POLITICAS Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL GRUPO EMPRESARIAL COOPERATIVO COOMEVA

TABLA DE CONTENIDO

1. Objetivo

Establecer las políticas y responsabilidades para la gestión de la seguridad y privacidad de la información que debe regir para todas las empresas del Grupo Empresarial Cooperativo Coomeva (**en adelante GECC**), así como la normatividad que aplica para sus colaboradores.

2. Alcance

Las políticas y responsabilidades que se establecen en el presente documento aplican para:

- Todas las empresas y unidades de negocios del **GECC.**
- Todos los dirigentes, administradores, colaboradores, proveedores y contratistas del **GECC.**

3. Términos y Definiciones

- **Activo de información**: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

- **Administradores:** Hace referencia a los Juntas Directivas de las empresas del GECC.

- **Algoritmos de cifrado**: Soluciones tecnológicas especializadas, para hacer que la información sea incomprensible para aquellas personas que no deban tener acceso a la información que se quiere proteger.

- **Ambientes de desarrollo**: Conjunto de recursos tecnológicos en los cuales se realiza la construcción, modificación y reparación de programas informáticos.

- **Backup**: Copia de la información original que se realiza como medida preventiva para recuperar la información en caso de daño o pérdida.

- **Cadena de suministro**: Conjunto de procesos y recursos involucrados de manera directa o indirecta en acciones orientadas a satisfacer las necesidades del cliente.

- **Ciclo de vida de la información**: Son los diferentes estados en los cuales se puede encontrar la información e incluye su creación, procesamiento, almacenamiento, trasmisión, eliminación y destrucción.

- **Cifrado de información**: Acción de aplicar soluciones tecnológicas especializadas, para hacer que la información sea incomprensible para aquellas personas que no deban tener acceso a la información que se quiere proteger.

- **Códigos fuente**: Conjunto de instrucciones seguidas por un computador para la ejecución de un programa informático.

- **Contratistas**: Colaboradores de Coomeva, administrados y contratados por empresas en Misión.

- **Dirigentes:** Hace referencia a los miembros del Consejo de Administración y Junta de Vigilancia del GECC.

- **Dispositivos móviles**: Computadores portátiles, tabletas, dispositivos para autenticación biométrica, teléfonos inteligentes y sus tarjetas de memoria.

- **EMM**: Solución tecnológica a través de la cual los dispositivos móviles se conectan la infraestructura empresarial

- **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta, a nombre y según las directrices del responsable del tratamiento.

- **Endpoint**: Solución tecnológica que proporciona funciones de seguridad para proteger estaciones de trabajo, smartphones y tablets.

- **Etiquetado de información**: Consiste en marcar la información para identificar su naturaleza y el tratamiento que debe recibir.

- **Fábricas de software:** Son aquellos proveedores que realizan tareas de desarrollo de software para el GECC.

- **Información personal:** Es toda aquella información asociada a una persona y que permite su identificación (documento de identidad, lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral o profesional).

- **Información sensible**: Es toda información que haga referencia a estado de salud, características físicas, ideología política, vida sexual de las personas.

- **Medios removibles**: Son aquellos elementos de almacenamiento de información que puede ser extraídos tales como cintas, discos, casetes, memorias de almacenamiento, unidades de almacenamiento removibles, discos compactos (CD), discos de video digital (DVD) e información impresa.

- **Oficial de protección de datos**: es la persona que tiene como función la vigilancia y control de la aplicación de la Política de Protección de Datos Personales, bajo la orientación y lineamientos del GECC. Toda vez que el GECC, está conformado por una agrupación de empresas, cada una de ellas, tiene designado un oficial de protección.

- **Teletrabajo:** Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.

- **Titular de los datos personales**: persona natural cuyos datos personales sean objeto de tratamiento.

- **Tratamiento de datos personales**: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

- **Usuario:** Persona que usa habitualmente un servicio.

- **VPN (Virtual Private Network):** Red de comunicación segura que permite la conexión a la red corporativa a través de una red pública o internet.

4. Descripción

Acogiendo las políticas generales definidas en la Resolución No.150 (RE-PE-AD-2013.150) y de aquellas que la complementen, modifiquen o sustituyan y que rigen para todas las unidades organizativas y las entidades que conforman el **GECC**, las siguientes políticas y responsabilidades de seguridad de la información se establecen en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad y privacidad de la información del **GECC**.

Este documento se modificará en respuesta a las novedades que a futuro se registren en la materia que trata, las cuales serán debidamente aprobadas y comunicadas.

5. Políticas y Responsabilidades de Seguridad y Privacidad de la Información del GECC

5.1. Organización Interna

5.1.1. Objetivo

Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

5.1.2. Alcance

Estas políticas y responsabilidades aplican para todos los administradores, colaboradores, proveedores y contratistas del **GECC**.

5.1.3. Roles y responsabilidades para la seguridad de la información

Definidos en el GC-DC-505 Manual Corporativo de Seguridad y Privacidad de la Información del GECC – Numeral 4.5 – Gobierno y Roles para la Gestión de Seguridad y Privacidad de la Información en el GECC.

5.1.4. Segregación de funciones

Es responsabilidad de la Gerencia Corporativa de Operaciones, la Gerencia Corporativa de Gestión Humana o quienes hagan sus veces en el GECC:

- Garantizar que las funciones y áreas de responsabilidad en conflicto estén separadas para reducir el uso indebido, accidental o deliberado, de los activos de información de una organización.

5.1.5. Contacto con las autoridades

Es responsabilidad de la Gerencia Corporativa de Riesgo, o quienes hagan sus veces en el GECC:

- Garantizar la creación y actualización del listado de contactos de las autoridades relacionadas con la Seguridad y Privacidad de la información.

- Definir y comunicar un procedimiento a través del cual se especifique el motivo, el medio y la autoridad a quien se debe comunicar los incidentes relacionadas con la Seguridad y Privacidad de la información.

5.1.6. Contacto con los grupos de interés

Es responsabilidad de la Gerencia Corporativa de Riesgo, o quienes hagan sus veces en el GECC:

- Garantizar la creación y actualización del listado de contactos con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad y privacidad de la información.

5.1.7. Seguridad de la información en la gestión de proyectos

Es responsabilidad de la Gerencia Corporativa Administrativa, la Gerencia Corporativa de Riesgo, o quienes hagan sus veces en el GECC:

- Garantizar que los riesgos de seguridad y privacidad de la información se identifiquen y traten como parte de un proyecto, independientemente de la naturaleza del proyecto.

5.2. Dispositivos móviles

5.2.1. Objetivo

Definir las reglas y requerimientos que deben cumplir los dirigentes, administradores, colaboradores, proveedores y contratistas del **GECC** que se conecten a través de dispositivos móviles personales o corporativos (computadores portátiles, tabletas, dispositivos para autenticación biométrica, teléfonos inteligentes y sus tarjetas de memoria) a los servicios de la red corporativa del **GECC**.

Estas reglas y requerimientos se definen con el fin de minimizar la exposición del **GECC** a daños ocasionados por accesos no autorizados a los recursos de la organización. Los daños incluyen la perdida de confidencialidad, integridad o disponibilidad de la información.

5.2.2. Alcance

Estas políticas y responsabilidades aplican para todos los dirigentes, administradores, colaboradores, proveedores y contratistas del **GECC**, que hagan uso de un dispositivo móvil personal o corporativo y se use para acceder a los recursos de la red corporativa. Esta política aplica para conexiones locales y remotas usadas para realizar trabajos en nombre del **GECC**.

5.2.3. Políticas y responsabilidades

Es responsabilidad de la Dirección de Servicios de TI CSA y/o el proveedor de servicios:

- Llevar un inventario actualizado de los dispositivos móviles autorizados para acceder a los recursos de la red corporativa.

- Definir, implementar y comunicar los procedimientos que garanticen la administración de los dispositivos móviles durante su ciclo de vida al interior de la organización (aprovisionamiento, actualización, borrado, desconexión, etc.).

- Disponer de los mecanismos necesarios para que los dispositivos móviles autorizados para acceder a los recursos de la red corporativa sean administrados de forma centralizada desde la solución definida por la organización (Endpoint & EMM).

- Asegurar que los dispositivos móviles autorizados para acceder a los recursos de la red corporativa cuenten con el software antivirus, anti-spam, anti-malware y firewall definido por el GECC, y se active la geo-localización del mismo.

- Asegurar que los dispositivos móviles autorizados para acceder a los recursos de la red corporativa cuenten con las versiones de sistema operativo autorizadas por la organización.

- Velar porque los dispositivos móviles autorizados para acceder a los recursos de la red corporativa sólo cuenten con software autorizado por la organización.

- Asegurar que todo dispositivo móvil autorizado para acceder a los recursos de la red corporativa cuente con una solución de seguridad que facilite el control, distribución y actualización de aplicaciones sobre el mismo.

- Mantener actualizadas las restricciones de acceso a los servicios de información corporativos (aplicaciones, compartidos, etc.) desde dispositivos móviles propios y de terceros.

- Asegurar que todo dispositivo móvil que almacene o acceda a información clasificada como confidencial o de uso interno, solicite credenciales de acceso para hacer uso del mismo.

- Asegurar el bloqueo de la cuenta del usuario o del dispositivo móvil (tabletas, datáfonos, teléfonos inteligentes) después de tres (3) intentos fallidos de autenticación.

- Asegurar que todo dispositivo móvil que almacene información clasificada como confidencial o de uso interno sea cifrado completamente (FDE – Full Disk Encription). Si el dispositivo móvil no soporta el cifrado, la empresa dueña del activo debe gestionar el remplazo del mismo o el mejoramiento de sus capacidades físicas. Si el dispositivo es personal, se restringirá el acceso a la información.

- Asegurar que todo dispositivo móvil que este bajo el riesgo de infección de malware corra el software de anti-virus de manera periódica (como mínimo una vez a la semana).

- Asegurar la inactivación del dispositivo móvil o el borrado de la información almacenada sobre el mismo a través de la herramienta EMM definida por la organización ante el robo o pérdida del mismo.

Es responsabilidad de líder del proceso:

- Autorizar a los colaboradores y contratistas del **GECC** que estén bajo supervisión directa, el uso de dispositivos móviles personales con fines laborales, además de garantizar la aceptación de las políticas corporativas que serían aplicadas sobre los dispositivos.

Es responsabilidad del Proveedor de servicios con el apoyo de la Dirección de Servicios de TI de CSA:

- Asegurar que las empresas del grupo que contraten el acceso a las bases de datos biométricas a través de la Registraduría Nacional del Estado Civil, cumplan con lo establecido en la Resolución 5633 de 2016 y sus anexos técnicos, cuando pretendan implementar un modelo de autenticación biométrica a través de un dispositivo móvil.

Es responsabilidad de los dirigentes, administradores, colaboradores y contratistas del GECC:

- Conocer y aceptar las políticas de seguridad y privacidad corporativas cuando se hace uso de dispositivos móviles personales con fines laborales (protección física, actualización de software, desistir de la propiedad de los datos, permitir el borrado remoto de los datos, etc.).

- Garantizar que el dispositivo móvil corra una versión actualizada del sistema operativo, con el fin de asegurar que esta puede recibir las actualizaciones de seguridad correspondientes.

- Reportar al área de Riesgo y Continuidad Tecnológica de CSA o a la Mesa de Servicio el robo o pérdida de los dispositivos móviles (tabletas y teléfonos inteligentes), para proceder a realizar la inactivación o borrado respectivo de forma remota.

- Asegurar que no se acceda a información clasificada como confidencial o de uso interno desde dispositivos de terceros.

Es responsabilidad de la Gerencia Corporativa de Riesgo:

- Garantizar la sensibilización del personal frente a los riesgos asociados al uso de dispositivos móviles.

- Monitorear el cumplimiento de las políticas y responsabilidades en materia de seguridad y privacidad de la información.

5.3. Teletrabajo

5.3.1. Objetivo

Definir las reglas y requerimientos que deben cumplir los administradores, colaboradores y contratistas del **GECC** que realicen actividades para el GECC bajo la modalidad de teletrabajo.

Estas reglas y requerimientos se definen con el fin de proteger la información a la que tendría acceso o que es procesada o almacenada en los lugares en donde se realiza teletrabajo.

5.3.2. Alcance

Estas políticas y responsabilidades aplican para todos los administradores, colaboradores, proveedores y contratistas del **GECC**, que hagan uso de la modalidad de teletrabajo.

5.3.3. Políticas y responsabilidades

Es responsabilidad de la Gerencia Corporativa de Gestión Humana, la Gerencia Corporativa de Jurídica, o quienes hagan sus veces en el GECC:

- Establecer los procedimientos y contratos de teletrabajo aplicables al GECC, cumpliendo con lo establecido en la Ley 1221 de 2008 y el Decreto 0884 de 2012 emitido por el Ministerio del trabajo.

5.4. Seguridad de los recursos humanos

5.4.1. Objetivo

Concientizar e informar de forma continua a los dirigentes, administradores, colaboradores y contratistas sobre las políticas que afectan el desarrollo de sus funciones y de sus responsabilidades en materia de seguridad y privacidad de la información.

5.4.2. Alcance

Estas políticas y responsabilidades aplican para todos los dirigentes, administradores, colaboradores y contratistas del GECC, que efectúen actividades dentro del ámbito del GECC, sea cual fuere su nivel jerárquico y/o su posicionamiento organizacional.

