar por el cumplimiento de las políticas complementarias de seguridad de la información que aplique a estas.

Normas Dirigidas a Todos los Colaboradores, Contratistas y Terceros

- Deben contar con un usuario y una contraseña autorizadas y provistas por el área de sistemas de Capital.
- No se permite almacenar información personal en las unidades de red compartida (música, vídeos, fotos personales).

5.11 Política de Seguridad del Centro de Datos y Cableado

Capital debe asegurar la protección de la información en las redes de datos y la Infraestructura Tecnológica.

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

Normas Dirigidas al Área de Sistemas

- 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 grave 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 Capital
- Velar por el correcto funcionamiento de las cámaras de seguridad instaladas en los centros de datos y cableado.

5.12 Política de Asignación de Usuarios y Protección de Claves de Acceso

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.

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

Normas Dirigidas al Área de Sistemas

- 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.
- Mantener mecanismos y controles que obliguen al usuario a cambiar sus contraseñas de accesos a red como mínimo cada 45 días.
- 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 alfanuméricas y contener caracteres especiales.
- Concientizar 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 siguientes reglas:
    - Usar mínimo 8 caracteres alfanuméricos donde se incluya algún carácter especial tales como puntos, asteriscos, signos de admiración, etc.
    - No se deben usar nombres personales, fechas importantes, números de identificación, números telefónicos, etc.
- Se debe informar al área de sistemas de la entidad si se detecta alguna anomalía en las cuentas de usuario para que se proceda bloquearlas mientras se reasignan nuevas credenciales de acceso, validando que se haya mitigado el riesgo generado.

5.13 Política de Uso de Activos de Información y Tecnológicos

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 y roles asignados.

5.13.1 Normas Generales para el Uso de Activos de Información y Tecnológicos

Normas Dirigidas a la Dirección de Capital

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

Normas Dirigidas al Área de Sistemas

- Asegurar la apropiada operación y administración de los activos de información y tecnológicos.
- Todos los procesos de Capital deben contar con un inventario y clasificación de sus activos de información y se debe evidenciar a través de los instrumentos dispuestos desde el área de sistemas.
- Monitorear periódicamente 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.

5.13.2 Clasificación de la Información

- 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 "INDICE 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.

5.14 Política de Adquisición de Software y Hardware

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

5.14.1 Normas Generales para la Adquisición de Software y Hardware

Normas Dirigidas al Área de Sistemas

- 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.

Normas Dirigidas al Área Jurídica

- Velar por que todos los requerimientos legales y condiciones establecidos al momento de la contratación por la entidad sean cumplidos por parte de los proveedores.

5.15 Política Gestión de Incidentes de Seguridad

El área de sistemas en conjunto con el agente de seguridad informática debe definir un documento oficial para la gestión de incidentes de seguridad de la información.

- El área de sistemas debe definir los canales para que los colaboradores, contratistas y terceros de Capital puedan reportar los incidentes de Seguridad de la Información.

- El área de sistemas es la encargada de la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos.
- El área de Sistemas es la encargada para la recolección de evidencias de los incidentes de seguridad de la información.

5.16 Política de Protección y Análisis de Software Malicioso

Capital proporcionara 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.

5.16.1 Normas Generales para la Protección y Análisis de Software Malicioso

Normas dirigidas al Área de Sistemas

- 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 esta almacenada información de la entidad.
- Verificar que las herramientas de protección cuentan con una licencia debida de uso que permita la actualización constate de parches de seguridad para así minimizar 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 de todo el 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 al área de sistemas de la entidad sobre cualquier hecho o acto que ponga en riesgo la seguridad de la información.

5.17 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.

5.17.1 Normas Generales para el BackUp y Restauración de la Información

Normas Dirigidas al Área de Tecnología

- Establecer los lineamientos para la generación y almacenamiento de las copias de respaldo de acuerdo a los requerimientos de la entidad.
- Realizar copias de seguridad a las bases de datos, documentos y demás servicios de forma diaria, rutinas que deben ser realizadas de forma automática.
- Generar reportes diarios de las copias de seguridad realizadas para así conocer el estado de estas.
- Realizar pruebas de restauración de información.

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.

6 Compromiso de la Dirección

La Gerencia de Capital aprueba este Manual de Políticas Complementarias de Seguridad de la Información como muestra de su compromiso al diseño e implementación del SGSI para que así se garantice la seguridad de la información de la Entidad.

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en el Manual de Políticas Complementarias de Seguridad de la Información.
- La promoción activa de una cultura de seguridad.

- Divulgar el Manual de Políticas Complementarias de Seguridad de la Información y el Manual de Políticas de Seguridad de la Información.
- Asegurar los recursos económicos necesarios para implementar y mantener el SGSI.
- Velar por el cumplimiento de los lineamientos establecidos en este Manual de Políticas Complementarias de Seguridad de la Información.