5.4.3. Políticas y responsabilidades

5.4.3.1. Antes de asumir el empleo

Es responsabilidad de la Gerencia Corporativa de Gestión Humana:

- Asegurar que, para el proceso de selección, se emplea un mecanismo de verificación de antecedentes ajustado a la ley, e informar la clasificación de información a la que tendría acceso el colaborador o contratista.

- Asegurar que, para el proceso de selección y contratación, se cuente con la autorización del tratamiento de datos personales por parte de los candidatos y colaboradores.

- Asegurar que todo colaborador y contratista acepte el acuerdo de confidencialidad y no divulgación y las políticas de la seguridad y privacidad de la información definidas por el **GECC**.

- Asegurar que todo colaborador y contratista conozca y acepte sus responsabilidades frente a la seguridad y privacidad de la información.

- Asegurar que todo colaborador y contratista conozca y acepte sus responsabilidades frente a la ley de derechos de autor y protección de datos personales.

- Durante el proceso de inducción a nuevos colaboradores, incluir una charla de concientización con apoyo de la Gerencia Corporativa de Riesgo sobre los requisitos de seguridad y privacidad de la información, responsabilidades legales, uso correcto de los

servicios de procesamiento de Información y procesos disciplinarios antes de que se les otorgue acceso a información o sistemas de información sensibles del GECC.

5.4.3.2. Durante la ejecución del empleo

Es responsabilidad de la Gerencia Corporativa de Riesgo:

- Asegurar que todos los colaboradores y contratistas conozcan y acepten las políticas de seguridad y privacidad de la información del GECC, así como, entender y aceptar las consecuencias y medidas a tomar por el incumplimiento de las mismas.

- Generar campañas periódicas de capacitación y sensibilización en seguridad y privacidad de la información.

- Establecer un programa de toma de conciencia, educación y formación frente a las políticas, controles definidos y procedimientos de seguridad y privacidad de la información relacionados con los cargos desempeñados por colaboradores o contratistas.

- Monitorear el cumplimiento de las políticas y responsabilidades en materia de seguridad y privacidad de la información.

- Ofrecer la asesoría requerida por los colaboradores o contratistas en materia de seguridad y privacidad de la información.

- Realizar una revisión anual o cuando sea necesario del material de capacitación en seguridad y privacidad de la información, a fin de evaluar la actualización y vigencia del mismo.

- Definir un mecanismo anónimo de reporte frente al incumplimiento de políticas y procedimientos de seguridad y privacidad de la información.

Es responsabilidad de la Presidencia Ejecutiva y la Gerencia Corporativa de Riesgo:

- Asegurar que los dirigentes, administradores, colaboradores y contratistas apliquen las políticas y procedimientos de seguridad y privacidad de la información definidos por la organización.

Es responsabilidad de la Gerencia Corporativa de Gestión Humana y Arquitectura Empresarial:

- Garantizar que todos los perfiles de cargo incluyan las responsabilidades frente a la seguridad y privacidad de la información.

Es responsabilidad de la Gerencia Corporativa de Gestión Humana:

- Establecer un proceso disciplinario formal, a través del cual se den a conocer y se apliquen las sanciones asociadas al incumplimiento o violación de las políticas y procedimientos de seguridad y privacidad de la información definidos por la organización.

5.4.3.3. Terminación y cambio de empleo

Es responsabilidad de la Gerencia Corporativa de Gestión Humana:

- Definir y comunicar un procedimiento a través del cual se informe de manera oportuna a la Unidad de Tecnología Informática de CSA y demás áreas interesadas el retiro de colaboradores y contratistas, para dar inicio al proceso de eliminación de usuarios y perfiles que les fueron asignados durante su permanencia en el GECC, al igual que la devolución de sus activos (dispositivo móvil, equipo de cómputo, carné, tarjeta de proximidad, etc.).

Es responsabilidad de cada supervisor de contrato designado por el GECC:

- Informar de manera oportuna a la Unidad de Tecnología Informática de CSA y demás áreas interesadas el retiro de contratistas, proveedores o terceros que tengan acceso a los recursos del GECC y a los diferentes sistemas de información.

5.5. Gestión de activos

5.5.1. Objetivos

El objetivo de estas políticas y responsabilidades es definir las reglas necesarias para realizar la identificación de los activos de información, con el fin de definir su clasificación de acuerdo a la sensibilidad y criticidad, y de esta forma garantizar que reciban un nivel de protección apropiado.

5.5.2. Alcance

Estas políticas y responsabilidades se aplican a todos los activos de información administrados en el GECC, cualquiera que sea el soporte o medio en que se encuentre.

5.5.3. Políticas y responsabilidades

5.5.3.1. Responsabilidad por los activos

Es responsabilidad de los líderes de proceso al interior del GECC:

- Asegurar la designación de los propietarios de los activos de información al momento de su creación o cuando son transferidos a la organización.

5.5.3.1.1. Inventario de activos

Es responsabilidad de los líderes de los procesos:

- Inventariar los activos de información (datos, información impresa, aplicaciones / software, equipos informáticos / hardware, redes de comunicaciones, medios de almacenamiento, servicios, recurso humano, instalaciones, equipamiento auxiliar) involucrados en el desarrollo de sus procesos y dentro del ciclo de vida de la información.

- Garantizar que los activos de información, se encuentran clasificados de acuerdo a las pautas establecidas por la Gerencia Corporativa de Riesgo para tal fin.

- Mantener un inventario de activos de información, de manera exacta y consistente. Este inventario debe ser actualizado al menos una vez por año.

- **Es responsabilidad de la Gerencia Corporativa de Riesgo y quienes hagan sus veces en el GECC,** realizar revisiones para verificar que los procesos mantienen actualizado su inventario de activos de información y que cumplen con el procedimiento definido para tal fin.

5.5.3.1.2. Propiedad de los activos

Es responsabilidad de la Gerencia Corporativa de Riesgo y quienes hagan sus veces en el GECC:

- Definir el procedimiento para la asignación de activos de información a colaboradores y contratistas.

- Definir los mecanismos y procedimientos que garanticen el apropiado tratamiento de los activos de información al momento de su eliminación o destrucción (física y digital).

Es responsabilidad de los líderes de los procesos:

- Garantizar la asignación de los activos de información requeridos por colaboradores y contratistas para el desarrollo de sus funciones con base en el procedimiento definido.

- Garantizar que los propietarios de los activos de información, sean colaboradores o procesos que tenga responsabilidad directa designada de la empresa sobre los mismos.

- Acoger los mecanismos y procedimientos definidos para la eliminación o destrucción de los activos de información.

- Validar de manera periódica las restricciones y clasificaciones de acceso a los activos importantes de acuerdo a las políticas de control de acceso aplicables.

Es responsabilidad de los propietarios de los activos de información:

- Garantizar la integridad, confidencialidad y disponibilidad de los activos a su cargo.

- Garantizar el manejo apropiado del activo cuando es eliminado o destruido.

5.5.3.1.3. Uso aceptable de los activos

Es responsabilidad de la Gerencia Corporativa de Riesgo, la Dirección de Servicios de TI CSA y quien haga sus veces en las empresas del GECC:

- Definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son para proteger su confidencialidad, integridad y disponibilidad.

Es responsabilidad de los dirigentes, administradores, colaboradores, proveedores y contratistas:

- Cumplir y acoger con integridad las políticas de seguridad definidas por la organización para dar un uso racional y eficiente a los activos asignados que son propiedad del **GECC**.

5.5.3.1.3.1. Respaldo de la información

Es responsabilidad de la Gerencia Corporativa de Riesgo, la Dirección de Servicios de TI CSA y quien haga sus veces en las empresas del GECC:

- Establecer mecanismos de respaldo que garanticen la confidencialidad, integridad y disponibilidad de la información sensible alojada en los equipos de cómputo.

Es responsabilidad de los propietarios de los activos de información:

- Adoptar los mecanismos de respaldo establecidos en el GECC.

Es responsabilidad de los colaboradores y contratistas:

- Alojar la información que necesita ser respaldad en los lugares establecidos para ello.

5.5.3.1.3.2. Protección EndPoint

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Asegurar el alistamiento para entrega inicial de los equipos de cómputo, garantizando la correcta instalación de la solución EndPoint.

- Aplicar la configuración definida para la solución EndPoint que garantice la protección de las estaciones de trabajo (portátiles, de escritorio) y servidores.

Es responsabilidad de los colaboradores, proveedores y contratistas del GECC:

- Reportar de inmediato a través de la mesa de servicio toda inconsistencia presentada con la protección EndPoint en su estación de trabajo (ausencia del software, desactualización, no detección, sospecha de virus).

- Analizar con la solución antivirus, todo archivo digital recibido de entes externos al **GECC** antes de su apertura en la estación de trabajo.

- Analizar con la solución antivirus, todo archivo digital antes de ser enviado a entes externos al **GECC.**

Es responsabilidad de los líderes de los procesos con apoyo de la Dirección de Servicios de TI CSA:

- Garantizar que a todas las estaciones de trabajo (portátiles y de escritorio) que almacenen información confidencial o de uso interno se le realice el cifrado completo del disco duro, haciendo uso de la solución definida por el **GECC**.

5.5.3.1.3.3. Uso responsable de las cuentas de acceso

Es responsabilidad de los dirigentes, administradores, colaboradores, proveedores y contratistas del GECC:

- Garantizar el correcto uso de las cuentas y contraseñas de acceso a los sistemas ya que su uso es personal e intransferible.

- La creación de contraseñas seguras donde no se incluya información personal como nombres, fechas de nacimiento u otros de fácil conocimiento por terceros.

- Efectuar el cambio de sus contraseñas de acceso a los diferentes sistemas de manera periódica o cuando estos consideren que ha sido expuesta a terceros.

Es responsabilidad de la Gerencia Nacional de Educación y Democracia y de la Presidencia Ejecutiva:

- Informar a través de la Mesa de Servicio, el retiro de la organización de los dirigentes y miembros de juntas directivas – administradores, respectivamente, tan pronto éste se produzca para realizar la correspondiente eliminación de cuentas en los sistemas de información.

Es responsabilidad de la Gerencia Corporativa de Gestión Humana y quienes hagan sus veces en el GECC:

- Informar a través de la Mesa de Servicio, el retiro de los colaboradores y contratistas de la organización tan pronto esta se produzca para realizar la correspondiente eliminación de cuentas en los sistemas de información.

Es responsabilidad de los líderes de proceso:

- Informar a través de la Mesa de Servicio, el retiro de los proveedores de la organización tan pronto esta se produzca para realizar la correspondiente eliminación de cuentas en los sistemas de información.

Es responsabilidad del propietario de un activo de información:

- Realizar una depuración periódica de las cuentas de acceso en cada uno de activos a los cuales aplique.

5.5.3.1.3.4. Uso de correo electrónico y sistemas de mensajería instantánea

Es responsabilidad de los colaboradores y contratistas del GECC:

- Asegurar que todas las comunicaciones laborales que se realicen a través de correo electrónico, tanto internas como externas, se efectúen solamente a través de la cuenta de correo electrónico corporativa.

- Abstenerse de utilizar la cuenta de correo corporativo para la recepción o envío de mensajes de tipo personal.

- Abstenerse de utilizar la cuenta de correo corporativo para la recepción y envío de mensajes spam (no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades), hoax (es un intento de hacer creer que algo falso es real), o con contenido que pueda resultar ofensivo o dañino para otros usuarios (como virus o pornografía).

- Respetar la privacidad de las cuentas de correo y evitar el envío de mensajes desde cuentas de otros usuarios.

- Administrar el espacio asignado a su cuenta de correo, realizando la descarga local de los mensajes y/o depuración, con el fin de evitar el desbordamiento y ampliaciones injustificadas del mismo.

- Garantizar que toda la información confidencial o de uso interno que deba ser transmitida a través de correo electrónico, emplee mecanismos de cifrado fuerte / certificados digitales, y a través de las redes de datos y sistemas internos únicamente.

- Abstenerse de utilizar el servicio de correo corporativo para la transmisión de cualquier correo masivo no solicitado, ya que el área autorizada para realizar este tipo de difusiones es la Gerencia Corporativa de Comunicaciones.

- Abstenerse del envió de información confidencial o de uso interno a través de los sistemas de mensajería instantánea.

- Abstenerse de enviar mensajes a través de correo electrónico o mensajería instantánea, que ofendan la dignidad, intimidad y buen nombre de las personas, de las instituciones, o para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil; de igual forma se prohíbe difundir ideas políticas, religiosas, propagandas entre otros.

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar que los administradores de las soluciones de correo electrónico y mensajería instantánea, no visualicen las comunicaciones de los dirigentes, administradores, colaboradores y contratistas, a menos que exista una autorización judicial o de autoridad competente.

Es responsabilidad de los Jefes directos de área:

- Determinar la necesidad de uso de las soluciones de mensajería instantánea aprobadas para el **GECC** y solicitar el acceso a las mismas para sus colaboradores y contratistas.

5.5.3.1.3.5. Uso del acceso a internet

Es responsabilidad de los colaboradores y contratistas del GECC:

- Utilizar el servicio con propósitos lícitos y en cumplimiento de las funciones específicas de su cargo; toda actividad de navegación es registrada por el GECC, quien podrá revelar cualquier acceso cuando una autoridad judicial así lo requiera.

- Evitar el acceso y abandonar sitios de internet catalogados como de baja reputación.

- Evitar la descarga de software de Internet, ya que esta labor sólo está permitida para el personal del área de Riesgo y Continuidad Tecnológica de CSA, quienes analizan y aprueban la instalación de software en los equipos del GECC.

- Abstenerse de descargar y usar software malicioso o documentos que brinden información sobre cómo atentar contra la seguridad y privacidad de la información de la organización.

- Abstenerse de alojar cualquier tipo de información corporativa en sitios de Internet que ofrezcan servicios para almacenar y/o compartir información, por ejemplo: Dropbox, Google drive, OneDrive, etc., si no se encuentra cifrada la información mediante los mecanismos definidos por el GECC.

- Evitar la descarga y/o emplear archivos de imagen, sonido o similares que puedan estar protegidos por derechos de autor sin la previa autorización de los mismos.

- Abstenerse de usar sitios que salten la seguridad del filtrado de contenido (Proxy).

- Desactivar la opción de autoguardado de contraseñas en los diferentes navegadores web.

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar el control técnico de acceso a sitios que puedan afectar la productividad de la organización, la seguridad y privacidad de su información o su personal.

5.5.3.1.3.6. Actividades prohibidas

- Ningún colaborador, proveedor o contratista del GECC está autorizado para realizar instalación de software en los dispositivos móviles o de escritorio de la organización. Toda solicitud al respecto debe ser escalada a través de la mesa de servicio y ejecutada por personal de soporte técnico, previa autorización del personal de Riesgo y Continuidad Tecnológica de CSA.

- La Dirección de Servicios de TI CSA, es la única instancia encargada de autorizar el uso de herramientas tecnológicas para análisis de tráfico y hacking ético al interior del GECC.

5.5.3.1.4. Devolución de activos

Es responsabilidad de la Gerencia Corporativa de Riesgo y quienes hagan sus veces en el GECC:

- Definir el procedimiento para la devolución de activos de información por parte de colaboradores y contratistas.

Es responsabilidad de los líderes de los procesos:

- Garantizar la devolución de los activos de información asignados a colaboradores y contratistas para el desarrollo de sus funciones con base en el procedimiento definido al terminar su relación laboral, este debe contemplar la entrega de elementos físicos, elementos electrónicos e información.

- Evitar que el colaborador o contratista realice copias no autorizadas de la información de la compañía al terminar su relación laboral.

- Asegurar la entrega de la información a la organización y el borrado seguro del activo tecnológico, cuando este sea vendido u obsequiado al colaborador o contratista.

5.5.3.2. Clasificación de la información

5.5.3.2.1. Clasificación de la información

Es responsabilidad de la Gerencia Corporativa de Riesgo y quienes hagan sus veces en el GECC:

- Definir los lineamientos para clasificación y manejo de la información en el GECC.
- Definir, implementar y comunicar el procedimiento para realizar la clasificación de la información del GECC.
- Definir los mecanismos de cifrado para la información de acuerdo al nivel de clasificación de la misma.

Es responsabilidad de los propietarios de los activos de información:

- Llevar a cabo la clasificación de los mismos, de acuerdo a los lineamientos establecidos.
- Actualizar la clasificación de la información, con base en variaciones de valor, sensibilidad, criticidad y exigencias legales para la misma.

Es responsabilidad de los líderes de proceso:

- Adoptar los lineamientos para la clasificación de la información como parte integral de su proceso.

5.5.3.2.2. Etiquetado de la información

Es responsabilidad de la Gerencia Corporativa de Riesgo y quienes hagan sus veces en el GECC:

- Definir los lineamientos para el etiquetado de la información del GECC soportada en formatos físicos o electrónicos.
- Definir, implementar y comunicar el procedimiento de etiquetado de información de acuerdo a la clasificación de la misma.

Es responsabilidad de los colaboradores y contratistas del GECC:

- Conocer y aplicar el procedimiento de etiquetado de la información.

5.5.3.2.3. Manejo de activos

Es responsabilidad de la Gerencia Corporativa de Riesgo y quienes hagan sus veces en el GECC:

- Definir, implementar y comunicar el procedimiento para el manejo de los activos de información de acuerdo a su clasificación.

Es responsabilidad de los líderes de proceso:

- Adoptar y garantizar la aplicación del procedimiento establecido para el manejo de activos de información en los procesos.

Es responsabilidad de los colaboradores y contratistas del GECC:

- Conocer y aplicar el procedimiento de manejo de activos.

5.5.3.3. Manejo de medios

5.5.3.3.1. Gestión de medios removibles

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar las condiciones físicas y ambientales necesarias para la preservación y seguridad de los medios removibles bajo su administración.

- Garantizar el inventario de los medios removibles utilizados dentro de la operación de TI, y llevar un registro de las actividades relacionados con los mismos.

Es responsabilidad de los colaboradores, proveedores y contratistas del GECC:

- Almacenar información confidencial o de uso interno en medios removibles autorizados por la organización, adoptando los mecanismos de cifrado establecidos por la misma**.**

Es responsabilidad de los líderes de proceso:

- Definir los permisos de acceso a las unidades de medios removibles de los equipos de cómputo, con base en las necesidades y responsabilidades de los colaboradores y contratistas bajo su cargo.

5.5.3.3.2. Disposición de los medios

Es responsabilidad de la Gerencia Corporativa de Riesgo y quienes hagan sus veces en el GECC:

- Definir, implementar y comunicar los procedimientos para el almacenamiento y eliminación segura de medios removibles del **GECC**, con el fin de evitar la fuga de información sensible para la organización.

- Apoyar en el análisis de riesgo en caso de daño de dispositivos que contienen información sensible, para determinar si los elementos se deberían destruir físicamente, reparar o desechar.

Es responsabilidad de los líderes de proceso:

- Aplicar los procedimientos de almacenamiento y eliminación segura de medios de almacenamiento bajo su responsabilidad.

- Mantener un registro actualizado de la disposición de los medios que contienen información confidencial o de uso interno.

5.5.3.3.3. Transferencia de medios físicos

Es responsabilidad de los líderes de proceso:

- Garantizar la trasferencia de los medios exclusivamente al destinatario a través de correo certificado o entidades especializadas.

- Mantener un registro actualizado de las empresas de correo certificado y autorizado, con las cuales se tiene relación.

- Garantizar la correcta protección física de los medios para su transferencia.

- Mantener una bitácora de trasferencia de medios, en la cual se detalle la información enviada, el tiempo de transferencia al destinatario y el recibo en su destino.

5.6. Control de acceso

5.6.1. Objetivo

Definir las reglas que se deben cumplir para el acceso seguro a las redes, equipos, sistemas de información, aplicaciones e instalaciones del **GECC**. Estas reglas y requerimientos están definidos con el fin de minimizar la exposición del **GECC** a daños que pueden ser el resultado de un acceso no autorizado a la información. Los daños incluyen la perdida de confidencialidad, integridad o disponibilidad de la información y/o sistemas críticos del **GECC**.

5.6.2. Alcance

Esta política aplica para todos los dirigentes, administradores, colaboradores, proveedores y contratistas del GECC.

5.6.3. Políticas y responsabilidades

5.6.3.1. Requisitos del negocio para control de acceso

- Todas las autorizaciones de acceso a los sistemas informáticos o redes del **GECC** deben proceder exclusivamente de personal autorizado, y se limitarán a los requerimientos del negocio, siempre bajo el precepto de la asignación de los menores privilegios posibles, garantizando adecuados niveles de segregación de funciones.

- Todos los colaboradores, proveedores y contratistas que requieran acceso a los sistemas informáticos y redes del **GECC**, deben contar con un identificador de usuario único y personalizado. Las contraseñas son definidas por el usuario y deben ajustarse al estándar establecido por el **GECC.**

- El acceso a las redes, equipos de cómputo (Estaciones de trabajo y Servidores), sistemas de información y aplicaciones está prohibido a menos que explícitamente se permita el acceso a un usuario o grupo de usuarios.

- El acceso a un activo de información sólo puede ser autorizado por su propietario, ya que este es el directamente responsable de cualquier incumplimiento, no conformidad y otros incidentes que se presente sobre el activo de información.

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar que sólo puedan tener acceso a la red local los equipos que se encuentren registrados en el dominio corporativo (conexión cableada, inalámbrica y VPN).

- Garantizar que sólo puedan tener acceso a los servicios de red los usuarios que hayan sido definidos en la matriz de perfiles por cargo.

- Definir, implementar y comunicar los procedimientos necesarios para realizar la gestión de acceso seguro de usuarios a las redes, equipos, sistemas de información y aplicaciones del **GECC.** Estos procedimientos deben cubrir todas las etapas del ciclo de vida desde el registro inicial hasta la cancelación del registro de usuarios y perfiles cuando ya no sea necesario su acceso.

- Garantizar que las conexiones remotas a los servicios corporativos que no están expuestos a internet se realicen exclusivamente a través del servicio VPN IPSec o SSL definidos por el **GECC.**

- Definir e implementar los procedimientos necesarios que garanticen el monitoreo de los servicios de red.

Es responsabilidad del propietario de un activo de información:

- Definir los roles de acceso a la información para usuarios estándar y privilegiados (solicitud de acceso, autorización de acceso, administración de acceso) y realizar una revisión y depuración periódica de los mismos.

Es responsabilidad de la Dirección de Servicios de TI CSA y del propietario de cada activo de información:

- Verificar de forma periódica (bimestral) los privilegios de acceso de los usuarios (estándar y privilegiados) a la información, con el fin de garantizar que los mismos sólo tengan acceso a los recursos para los que fueron autorizados.

Es responsabilidad de los líderes de proceso:

- Informar a la Unidad de Tecnología Informática de CSA y partes externas involucradas (terceros) la terminación de empleo de un funcionario; con el objetivo de controlar el intercambio de información entre las partes.

- Solicitar a la Unidad de Tecnología Informática de CSA realizar la validación y aplicación de cada uno de los puntos de la lista de validación técnica, cada vez que un proveedor requiera conectar su computador portátil a la red local.

5.6.3.2. Gestión de acceso de usuarios

Es responsabilidad de los Gerentes o Directores de Tecnología de las empresas del GECC:

- Apalancar los procesos de aprovisionamiento automático de usuarios a través de la solución de gestión de identidades (IDM) definida por la organización.

- Garantizar que el personal de la mesa de servicio no solicite las contraseñas de los usuarios como parte de la prestación de sus servicios, dado que el manejo de contraseñas es personal e intransferible.

Es responsabilidad de la Gerencia Corporativa de Riesgo y la Dirección de Servicios de TI CSA:

- Definir, implementar y comunicar los procedimientos necesarios para la gestión adecuada de usuarios privilegiados sobre los sistemas o procesos de la organización (sistemas operativos, bases de datos, aplicaciones y usuarios).

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar la gestión automatizada de los usuarios de las empresas a través de la solución de gestión de identidades (IDM) definida por la organización.

- Garantizar la asignación de usuarios personalizados para acceder a la red y servicios de red; evitando al máximo la asignación de usuarios genéricos para tal fin. En caso de ser necesario el uso de usuarios genéricos, se deberá garantizar un procedimiento a través del cual se asegure la confidencialidad de las credenciales asignadas al mismo, la periodicidad de cambio de contraseña, la inactivación del usuario, etc.; y adicionalmente se debe contar con el visto bueno de los responsables de tecnología de las empresas y la auditoria.

- Establecer los procedimientos necesarios para verificar la identidad de un usuario solicitante antes de cambiar la contraseña actual o asignar una nueva por parte del personal de soporte.

- Establecer los procedimientos necesarios para suministrar de manera segura las credenciales asignadas a los usuarios (confidencialidad).

- Garantizar que las credenciales por defecto utilizadas por fabricantes sean cambiadas tan pronto se realice la instalación del hardware o software adquirido por la organización.

- Garantizar que las contraseñas de usuarios con privilegios especiales sean actualizadas inmediatamente después del retiro de un colaborador con dicho conocimiento.

Es responsabilidad de los líderes de proceso:

- Informar a la Unidad de Tecnología Informática de CSA los cambios de rol de su personal o terminación de empleo; con el objetivo de ejecutar los procesos de depuración de privilegios respectivos.

5.6.3.3. Responsabilidades de los usuarios

Es responsabilidad de los dirigentes, administradores, colaboradores, proveedores y contratistas del GECC:

- Evitar el registro de sus credenciales en papel, notas electrónicas, dispositivos móviles; a menos que se cuente con mecanismos de almacenamiento seguros, y estos hayan sido aprobados por la Gerencia Corporativa de Riesgo y la Dirección de Servicios de TI CSA.

- Realizar el cambio de sus credenciales cuando estos consideren que ha sido expuesta a terceros.

- Definir contraseñas de acceso que se ajusten a las políticas definidas para los servicios de red.

- No compartir sus cuentas de usuario y contraseñas por ningún motivo, en el evento en que se detecte el préstamo de usuarios o contraseñas por asuntos tales como vacaciones, inasistencia o licencia, el caso será notificado a la Gerencia Corporativa de Riesgo o quien haga sus veces para que sean tomadas las medidas correctivas y disciplinarias del caso.

- Quienes hagan uso de las redes, equipos, sistemas de información y aplicaciones deben hacerse responsables de las acciones realizadas en los mismos con sus credenciales, así como del usuario y contraseña asignados para el acceso a estos.

- Tener cuidado de la presencia de terceros al momento de ingresar la contraseña para que no puedan observarla. En el caso que la contraseña pueda encontrarse en evidencia se debe cambiar inmediatamente.

5.6.3.4. Control de acceso a sistemas y aplicaciones

Es responsabilidad de la Gerencia Corporativa de Riesgo y la Dirección de Servicios de TI CSA:

- Definir, implementar y comunicar los procedimientos necesarios que garanticen la adopción de mecanismos de autenticación adecuados en las aplicaciones desarrolladas o adquiridas por la organización; al igual que la utilización de mecanismos de autenticación fuerte (medios criptográficos, tarjetas inteligentes, tokens o medios biométricos) cuando estos sean requeridos.

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar que las aplicaciones desarrolladas o adquiridas por la organización cuenten con los controles técnicos necesarios que permitan parametrizar y automatizar roles de acceso definidos para la aplicación.

- Garantizar que los recursos compartidos a través de la red (carpetas, unidades de disco, etc.) cuenten con los menores privilegios posibles para evitar el acceso a la información por parte de personal no autorizado.

- Definir, implementar y comunicar los procedimientos necesarios que garanticen la calidad y gestión interactiva de contraseñas en las aplicaciones desarrolladas o adquiridas por la organización.

Es responsabilidad de la Dirección de Servicios de TI CSA y los responsables de tecnología de las empresas del GECC:

- Restringir el acceso a los códigos fuente de los programas de la organización.

Es responsabilidad de las áreas de contratación de las empresas del GECC:

- Definir los controles necesarios para que los proveedores de desarrollo de software que prestan servicios al GECC restrinjan el acceso a los códigos fuente de los programas desarrollados.

5.6.3.5. Sistema de gestión de contraseñas

Es responsabilidad de la Dirección de Servicios de TI CSA, definir y garantizar el cumplimiento de los lineamientos para la creación de contraseñas seguras, implementando las siguientes políticas:

- Longitud mínima de 6 caracteres.
- Longitud máxima de 128 caracteres.
- La contraseña incluye caracteres de tres (3) de las siguientes categorías:
  - La contraseña debe tener al menos una (1) letra del alfabeto latino en mayúscula (A - Z).
  - La contraseña debe tener al menos una (1) letra del alfabeto latino en minúscula (a - z).
  - La contraseña debe tener al menos un (1) dígito en base decimal (0 - 9).
  - La contraseña debe tener al menos un (1) caracter no alfanumérico, como símbolos de exclamación, (¡!), de peso ($), o de almohadilla (#).
- Puede utilizar números en la contraseña.
- La contraseña distingue entre mayúsculas y minúsculas.
- Se pueden utilizar caracteres especiales en la contraseña.
- Debe utilizar una contraseña exclusiva.
- No puede utilizar los siguientes valores de atributo para la contraseña:
  - CN
  - displayName
  - Full Name
  - Given Name
  - Surname
- En aquellos sistemas en los que se pueda implantar, se debe llevar un histórico de contraseñas, mínimo 12, de tal forma que los usuarios no usen las contraseñas utilizadas anteriormente.
- Las contraseñas no se deben presentar en texto claro por ningún medio.
- Los sistemas de información de la organización deben obligar automáticamente a que las contraseñas de las cuentas de usuarios se cambien al menos una vez cada treinta (30) días.
- El sistema controlará el tiempo de inactividad del usuario y bloqueará la sesión automáticamente después de 5 minutos.
- A todos los usuarios se les deben revocar los privilegios de acceso automáticamente cuando no han tenido actividad durante un período de treinta (30) días calendario.
- Cuando se realice la creación de un usuario en un sistema, el administrador puede asignar una contraseña inicial, pero el sistema automáticamente debe solicitar cambio de la misma al titular de la cuenta cuando se presente el primer acceso.
- Al ingresar tres (3) intentos fallidos de contraseña en los sistemas de información, se bloqueará el usuario.

5.7. Criptografía

5.7.1. Objetivo

Definir las reglas y requerimientos que deben cumplir los dirigentes, administradores, colaboradores, proveedores y contratistas del **GECC** que hagan uso de la información clasificada como confidencial o de uso interno, para proteger la confidencialidad, autenticidad e integridad de la misma.

Estas reglas y requerimientos están definidos con el fin de minimizar la exposición del **GECC** a daños que pueden ser el resultado de un acceso no autorizado a la información. Los daños incluyen la perdida de confidencialidad, integridad o disponibilidad de la información y/o sistemas críticos del **GECC.**

5.7.2. Alcance

Esta política aplica para todos los dirigentes, administradores, colaboradores, proveedores y contratistas del **GECC,** que hagan uso de la información confidencial o de uso interno del **GECC.**

5.7.3. Políticas y responsabilidades

5.7.3.1. Controles criptográficos

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Disponer los mecanismos para el uso de algoritmos de cifrado para el aseguramiento de las conexiones de acceso remoto a la red y recursos de la organización.

- Establecer un procedimiento para garantizar que los dirigentes, administradores, colaboradores, proveedores y contratistas puedan tener acceso a información que se encuentre cifrada cuando sea necesario, y se tenga la autorización del propietario de la información.

- Establecer un procedimiento para poder gestionar las llaves electrónicas, de tal forma que se pueda controlar el cifrado y descifrado de la información confidencial o de uso interno, y de esta forma poder asegurar la confidencialidad, autenticidad e integridad de la información.

- Asegurar que todo dispositivo móvil o medio removible que almacene información confidencial o de uso interno, sea cifrado usando las herramientas de cifrado designadas por el GECC, independientemente de quien sea el propietario.

Es responsabilidad de los dirigentes, administradores, colaboradores y contratistas del GECC:

- Asegurar que la información clasificada como confidencial o de uso interno que requiera ser almacenada en cualquier nube pública debe ser cifrada antes de realizar dicho proceso; y de esta forma poder asegurar la confidencialidad e integridad de la información.

- Se deben implementar mecanismos de cifrado para el envío y recepción de información confidencial con los terceros contratados.

Es responsabilidad de los dirigentes, administradores, colaboradores, proveedores y contratistas del GECC, asegurar que la información clasificada como confidencial o de uso interno que vaya a ser usada por fuera de la organización, sea cifrada.

Es responsabilidad de la Gerencia Corporativa de Riesgo y la Dirección de Servicios de TI CSA:

- Establecer un marco de gestión del control criptográfico para el GECC, soportado en los requerimientos de clasificación y tratamiento de la información establecidos.

- Revisar cada año los algoritmos de cifrado (simétricos y/o asimétricos) usados y las longitudes de clave; y en caso de ser necesario realizar las actualizaciones necesarias para mantener la seguridad requerida, de acuerdo a los avances en técnicas de descifrado.

5.8. Seguridad física y del entorno

5.8.1. Objetivo

Prevenir e impedir accesos no autorizados, daños, interrupciones e interferencias a las instalaciones, sedes e información del GECC; controlar incendios, inundaciones, terremotos, disturbios civiles y otras formas de desastres naturales o causadas por el hombre que podrían perjudicar el correcto funcionamiento de los recursos informáticos que albergan la información del **GECC.**

5.8.2. Alcance

Las políticas y responsabilidades se aplican a todos los recursos físicos relativos a los sistemas de información GECC: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

5.8.3. Políticas y responsabilidades

Todas las áreas de sistemas, áreas de informática y equipos informáticos de las empresas del **GECC** deben cumplir las políticas y procedimientos de seguridad física, con el fin de restringir el acceso a personal no autorizado y evitar daños e interferencias en la información y los recursos tecnológicos que la soportan.

5.8.3.1. Áreas seguras

5.8.3.1.1. Perímetro de seguridad física

Es responsabilidad de la Dirección de Servicios de TI CSA, la Jefatura Nacional de Seguridad Física de CSA y la Gerencia Corporativa de Riesgo:

- Documentar los procedimientos necesarios para garantizar la definición, instalación y monitoreo de perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información (Centro de Datos), de suministros de energía eléctrica (Planta Eléctrica), de aire acondicionado (Aire Central), cuartos técnicos y de cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

- Definir y hacer cumplir las recomendaciones de seguridad de la información para el ingreso a las instalaciones de procesamiento de información (Centro de Datos), de suministros de energía eléctrica (Planta Eléctrica), de aire acondicionado (Aire Central), cuartos técnicos y de cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

Es responsabilidad de la Dirección de Servicios de TI CSA y la Jefatura Nacional de Seguridad de CSA:

- Garantizar la instalación y monitoreo de perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información (Centro de Datos), de suministros de energía eléctrica (Planta Eléctrica), de aire acondicionado (Aire Central), cuartos técnicos y de cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

Es responsabilidad de la Dirección de Servicios de TI CSA, la Jefatura Nacional de Seguridad de CSA, la Gerencia Corporativa de Riesgo y la Auditoría Corporativa:

- Garantizar que las instalaciones de procesamiento de información tengan perímetros de seguridad construidos con base en las buenas prácticas nacionales e internacionales (techos, paredes, pisos, puertas de acceso, ventanas, alarmas, recepción para control de acceso físicos, barreras de seguridad, etc.).

Es responsabilidad de la Gerencia Corporativa Administrativa, la Jefatura Nacional de Seguridad de CSA y la Gerencia Corporativa de Riesgo:

- Llevar un registro actualizado de los sitios protegidos, indicando la identificación del edificio y área, los principales elementos a proteger y las medidas de protección física implementadas.

- Realizar un análisis de riesgos (anual o por demanda) sobre los procesos e instalaciones de procesamiento de información, suministro de energía, aire acondicionado y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

5.8.3.1.2. Controles de acceso físico

Es responsabilidad de la Jefatura Nacional de Seguridad de CSA, la Dirección de Servicios de TI CSA o quien haga sus veces en el GECC:

- Implementar controles de acceso físico para proteger el acceso a los perímetros de seguridad definidos por el GECC.

- Supervisar o inspeccionar a los visitantes de áreas protegidas, validar su identidad y registrar la fecha y hora de ingreso y salida del lugar. Sólo se permitirá el acceso para propósitos específicos y autorizados, notificando al visitante al momento del ingreso sobre los requisitos de seguridad del área y los procedimientos de emergencia.

Es responsabilidad de la Jefatura Nacional de Seguridad de CSA:

- Limitar y controlar el acceso a la información corporativa y a las instalaciones de procesamiento de información sólo para personal autorizado a través de controles electrónicos, biométricos o físicos. Los controles generarán un registro protegido para permitir auditar todos los accesos.

Es responsabilidad de la Gerencia Corporativa Administrativa y Jefatura Nacional de Seguridad de CSA:

- Garantizar que los dirigentes, administradores, colaboradores, proveedores, contratistas y visitantes del GECC porten de manera visible el carné de la empresa.

- Garantizar el cumplimiento de los protocolos establecidos para el ingreso y control de visitantes, contratistas y proveedores a las instalaciones del GECC con base en los lineamientos definidos en el Manual de Seguridad de Oficinas.

Es responsabilidad de los dirigentes, administradores, colaboradores, proveedores, contratistas y visitantes del GECC, no prestar el carné de acceso ya que es de uso personal e intransferible, siendo considerados como una contraseña de acceso físico.

Es responsabilidad de la Jefatura Nacional de Seguridad de CSA y la Dirección de Servicios de TI CSA:

- Revisar y actualizar cada tres (3) meses, los derechos de acceso a las áreas protegidas, los cuales serán documentados y firmados por la persona responsable.

- Revisar los rastros o registros de acceso a las áreas protegidas.

Es responsabilidad de la Auditoría Corporativa del GECC o en su defecto quien sea propuesto por el Comité Técnico Corporativo de Seguridad de la Información:

- Realizar la validación correspondiente, para revocar aquellos accesos no requeridos o no autorizados.

5.8.3.1.3. Seguridad de las oficinas, recintos e instalaciones

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Ubicar las instalaciones clave (centro de datos principal y centro de datos alterno) en lugares a los cuales no pueda acceder personal no autorizado.

Es responsabilidad de la Gerencia Corporativa Administrativa y la Dirección de Gestión Integral de Instalaciones de CSA:

- Ubicar las instalaciones clave (servicios de suministros y cuartos técnicos) en lugares a los cuales no pueda acceder personal no autorizado.

Es responsabilidad de la Gerencia Corporativa Administrativa y la Dirección de Servicios de TI CSA:

- Garantizar que los edificios o sitios donde se realicen actividades de procesamiento de información sean discretos y ofrezcan un señalamiento mínimo de su propósito.

Es responsabilidad de la Gerencia Corporativa Administrativa:

- Garantizar que las instalaciones donde se ejecutan actividades o manipula información confidencial o de uso interno no sean visibles o auditables desde el exterior.

- Garantizar que los directorios y guías telefónicas internas que identifican las instalaciones de procesamiento de información confidencial o de uso interno no sean accedidas por personal no autorizado.

5.8.3.1.4. Protección contra amenazas externas y ambientales

- **Es responsabilidad de la Gerencia Corporativa Administrativa y la Gerencia Corporativa de Riesgo,** contratar asesoría especializada que permita evitar o mitigar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre.

5.8.3.1.5. Trabajo en áreas seguras

Es responsabilidad de la Gerencia Corporativa de Gestión Humana y líderes de proceso:

- Dar a conocer al personal sobre la existencia de áreas protegidas, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.

Es responsabilidad de la Dirección de Servicios de TI CSA, la Gerencia Corporativa Administrativa y la Jefatura Nacional de Seguridad de CSA:

- Garantizar que el trabajo de dirigentes, administradores, colaboradores, contratistas y proveedores en áreas seguras siempre sea supervisado por el personal responsable.

- Garantizar la revisión periódica de las áreas seguras, al igual que cerrarlas con llave cuando estas se encuentren vacías.

- Garantizar que no se haga uso de equipo fotográfico, de video, audio u otro equipo de grabación (cámaras en dispositivos móviles) dentro de las áreas seguras a menos que se cuente con la autorización respectiva.

5.8.3.1.6. Áreas de despacho y carga

Es responsabilidad de la Jefatura Nacional de Seguridad de CSA garantizar:

- Que el acceso al área de carga y despacho desde el exterior del edificio sea restringido al personal identificado y autorizado.

- Que las puertas de las áreas de carga y despacho se encuentren cerradas cuando el personal que ejecuta la labor se encuentre al interior de la organización.

- La inspección del material que ingresa con el fin de detectar la presencia de explosivos, químicos u otros materiales peligrosos antes de retirarse del área de carga y despacho.

Es responsabilidad de la Gerencia Corporativa Administrativa y Jefatura Nacional de Seguridad de CSA:

- Garantizar que las áreas de carga y despacho se diseñen de forma tal que el personal encargado de estas actividades realice su trabajo sin tener acceso a otras locaciones del edificio.

5.8.3.2. Equipos

5.8.3.2.1. Ubicación y protección de los equipos

Es responsabilidad de la Dirección de Servicios de TI CSA, la Gerencia Corporativa Administrativa y la Jefatura Nacional de Seguridad de CSA:

- Ubicar y proteger los equipos del GECC de forma adecuada, con el fin de reducir los riesgos de amenazas y peligros del entorno, y el posible acceso no autorizado.

Es responsabilidad de la Dirección de Servicios de TI CSA, la Gerencia Corporativa Administrativa, la Dirección de Gestión Integral de Instalaciones de CSA y la Jefatura Nacional de Seguridad de CSA:

- Ubicar los equipos (servidores, equipos de comunicaciones, equipos de cómputo, equipos de monitoreo, plantas eléctricas, plantas telefónicas, etc.) en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.

Es responsabilidad de la Dirección de Servicios de TI CSA y los líderes de tecnología de las empresas del GECC:

- Ubicar las instalaciones de procesamiento y almacenamiento de información donde maneja información confidencial o de uso interno en sitios que permitan la supervisión continua, reduciendo riesgos de visualización de información por personal no autorizado y fuga de información debido a filtración.

Es responsabilidad de la Dirección de Servicios de TI CSA y la Jefatura Nacional de Seguridad de CSA:

- Aislar los elementos que requieren protección especial para reducir el nivel general de protección implementada.

Es responsabilidad de la Jefatura Nacional de Seguridad de CSA y la Dirección de Gestión Integral de Instalaciones de CSA:

- Adoptar controles para minimizar los riesgos de amenazas físicas y ambientales (robo, incendio, explosivos, humo, agua, falla del suministro de agua, polvo, vibración, efectos químicos, falla del suministro eléctrico, interferencia en comunicaciones, radiación, electromagnética, vandalismo, etc.).

Es responsabilidad de los Colaboradores, Proveedores, Contratistas y Visitantes:

- Abstenerse del consumo de alimentos, bebidas, tabaco o similares, dentro de las instalaciones de procesamiento de información o en sus cercanías.

- No proveer información sobre los sistemas de control de acceso, seguridad física e informática, así como de la ubicación de las áreas donde se procesa información a personas no autorizadas.

- Aplicar los controles definidos por el GECC para garantizar un trabajo seguro desde la casa, teletrabajo y sitios temporales.

Es responsabilidad de la Gerencia Corporativa de Gestión Humana:

- Definir y aplicar las sanciones respectivas ante el incumplimiento de la política de consumo de alimentos, bebidas, tabaco o similares, dentro de las instalaciones de procesamiento de información o en sus cercanías.

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Hacer seguimiento a las condiciones ambientales (temperatura y humedad) para garantizar que estas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de información "propias", y exigir el seguimiento a los proveedores para las instalaciones de procesamiento tercerizadas. Esta revisión se realizará cada seis (6) meses o cuando sea necesario.

Es responsabilidad de la Dirección de Gestión Integral de Instalaciones de CSA y la Gerencia Corporativa Administrativa:

- Proteger las instalaciones del GECC frente a descargas eléctricas atmosféricas, al igual que las líneas de comunicaciones y de potencia entrantes.

5.8.3.2.2. Servicios de suministro

Es responsabilidad de la Dirección de Gestión Integral de Instalaciones de CSA y la Gerencia Corporativa Administrativa:

- Proteger los equipos del **GECC** contra fallas de energía u otras interrupciones causadas por fallas en los servicios de suministro.

- Garantizar que los servicios de suministro, tales como: electricidad, agua, alcantarillado, ventilación y aire acondicionado, sean inspeccionados y probados periódicamente para asegurar su vigencia, adecuado funcionamiento y la autonomía requerida.

- Dotar a las instalaciones de un sistema de alimentación ininterrumpida (UPS) para asegurar el apagado regulado y sistemático, o la ejecución continua del equipamiento que sustenta las operaciones críticas del GECC.

- Disponer de generadores de respaldo en las instalaciones del **GECC** para dar respuesta a los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía eléctrica.

- Disponer de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la(s) UPS permita el encendido manual de los mismos.

- Garantizar la instalación de iluminación y comunicaciones de emergencia en las instalaciones del **GECC.** De igual forma, garantizar que los interruptores y válvulas de emergencia para interrumpir el suministro de energía, agua, gas u otros servicios estén ubicados cerca de las salidas de emergencia o cuartos de equipos.

- Realizar la gestión necesaria para dar redundancia a los servicios de suministro básico como agua y energía.

- Garantizar el suministro de agua estable y adecuado para la alimentación del aire acondicionado y los sistemas de extinción de incendios en las instalaciones del GECC.

Es responsabilidad de los líderes de proceso:

- Garantizar el desarrollo de los planes de contingencia que contemplarán las acciones que han de emprenderse ante una falla de la(s) UPS del GECC.

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Disponer de dos (2) o más rutas para la conexión de los equipos de comunicaciones con el proveedor del servicio, garantizando los protocolos legales locales para comunicaciones de emergencia.

5.8.3.2.3. Seguridad del cableado

Es responsabilidad de la Dirección de Servicios de TI CSA y la Dirección de Gestión Integral de Instalaciones de CSA:

- Garantizar que el cableado de energía eléctrica y de telecomunicaciones que transporta datos o brinda apoyo a los servicios de información del GECC esté protegido contra interceptación, interferencia o daño.

- Garantizar que las líneas de energía eléctrica y de telecomunicaciones que ingresan a instalaciones de procesamiento de información sean subterráneas o tengan una protección alternativa.

- Garantizar que los cables de energía eléctrica estén separados de los cables de comunicaciones para evitar interferencia.

- Utilizar estándares para la identificación y etiquetado de cables y equipos con el fin de minimizar errores en la manipulación.

- Garantizar que los centros de cableado del centro de datos y las instalaciones del GECC estén protegidos con llave para evitar manipulación o acceso por parte de personal no autorizado.

5.8.3.2.4. Mantenimiento de equipos

Es responsabilidad de la Dirección de Gestión Integral de Instalaciones de CSA:

- Garantizar el mantenimiento preventivo del equipamiento (equipos de monitoreo, plantas eléctricas, plantas telefónicas, etc.) del **GECC** de acuerdo con los intervalos de servicio y especificaciones recomendadas por el proveedor, fabricante o distribuidor autorizado; con el fin de asegurar su disponibilidad e integridad.

- Mantener un inventario actualizado del equipamiento del **GECC** con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

- Garantizar que las tareas de mantenimiento y reparaciones de los equipos del GECC sean realizadas por personal autorizado y certificado por el fabricante.

- Llevar una bitácora de todas las fallas y mantenimientos preventivos y mantenimientos correctivos sobre el equipamiento.

- Implementar los controles adecuados para el mantenimiento y protección de la información confidencial, teniendo en cuenta si dicho mantenimiento es realizado localmente o fuera de las instalaciones del **GECC**.

5.8.3.2.5. Retiro de activos

Es responsabilidad de la Dirección de Servicios de TI CSA y el Propietario del Activo:

- Garantizar que los equipos (servidores, equipos de comunicaciones, equipos de cómputo, equipos de monitoreo, plantas eléctricas, plantas telefónicas, etc.), información y software del **GECC** no sea retirado de las instalaciones sin la autorización correspondiente, al igual que dejar un soporte de la persona que ejecuta la acción (identificación, empresa, rol, número de contacto, etc.).

5.8.3.2.6. Seguridad de equipos y activos fuera de las instalaciones

Es responsabilidad de la Dirección de Tecnología Informática CSA y la GCR:

- Definir e implementar los controles para garantizar un trabajo seguro desde la casa, teletrabajo y sitios temporales.

5.8.3.2.7. Disposición segura o reutilización de equipos

Es responsabilidad de líderes de proceso:

- Garantizar que los equipos de los colaboradores, proveedores y contratistas a su cargo sean entregados a la Unidad de Tecnología Informática de CSA para la ejecución de los procesos de borrado seguro o sanitización antes de ser reasignados a otros funcionarios o enviados a su disposición final.

Es responsabilidad de la Dirección de Tecnología Informática CSA:

- Garantizar que los equipos que contengan medios de almacenamiento pasen por un proceso de borrado seguro o sanitización para asegurar que la información corporativa o software licenciado sea eliminado o sobrescrito antes de su disposición final o reúso.

- Garantizar que los medios de almacenamiento que contengan información confidencial, de uso interno o protegida por derechos de autor sean destruidos físicamente, o se ejecuten procesos de borrado seguro sobre la información (sanitización).

- Disponer las herramientas tecnológicas que permitan ejecutar procesos de borrado seguro o sanitización sobre los equipos de los colaboradores, proveedores y contratistas del GECC.

- Garantizar que los equipos dañados que tengan medios de almacenamiento, pasen por un proceso de valoración de riesgos que determine si el medio debe destruirse físicamente o enviarlos a reparar sin riesgo de compromiso de la información.

- Garantizar el cifrado de disco de los equipos (Estaciones de trabajo con información confidencial o de uso interno y equipos portátiles en general) a través de la solución Endpoint definida por el **GECC**; con el fin de reducir el riesgo de divulgación de información confidencial. Las llaves criptográficas utilizadas dentro del proceso de cifrado deberán ser lo suficientemente largas para evitar ataques de fuerza bruta y mantenerse confidenciales.

5.8.3.2.8. Equipos de usuario desatendidos

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar la definición e implementación de controles de seguridad que garanticen el bloqueo automático de los computadores y dispositivos móviles cuando estos permanecen desatendidos y se active un protector de pantalla protegido con contraseña, después de tres (3) minutos de inactividad.

Es responsabilidad de los colaboradores, contratistas y proveedores del GECC:

- Garantizar el cierre de las sesiones de aplicación y servicios de red cuando ya no sean requeridos.

- Utilizar guayas de seguridad para la protección de los equipos portátiles del GECC cuando permanezcan desatendidos.

- Garantizar el bloqueo de los equipos que se encuentren conectados a la red corporativa cuando deje desatendido el equipo.

Es responsabilidad de la Gerencia Corporativa de Riesgo:

- Desarrollar procesos de capacitación y sensibilización en seguridad de la información para evitar que los equipos permanezcan desatendidos sin controles de seguridad y mitigar riesgos relacionados con la fuga de información.

5.8.3.2.9. Política de escritorio limpio y pantalla limpia

Es responsabilidad de los colaboradores, contratistas y proveedores del GECC:

- Garantizar que no se publique o se deje a la vista información sensible de acceso a los diferentes sistemas, como por ejemplo contraseñas, direcciones IP, contratos, números de cuenta, listados de clientes, datos de empleados y todo aquello que no se desea publicar.

- Garantizar que la información confidencial o de uso interno (papeles, medios de almacenamiento electrónico, etc.) permanezca guardada cuando no se requiera (caja fuerte o gabinete con llave); y especialmente cuando la oficina se encuentre desocupada.

- Garantizar que la información confidencial o de uso interno se retire de manera inmediata de los equipos multifuncionales.

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar el aseguramiento de equipos multifuncionales (escáner, fax, impresora, copiadora) utilizados por colaboradores, contratistas y proveedores del GECC. De igual forma, se debe garantizar el borrado de la información que permanece en memoria dentro de los dispositivos multifuncionales, tan pronto finalice el proceso.

5.9. Seguridad de las operaciones

5.9.1. Objetivo

Definir las reglas y requerimientos que deben cumplir los dirigentes, administradores, colaboradores, proveedores y contratistas del **GECC** para poder garantizar el funcionamiento adecuado, correcto y seguro de las instalaciones de procesamiento de la información y las comunicaciones del **GECC**. Estas reglas y requerimientos están definidos con el fin de proteger la confidencialidad, integridad y disponibilidad de la información que se maneja en las instalaciones de procesamiento y también poder asegurar que los cambios que se efectúen sobre los recursos tecnológicos, sean controlados de forma adecuada y debidamente autorizados.

5.9.2. Alcance

Estas políticas y responsabilidades aplican para todos los dirigentes, administradores, colaboradores, proveedores y contratistas del GECC que hagan uso de cualquier instalación de procesamiento y transmisión de información del GECC.

5.9.3. Políticas y responsabilidades

5.9.3.1. Procedimientos operacionales y responsabilidades

5.9.3.1.1. Procedimientos de operación documentados

- **Es responsabilidad de la Dirección de Servicios de TI CSA**, garantizar que se definan, comuniquen y mantengan actualizados los procedimientos operativos asociados con las instalaciones de procesamiento y comunicación del GECC, los cambios de estos procedimientos solo serán autorizados por esta dirección.

5.9.3.1.2. Gestión de cambios

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos para el control de los cambios en el ambiente productivo y de comunicaciones del **GECC.** Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad por parte del Comité de Control de Cambios definido al interior, a menos que se considere un cambio estándar.

- Asegurar que se conserve un registro de auditoría que contenga toda la información relevante de cada cambio implementado (Herramienta de Control de Cambios definida por la Organización).

- Asegurar que los cambios que se lleven a cabo sean evaluados y probados de forma integral y que se cuente con la participación de los líderes de los procesos usuarios, a fin de revisar y garantizar la funcionalidad de los cambios realizados en los diferentes componentes de la solución.

5.9.3.1.3. Gestión de la capacidad

- **Es responsabilidad de la Dirección de Servicios de TI CSA**, garantizar que se definan, comuniquen y mantengan actualizados los procedimientos asociados con la gestión de la capacidad de la demanda de los sistemas en operación, de los recursos humanos, oficinas e instalaciones y la proyección de futuras demandas, con el fin de garantizar un procesamiento y almacenamiento adecuado e ininterrumpido.

- Generar ajustes, mejoras, mantenimientos y/o planes de acción, resultado del monitoreo y gestión de la capacidad, que permitan garantizar la continuidad en la prestación del servicio de la organización y minimizar la posibilidad de ocurrencia de eventos de no disponibilidad.

5.9.3.1.4. Separación de los ambientes de desarrollo, pruebas y producción

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar que exista una separación física y lógica de los ambientes de desarrollo, pruebas y producción; con el fin de reducir los riesgos de cambio accidental o acceso no autorizado al software operacional y a la información clasificada como confidencial o de uso interno.

- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos asociados con la transferencia de software del estatus de desarrollo al de producción.

- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos que aseguren que los cambios en los sistemas de producción y aplicaciones se han puesto en prueba, en un ambiente de pruebas antes de aplicarlos en el ambiente de producción.

- Garantizar que se impida el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente de producción, cuando no sean indispensables para el funcionamiento del mismo.

- Garantizar que los usuarios usen diferentes perfiles en los sistemas de producción y de pruebas, y los menús deberían mostrar mensajes de identificación apropiado con el fin reducir el riesgo de error.

- Garantizar que los datos clasificados como confidenciales no sean copiados en el ambiente de pruebas o desarrollo sin el proceso de transformación o enmascaramiento correspondiente con el fin de reducir el acceso no autorizado o robo de esta información. Para esto, las empresas harán uso de las herramientas tecnológicas definidas a nivel corporativo para tal fin.

5.9.3.2. Protección contra códigos maliciosos

5.9.3.2.1. Controles contra códigos maliciosos

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar que todos los dispositivos móviles y de escritorio sólo cuenten con software autorizado por la organización.

- Garantizar la prohibición y detección del uso de sitios web maliciosos o que se sospecha lo son.

- Evitar la descarga de archivos y software desde o a través de redes externas, o por cualquier otro medio.

- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos que ayuden a reducir las vulnerabilidades de las cuales pueda aprovecharse el software malicioso.

- Garantizar que se realiza una revisión periódica del contenido de software y datos de los equipos que apoyan los procesos críticos del **GECC**, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.

- Garantizar que se realice de forma continua un análisis de los computadores y medios del GECC, con el fin de protegerlos contra código malicioso. El análisis debe incluir cualquier archivo recibido por la red o cualquier medio de almacenamiento antes de su uso, el análisis

de los adjuntos y descargas de los correos electrónicos antes de su uso y el análisis de páginas web.

Es responsabilidad de la Dirección de Servicios de TI CSA y la Gerencia Corporativa de Riesgo o quien haga sus veces en el GECC, garantizar la instalación y actualización regular del software de detección y reparación del software malicioso en los equipos portátiles, de escritorio y de procesamiento.

Es responsabilidad de la Gerencia Corporativa de Riesgo, generar campañas periódicas de capacitación y sensibilización en seguridad de la información, con el fin de dar a conocer las precauciones apropiadas acerca de los peligros y amenazas de los códigos maliciosos y de los controles con los que cuenta la organización para mitigar los riesgos de los mismos.

5.9.3.3. Copias de respaldo

5.9.3.3.1. Respaldo de la información

Es responsabilidad de la Dirección de Servicios de TI CSA, la Gerencia Corporativa de Riesgo o quien haga sus veces en el GECC y los propietarios de la información, determinar los requisitos para copias de respaldo de la información y los sistemas en función de su criticidad y clasificación. Con base a ello, se definirá y documentará un esquema de retención y protección.

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Asegurar que se cuenta con las instalaciones adecuadas para el almacenamiento de las copias de respaldo, con el fin de asegurar que la información y los sistemas se puedan recuperar después de un desastre o falla del medio.

- Asegurar que las copias de respaldo se almacenen en una ubicación remota a los sitios de procesamiento principal, con el fin de poder escapar de cualquier daño que pueda ocurrir en el sitio principal.

- Asegurar que se implementa una protección por medio de cifrado, haciendo uso de los algoritmos definidos por el GECC, para los repositorios donde se almacene información clasificada como confidencial o de uso interno.

- Definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información y los sistemas que son almacenadas externamente, con el fin de evitar la pérdida de su integridad y confidencialidad.

- Realizar ejercicios periódicos de restauración de copias de respaldo en ambientes controlados, de tal forma que permitan garantizar la disponibilidad de los medios de respaldo y de la información contenida en ellos, y minimizar la posibilidad de falla cuando se requiera realizar una restauración de dicha información.

Es responsabilidad de los propietarios de la información, definir la información a ser respaldada, los periodos de rotación, frecuencia de las copias de respaldo con el objeto de garantizar el normal desarrollo de los procesos, la continuidad de negocio, la consulta histórica de la misma y el cumplimiento de la legislación.

5.9.3.4. Registro (logging) y seguimiento

5.9.3.4.1. Registro de eventos

Es responsabilidad de la Dirección de Servicios de TI CSA, la Gerencia Corporativa de Riesgo o quien haga sus veces en el GECC y los propietarios de la información

- Determinar los eventos que generarán un registro de auditoria de los sistemas y equipos del **GECC**.

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Asegurar la integridad, confidencialidad y disponibilidad de los registros de auditoria de los sistemas y equipos del GECC.

- Conservar y revisar regularmente los registros (Logs) acerca de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

5.9.3.4.2. Protección de la información de registro

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Asegurar que en donde sea posible, los administradores de sistemas no tengan permiso para borrar o desactivar registros de auditoria de sus propias actividades.

- Asegurar que los registros de auditoria serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de retención de registros.

5.9.3.4.3. Registros del administrador y del operador

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Asegurar el registro de las actividades realizadas por los operadores y administradores de los sistemas del GECC.

Es responsabilidad de la Auditoría Corporativa o quien sea designado por el Comité Técnico Corporativo de Seguridad de la Información:

- Contrastar los rastros de las actividades realizadas por los operadores y administradores en relación con los procedimientos descriptivos de sus labores.

5.9.3.4.4. Sincronización de relojes

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar que se defina, comunique y mantenga actualizado el procedimiento que asegure el ajuste de relojes de los equipos, el cual contemplará la verificación de estos contra el Instituto Nacional de Metrología; estableciendo los correctivos ante cualquier variación significativa, con el fin de evitar que los registros de auditoria que puedan ser necesarios para investigaciones, sean inexactos y puedan dificultar estas investigaciones y afectar la credibilidad de la evidencia.

5.9.3.5. Control de software operacional

5.9.3.5.1. Instalación de software en sistemas operativos

Es responsabilidad de la Dirección de Servicios de TI CSA garantizar:

- Que se defina, comunique y mantenga actualizado el procedimiento que asegure el control sobre la instalación de actualizaciones en sistemas operativos.

- Que los sistemas operativos sólo contengan códigos ejecutables aprobados y no el código de desarrollo o compiladores.

- Antes que cualquier sistema operativo sea puesto en operación en la organización, se debe aplicar las líneas base de seguridad.

- Que se defina, comunique y mantenga actualizado el procedimiento con el cual se lleve un control de la configuración, con el fin de mantener un control de todo el software implementado, al igual que la del sistema operativo.

5.9.3.6. Gestión de la vulnerabilidad técnica

5.9.3.6.1. Gestión de las vulnerabilidades técnicas

Es responsabilidad de la Dirección de Servicios de TI CSA y de los líderes de los procesos:

- Mantener un inventario actualizado y completo de los activos de información.

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Garantizar que se defina, comunique y mantenga actualizado el procedimiento que asegure una gestión eficaz para las vulnerabilidades técnicas que sean identificadas.

- Garantizar que sólo se utilice un hardware de propósito específico homologado por el Common Vulnerabilities and Exposures (CVE) para realizar las evaluaciones de vulnerabilidad sobre los activos críticos del GECC.

- Garantizar que se realice un escaneo semanal a todos los activos definidos como críticos haciendo uso del hardware de propósito específico definido por el GECC para este propósito.

- Presentar un informe periódico sobre el estado de las vulnerabilidades para los activos críticos definidos por las empresas del GECC.

- Garantizar que los indicadores de riesgo de los activos críticos, se mantengan en el nivel definido por el Comité Técnico Corporativo de Seguridad de la Información.

- Gestionar que el cierre o mitigación de las vulnerabilidades se realice en los tiempos definidos por el Comité Técnico Corporativo de Seguridad de la Información.

- Garantizar que las labores de tratamiento de las vulnerabilidades deben gestarse en coherencia con los procedimientos definidos para el control de los cambios.

Es responsabilidad de la Gerencia Corporativa de Riesgo o quien haga sus veces en el GECC:
- Realizar una revisión periódica (mensual) sobre la gestión de vulnerabilidades.

5.9.3.6.2. Restricciones sobre la instalación de software

Es responsabilidad de la Dirección de Servicios de TI CSA:
- Garantizar la implementación de controles técnicos que impidan la instalación de software por parte de los colaboradores, proveedores y contratistas sobre sus estaciones de trabajo, a través de las soluciones de seguridad adquiridas por el GECC.

5.9.3.7. Consideraciones sobre auditorías de sistemas de información

5.9.3.7.1. Controles sobre auditorías de sistemas de información

Es responsabilidad de la Auditoría Corporativa:
- Acordar con la Dirección de Servicios de TI CSA los requisitos de auditoria para acceso a los sistemas y a los datos.

- Acordar con la Dirección de Servicios de TI CSA el alcance de las pruebas técnicas de auditoria, y estas deben ser ejecutadas por la Dirección de Servicios de TI CSA.

Es responsabilidad de la Dirección de Servicios de TI CSA:
- Garantizar que las pruebas de auditoria se limiten a acceso de software y datos únicamente para lectura.

- Garantizar que las pruebas de auditoria que puedan afectar la disponibilidad del sistema sean realizadas fuera de horas laborales.

5.10. Seguridad de las comunicaciones

5.10.1. Objetivo

Definir los responsables de desarrollar los procedimientos e implementar los controles que eviten los daños e interferencias a la información del **GECC**, las instalaciones de procesamiento de la información y ayuden a mantener la seguridad de la información que transfiere el **GECC** internamente o con entidades externas.

5.10.2. Alcance

Estas políticas y responsabilidades aplican para todos los dirigentes, administradores, colaboradores, proveedores y contratistas del GECC, que transfieran información al interior del GECC o contra entidades externas.

5.10.3. Políticas y responsabilidades

5.10.3.1. Gestión de la seguridad de las redes

5.10.3.1.1. Controles de redes

Es responsabilidad de la Dirección de Servicios de TI CSA y el proveedor de TI:

- Establecer las responsabilidades y procedimientos para la gestión de equipos de redes.
- Garantizar que la responsabilidad operacional de las redes esté separada de las operaciones de computo.
- Garantizar la implementación de controles para asegurar la confidencialidad e integridad de la información corporativa que viaja sobre redes públicas o inalámbricas, para proteger los sistemas y aplicaciones conectados.
- Garantizar que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos.
- Garantizar el cumplimiento del control de los accesos de los usuarios a los servicios de información.

5.10.3.1.2. Seguridad de los servicios de red

Es responsabilidad de la Dirección de Servicios de TI CSA y el proveedor de TI:

- Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
- Establecer una línea base de configuración de los dispositivos de seguridad y de red que hacen parte de la plataforma tecnológica del GECC, acogiendo buenas prácticas de configuración segura.

- Establecer los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red.

- Garantizar que se defina, comunique y mantenga actualizado el procedimiento para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.

5.10.3.1.3. Separación en las redes

- Garantizar la segmentación de las redes en función de los grupos de servicios, usuarios y sistemas de información.

5.10.3.2. Transferencia de información

5.10.3.2.1. Políticas y procedimientos de transferencia de información

Es responsabilidad de la Dirección de Servicios de TI CSA y el proveedor de TI:

- Garantizar que se defina, comunique y mantenga actualizado los procedimientos para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción.

- Garantizar que se defina, comunique y mantenga actualizado los controles para la detección de software malicioso y protección contra éste, que pueda ser transmitido mediante el uso de comunicaciones electrónicas.

- Hacer gestión para que se utilicen las técnicas de cifrado adecuadas para proteger la confidencialidad, integridad y autenticidad de la información.

- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos para evitar que se tenga acceso no autorizado a los mensajes almacenados en equipos multifuncionales y teléfonos IP que estén bajo su gestión.

- Garantizar que se definan, comuniquen y mantengan actualizados los procedimientos para evitar que se logren programar las máquinas o servicios de fax de forma deliberada o accidental para enviar mensajes a números específicos.

Es responsabilidad de la Gerencia Corporativa de Riesgo:

- Generar campañas periódicas de capacitación y sensibilización en seguridad de la información, con el fin de dar a conocer las precauciones apropiadas acerca de no revelar información confidencial o de uso interno por cualquier medio de comunicación.

- Generar campañas periódicas de capacitación y sensibilización en seguridad de la información, con el fin de dar a conocer las precauciones apropiadas acerca de no tener

conversaciones confidenciales en lugares públicos, o mediante canales de comunicación no seguros, oficinas abiertas y lugares de reunión.

- Generar campañas periódicas de capacitación y sensibilización en seguridad de la información, con el fin de dar a conocer las precauciones apropiadas acerca de no dejar información expuesta en dispositivos de impresión, reproducción, copiado, escaneo, duplicado, facsímil, contestadores telefónicos automáticos u otros.

- **Es responsabilidad de los colaboradores y contratistas del GECC,** asegurar que no se deja ningún tipo de mensaje que contenga información confidencial o de uso interno, en las máquinas contestadoras, debido a que estos mensajes pueden ser escuchados por personas no autorizadas.

5.10.3.2.2. Acuerdos sobre transferencia de información

Es responsabilidad de la Gerencia Corporativa de Riesgo:

- Definir cómo se debe realizar el intercambio de información con terceros, según los acuerdos de intercambio y cumplir con la legislación correspondiente, con el fin de proteger la integridad y confidencialidad de la información.

- Definir y revisar los acuerdos de confidencialidad e intercambio de información que se puedan dar entre el **GECC** y terceros.

- Realizar la autorización para el establecimiento de un vínculo de transmisión de información con terceros.

- **Es responsabilidad de los colaboradores y contratistas del GECC,** que la información confidencial o de uso interno que se envíe por cualquier medio digital (correo electrónico, DVD, CD, USB, entre otros) debe estar cifrada de acuerdo a los mecanismos que defina el GECC, así mismo la que se envíe en documento físico debe ir en sobre cerrado.

5.10.3.2.3. Mensajería electrónica

Es responsabilidad de la Dirección de Servicios de TI CSA, garantizar que se definan, comuniquen y mantengan actualizados los procedimientos que garanticen la protección adecuada de la información incluida en la mensajería electrónica (correo electrónico, intercambio electrónico de datos y redes sociales).

Es responsabilidad de los colaboradores y contratistas del GECC:

- Que los mensajes de correo electrónico y cualquier otro tipo de comunicación enviada o recibida a través de los sistemas informáticos de la organización no deben utilizarse para crear, almacenar ni transmitir información de carácter hostil, malicioso, ilegal, obscena, discriminatoria, vulgar, ofensiva, despectiva o de índole acosadora. Dichos sistemas tampoco

deben utilizarse para acceder en forma intencional a sitios web cuyo contenido sea ilegal, indecente o discriminatorio.

- No emplear direcciones de correo electrónico diferentes a las cuentas corporativas para atender asuntos de la empresa.

5.10.3.2.4. Acuerdos de confidencialidad o de no divulgación

Es responsabilidad de las áreas de Contratación del GECC garantizar:

- Que en los contratos que se realicen con terceros se establezcan los acuerdos de confidencialidad o no divulgación necesarios con el fin de proteger la información del GECC.

- Que en los acuerdos de confidencialidad o no divulgación se definan las responsabilidades legales asignadas a los firmantes por la divulgación no autorizada o uso incorrecto de información del GECC.

- Que los acuerdos de confidencialidad o no divulgación se revisen de forma periódica, y cuando ocurran cambios que influyan en estos acuerdos.

5.11. Adquisición, desarrollo y mantenimiento de sistemas

5.11.1. Objetivo

Asegurar que durante todo el ciclo de vida de desarrollo de los sistemas de información se incluyan los requerimientos de seguridad de la información con el fin de lograr sistemas de información más seguros y capaces de resistir ataques.

5.11.2. Alcance

Estas políticas y responsabilidades aplican frente a todos los sistemas informáticos, tanto desarrollos propios o de terceros, como a todos los sistemas operativos y/o software de base que integren cualquiera de los ambientes administrados por el GECC.

5.11.3. Políticas y responsabilidades

5.11.3.1. Requisitos de seguridad de los sistemas de información

5.11.3.1.1. Análisis y especificación de requisitos de seguridad de la información

Es responsabilidad de la Dirección de Servicios de TI CSA y el proveedor de TI:

- Garantizar que los desarrollos y mejoras sobre los sistemas de información a cargo de la Unidad de Tecnología Informática de CSA apliquen metodologías de desarrollo seguro durante todo el ciclo de vida (Análisis, Diseño, Codificación, Pruebas, Implementación y Mantenimiento), que permitan garantizar aplicaciones de calidad desde el propio inicio del

proyecto, contemplando los servicios de seguridad como confidencialidad, integridad y disponibilidad.

- Asegurar que se realicen las actividades de identificación de requerimientos de seguridad de la información, teniendo en cuenta las políticas de seguridad de la información, estándares, regulaciones y aspectos legales. Estos requisitos de seguridad de la información deben ser justificados, aceptados y documentados, por las áreas de Procesos, Gerencia Corporativa de Riesgo y Auditoria Corporativa.

- Asegurar que durante la fase de diseño se tengan presentes los requerimientos de seguridad de la información para la construcción de los controles de seguridad, tales como: controles de acceso, opciones de cifrado, aspectos de continuidad de negocio, registros de auditoría, etc.

- Asegurar que las aplicaciones desarrolladas cuenten con una matriz de roles al momento de su entrega, con el objetivo de facilitar el levantamiento de la matriz de perfiles por cargo.

- Disponer las herramientas tecnológicas que permitan detectar fallas de seguridad en el código fuente de las aplicaciones desarrolladas al interior o por parte de terceros.

- Garantizar que, durante la fase de pruebas de los nuevos sistemas de información o mejoras realizadas sobre estos, sean expuestos a procesos de análisis de penetración o escaneo de vulnerabilidades antes de salir a producción.

- Considerar antes de la adquisición de cualquier sistema de información, el riesgo introducido y los controles asociados a los sistemas que no cumplan con los requisitos de seguridad de la información.

5.11.3.1.2. Seguridad de servicios de las aplicaciones en redes públicas

- **Es responsabilidad de la Dirección de Servicios de TI CSA y de la Gerencia Corporativa de Riesgo**, garantizar que la información involucrada en los servicios de aplicaciones que viaja a través de redes públicas se debe proteger de actividades fraudulentas.

5.11.3.1.3. Protección de transacciones de los servicios de las aplicaciones

- **Es responsabilidad de la Dirección de Servicios de TI CSA**, hacer gestión para proteger la información involucrada en las transacciones de los servicios de las aplicaciones para evitar alteraciones en la información o divulgación no autorizada.

- **El propietario del activo de información** debe asegurar que las partes involucradas en las transacciones sobre redes públicas hagan uso de mecanismos de seguridad que garanticen la autenticidad, integridad, confidencialidad y no repudio como firmas o certificados digitales.

5.11.3.2. Seguridad en los procesos de desarrollo y de soporte

5.11.3.2.1. Políticas de desarrollo seguro

- **Es responsabilidad de la Dirección de Servicios de TI CSA**, y el proveedor adoptar procedimientos de desarrollo seguro de software o de sistemas, para los desarrollos que se realicen al interior de la organización.

5.11.3.2.2. Procedimientos de control de cambios en sistemas

- **Es responsabilidad de la Dirección de Servicios de TI CSA**, garantizar que se definan, comuniquen, apliquen y mantengan actualizados los procedimientos para el control de los cambios durante el ciclo de vida de desarrollo de software o de sistemas.

5.11.3.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

Es responsabilidad de la Dirección de Servicios de TI CSA y el proveedor de TI:

- Garantizar que cada vez que se realice un cambio en la plataforma de operación (sistema operativo, bases de datos o software de capa media) se revisen los sistemas del GECC para evitar que se produzca un impacto en su funcionamiento y en la seguridad.

- Garantizar que durante la revisión técnica de las aplicaciones se tenga presente las siguientes consideraciones:

  - Revisar los procedimientos de integridad y control de aplicativos para garantizar que no hayan sido comprometidos por el cambio.
  - Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación
  - Asegurar la actualización del plan de continuidad de las actividades del GECC.

5.11.3.2.4. Restricciones en los cambios a los paquetes de software

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Asegurar que cualquier modificación de paquetes de software suministrados por proveedores al GECC considere los siguientes lineamientos:
- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- Determinar la conveniencia de que la modificación sea efectuada internamente, por el proveedor o por un tercero calificado.
- Evaluar el impacto que se produce si la organización se hace cargo del mantenimiento de la aplicación por los cambios efectuados.
- Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

5.11.3.2.5. Principios de construcción de sistemas seguros

Es responsabilidad de la Dirección de Servicios de TI CSA y fábricas de software: y proveedores

- Ejecutar procesos de análisis de riesgos durante la fase de construcción.

- Incluir la seguridad en el diseño de todas las capas de arquitectura (negocio, datos, aplicaciones y tecnología), con el fin de equilibrar la necesidad de seguridad de la información con la necesidad de accesibilidad.

- Realizar una revisión del diseño de la aplicación y problemas relacionados a la arquitectura, para detectar problemas de manera temprana en el proceso de desarrollo de la aplicación, antes de que sea liberada.

- Garantizar la revisión o verificación del código fuente de la aplicación para detectar huecos de seguridad.

- Aplicar metodologías para el desarrollo de aplicaciones seguras y capaces de resistir ataques.

5.11.3.2.6. Ambiente de desarrollo seguro

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Establecer ambientes de desarrollo seguros para las labores de desarrollo de sistemas específicos, considerando:

    - Los controles de seguridad ya implementados por la organización, que brindan soporte al desarrollo del sistema;
    - La sensibilidad de los datos a procesar, almacenar y trasmitir.
    - El control de acceso al ambiente de desarrollo.
    - El control sobre el movimiento de datos desde y hacia el ambiente de desarrollo.

- Una vez se determine el nivel de protección para un ambiente de desarrollo, debe documentar los procesos correspondientes en procedimientos de desarrollo seguro y suministrarlos a todos los individuos que los necesiten.

5.11.3.2.7. Desarrollo contratado externamente

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Supervisar y realizar seguimiento a la actividad de desarrollo de los sistemas de información contratados externamente.

- Considerar los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.

- Garantizar que las fábricas de software cumplan con los principios de construcción de sistemas seguros, al igual que los definidos por la organización.

- Velar por el cumplimiento de las leyes que apliquen a las diferentes soluciones de sistemas de información en la organización aun cuando sean desarrollados por entes externos.

Es responsabilidad de las áreas de contratación de las empresas del GECC:

- Definir acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.

- Incluir contractualmente las pólizas de cumplimiento y calidad del trabajo realizado.

- Incluir derechos contractuales para auditar la calidad y exactitud del trabajo realizado.

- Definir requisitos contractuales sobre la calidad, seguridad y funcionalidad del código.

- Incluir dentro de los contratos con terceros que estos deben cumplir con las políticas de seguridad de la información.

- Siempre que se contrate un externo para el desarrollo de software se debe exigir lo siguiente:

    - **Firmas de acuerdos de confidencialidad**. Con esto se previene al tercero divulgar información crítica de la Empresa.
    - **Certificación de Seguridad en el Proceso de Desarrollo**. El tercero debe garantizar que su proceso de desarrollo recoge las mejores prácticas para el desarrollo seguro de aplicaciones.
    - **Contratos de Entrega de Producto**. En estos contratos se garantiza la aceptabilidad del producto final. Se debe incluir que los criterios de aceptación incluyen las pruebas funcionales, las pruebas de seguridad (casos de abuso y test de intrusión). Dichas pruebas deben ser exitosas y se deben hacer las correcciones pertinentes respecto a cualquier hallazgo encontrado.
    - **Inclusión de los Requerimientos de Seguridad**. Los terceros deben entregar un producto que cumpla con el numeral de “Requisitos de seguridad de los sistemas de información” del presente documento.
    - **Certificación Libre de Malware**. El proveedor debe certificar que el producto entregado se encuentra libre de malware, troyanos o puertas traseras que pueden poner en peligro la seguridad del sistema de información.
    - **Auditorias**. El proveedor debe permitir procesos de auditorías por la organización. Este tipo de auditoría debe estar orientada a la verificación del proceso de desarrollo del proveedor y que cumpla la definición de requerimientos de seguridad de la aplicación y que se ejecute las pruebas de seguridad.

5.11.3.2.8. Pruebas de seguridad de sistemas

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Desarrollar un programa de pruebas de seguridad efectivo que cuente con componentes que comprueben: las personas (para asegurarse de que se tiene la educación y concientización adecuadas), los procesos (para asegurarse que existen las políticas y estándares adecuados, y que las personas saben cómo seguir dichas políticas), la tecnología (para asegurarse de que el proceso ha sido efectivo en su implementación) y de esta manera poder prever incidentes o problemas que más tarde se pueden manifestar en forma de defectos en la tecnología; y así erradicar bugs de forma temprana e identificar las causas de los defectos.

- Realizar pruebas de seguridad sobre las aplicaciones nuevas en las fases de Análisis, Diseño, Codificación, Pruebas, Implementación y Mantenimiento para descubrir vulnerabilidades y establecer un estándar mínimo para la liberación de la aplicación.

- Realizar pruebas de vulnerabilidad a las aplicaciones críticas de la organización cada mes con el fin de poder generar planes de acción para mitigar las vulnerabilidades detectadas. Cuando se realicen cambios en los sistemas, deberá realizarse una prueba adicional.

- Producir un registro formal de que comprobaciones se han realizado, y los detalles de los hallazgos. El reporte debe ser claro para los líderes de proceso o propietarios de la información, desarrolladores y personal de seguridad de la información.

5.11.3.2.9. Prueba de aceptación de sistemas

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Definir los criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Estas pruebas deben incluir las pruebas de requisitos de seguridad de la información y la adherencia a prácticas de desarrollo seguro.

- Asegurar que se cuente con ambientes de pruebas iguales a los ambientes de producción para evitar que se introduzcan vulnerabilidades al ambiente de producción.

Es responsabilidad de los colaboradores y contratistas del GECC, participar y mantener la seguridad de la información en las pruebas y usuarios de pruebas para nuevos sistemas de información, actualizaciones y nuevas versiones, antes de su aprobación definitiva.

5.11.3.3. Datos de prueba

5.11.3.3.1. Protección de datos de prueba

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Llevar un registro de autorización formal otorgada por el propietario de la información para realizar copias de la información operativa a los ambientes de prueba.

- Alterar (ofuscamiento) los datos de pruebas de producción cuando sea necesario utilizarlos, de tal forma que no se pueda realizar una asociación entre la información de pruebas y producción.

- Hacer gestión para evitar el uso de datos operacionales que contengan información de datos personales o confidenciales para efectos de pruebas.

- Eliminar a la mayor brevedad y una vez completadas las pruebas, la información operativa utilizada.

5.12. Relaciones con los proveedores

5.12.1. Objetivos

Definir lineamientos que garanticen la protección de los activos de información a los cuales tienen acceso proveedores y contratistas del **GECC** y asegurar el cumplimiento de los acuerdos de seguridad de la información establecidos con los proveedores del **GECC.**

5.12.2. Alcance

Estas políticas y responsabilidades se aplican a todos los proveedores y contratistas que establezcan una relación contractual con el **GECC** y que para la prestación de sus servicios accedan a los activos de información propiedad del **GECC.**

5.12.3. Políticas y responsabilidades

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

Es responsabilidad de la Dirección de Negociación y Compras de CSA:

- Asegurar que todos los proveedores con los cuales se establecerá relación, conozcan y acepten las políticas, normas y procedimientos de seguridad y privacidad de la información establecidos por el GECC.

- Mantener y suministrar a la Gerencia Corporativa de Riesgo, una base de datos actualizada de los proveedores que tienen relación con el GECC y los tipos de productos y servicios ofrecidos.

- Definir un proceso y ciclo de vida para la gestión de las relaciones con los proveedores.

- Incluir dentro de todos los términos de referencia que se publiquen para adquisición de bienes y servicios de tecnología de la información y de comunicaciones, los requisitos de seguridad y privacidad de la información establecidos por la Gerencia Corporativa de Riesgo.

- Obtener de los proveedores la autorización del tratamiento de datos personales.

- Definir las finalidades para las cuales permitirá el acceso de información del **GECC** al proveedor y responsabilidades para su tratamiento y uso.

Es responsabilidad de la Gerencia Corporativa de Riesgo y la Dirección de Negociación y Compras de CSA, garantizar que los proveedores extranjeros proporcionen los niveles adecuados de protección de datos personales.

- **Es responsabilidad de la Dirección de Servicios de TI CSA y la Gerencia Corporativa de Riesgo,** brindar apoyo a los líderes de proceso para la definición de los tipos y niveles de acceso a la información del GECC que será asignada a los proveedores.

- **Es responsabilidad de la Gerencia Corporativa de Riesgo en conjunto con los líderes de proceso,** definir los requisitos mínimos de seguridad y privacidad de la información para cada tipo de información y cada tipo de acceso permitido a los proveedores y contratistas del GECC.

- **Es responsabilidad de la Gerencia Corporativa Jurídica** o quien haga sus veces en el **GECC,** incluir dentro de los modelos de contratos y acuerdos con proveedores las obligaciones de seguridad y privacidad de la información definidas por la Gerencia Corporativa de Riesgo.

Es responsabilidad de la Gerencia Corporativa de Riesgo:

- Realizar el tratamiento a los incidentes de seguridad y privacidad de la información relacionados con el acceso de proveedores.

- Definir las responsabilidades tanto de la organización como de los proveedores y terceros, frente a los incidentes de seguridad y privacidad de la información.

- La capacitación y concientización del área de Negociación y Compras de CSA, frente a políticas, procesos y procedimientos de seguridad y privacidad de la información aplicables.

- La capacitación y toma de conciencia del personal interno que interactúa con proveedores, en cuanto al comportamiento e interacción adecuada con el proveedor de acuerdo al nivel de acceso que éste tiene a los sistemas e información del GECC.

- Acordar con los proveedores los procedimientos necesarios que garanticen la seguridad y privacidad de la información durante el periodo de transición (movimiento, traslado, eliminación) de los activos de información que así lo requieran.

- Brindar acompañamiento a la Gerencia Corporativa Jurídica o quien haga sus veces en el GECC para establecer y documentar acuerdos y responsabilidades de seguridad y privacidad de la información con los proveedores del **GECC** que tienen acceso, procesan, almacenan, comunican o suministran componentes que gestionan información del **GECC**.

- Definir los requisitos de seguridad y privacidad de la información para los proveedores de bienes y servicios de tecnología de la información y de comunicaciones del **GECC**.

Es responsabilidad de cada supervisor de contrato designado por el GECC:

- Garantizar que los proveedores de productos y servicios de tecnología de información y de comunicaciones verifiquen el cumplimiento de los requisitos y buenas prácticas de seguridad y privacidad de la información exigidos por el **GECC** a lo largo de toda su cadena de suministro, y personal subcontratado para la prestación de sus servicios a la organización.

- Establecer un proceso para identificación de componentes críticos de los productos y servicios, que podrían afectar su funcionalidad y a los cuales debe realizarse un mayor seguimiento especialmente en los casos que son subcontratados por el proveedor del **GECC**.

- Solicitar a los proveedores de productos de tecnología de información y comunicación, la implementación de procesos que garanticen la gestión del ciclo de vida de estos componentes y su disponibilidad.

- Solicitar a los proveedores de productos de tecnología de información y comunicación, la implementación de procesos para gestión de riesgos de seguridad y privacidad asociados a los componentes y al suministro de los mismos por parte de los proveedores involucrados.

- Controlar, definir y autorizar los accesos por parte de terceros a la red del **GECC** y a los diferentes sistemas de información.

Todos los contratistas y proveedores de las empresas y unidades del GECC deben:

- Firmar un acuerdo de confidencialidad que garantice el compromiso con el cumplimiento de las políticas de seguridad y privacidad de la información establecidas por el **GECC**.

- Cumplir con las políticas de seguridad y privacidad de la información y desempeñar un papel proactivo para la protección, atendiendo a los roles y responsabilidades establecidos para sus actividades empresariales y respondiendo en pro de las políticas que orientan la seguridad y privacidad de la información.

- Velar por el cumplimiento de sus responsabilidades frente la seguridad y privacidad de la Información, dentro del marco organizacional y normativo definido.

- Aportar al buen uso de los activos del **GECC**, para los fines adecuados y por las personas autorizadas.

- Mantener la confidencialidad respecto de toda la información a la que tengan acceso en el desempeño de sus funciones para el **GECC**, aunque ésta no haya sido clasificada.

5.12.3.2. Gestión de la prestación de servicios de proveedores

Es responsabilidad de cada supervisor de contrato designado por el GECC:

- Realizar seguimiento y velar por el cumplimiento de los acuerdos de servicio establecidos con los proveedores de servicios de tecnología de información, de comunicaciones y otros.

- Socializar y analizar con los proveedores, los informes de incidentes de seguridad y privacidad de la información suministrados por la Gerencia Corporativa de Riesgo.

- Solicitar y validar con los proveedores que corresponda, la información que soporte el cumplimiento de requisitos de seguridad y privacidad de información por parte de los proveedores con los cuales tercerizan sus servicios.

Es responsabilidad de la Gerencia Corporativa de Riesgo:

- Realizar seguimiento periódico a los informes de estado suministrados por los proveedores que administran las diferentes soluciones de seguridad informática del **GECC**.

- Suministrar de manera periódica al supervisor de contrato los informes de incidentes de seguridad y privacidad de la información relacionados con el proveedor a cargo.

- Garantizar el mantenimiento y mejora de políticas, controles y procedimientos de seguridad y privacidad de la información para proveedores del **GECC**.

Es responsabilidad de la Auditoria Corporativa:

- Auditar los procesos y prácticas de los proveedores, así como la adopción de los requisitos de seguridad y privacidad de la información establecidos por el **GECC** y realizar seguimiento a los hallazgos de auditoria en los procesos de los proveedores.

- Verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

- **Es responsabilidad de la Dirección de Servicios de TI CSA y la Dirección de Negociación y Compras de CSA,** establecer un proceso formal para la gestión de cambios en los acuerdos con los proveedores, cambios realizados por la organización y cambios en los servicios propuestos por los proveedores.

5.13. Gestión de Incidentes de seguridad de la información

5.13.1. Objetivo

Definir los lineamientos para la gestión eficaz de los eventos e incidentes de seguridad y privacidad de la información al interior del **GECC.**

5.13.2. Alcance

Estas políticas y responsabilidades aplican a todos los dirigentes, administradores, colaboradores, proveedores y contratistas del **GECC** que tienen la responsabilidad de identificar

y reportar los eventos e incidentes de seguridad y privacidad de la información que se presenten en el **GECC.**

5.13.3. Políticas y responsabilidades

5.13.3.1. Responsabilidades y procedimientos de la gestión de incidentes de seguridad y privacidad de la información

Es responsabilidad de la Gerencia Corporativa de Riesgo o quienes hagan sus veces en el GECC:

- Definir y comunicar los procedimientos que garanticen el reporte, detección, análisis, evaluación, respuesta y seguimiento de eventos e incidentes de seguridad y privacidad de la información reportados por los dirigentes, administradores, colaboradores, proveedores y contratistas de las empresas y unidades del GECC.

- Garantizar la alineación entre el procedimiento de gestión de incidentes de seguridad y privacidad de la información y procedimiento de gestión de incidentes de TI definido por la Dirección de Servicios de TI de CSA.

- Analizar, revisar y dar respuesta a los eventos e incidentes de seguridad y privacidad de la información reportados por los dirigentes, administradores, colaboradores, contratistas y proveedores del GECC; de manera rápida, eficaz y ordenada de los mismos.

- Definir y comunicar los procedimientos que garanticen el manejo de evidencia forense relacionada con los incidentes de seguridad de la información y protección de datos personales.

- Revisar y documentar las lecciones aprendidas de la gestión de incidentes de seguridad y privacidad de la información con el fin de reducir la probabilidad de incidentes futuros que tengan una causa u origen similar.

Es responsabilidad del Equipo de Seguridad de la Información de la GCR:

- Liderar los procesos de sensibilización de los usuarios (internos y externos) relacionados con la identificación y reporte de eventos de seguridad y privacidad de la información para las empresas que están bajo la supervisión de la **GCR**.
- Liderar y documentar las pruebas que se programen sobre el esquema de gestión de incidentes de seguridad y privacidad de la información definido por el GECC.

Es responsabilidad del Jefe Corporativo de Seguridad de la Información:

- Liderar el Equipo de Respuesta a Incidentes de Seguridad y Privacidad de la Información (ISIRT – Information Security Incidente Response Team) de las empresas que están bajo la supervisión de la **GCR**.
- Presentar ante el **COMITÉ TÉCNICO CORPORATIVO DE SEGURIDAD DE LA INFORMACIÓN**, los incidentes de seguridad y privacidad de la información, con el fin de

conocer las tendencias, categorías y tratamiento de los mismos, sin perjuicio de las líneas de reporte que formalmente se establezcan por parte de la **GCR**.
- Definir una lista de posibles proveedores de servicios especializados de consultoría y análisis forense digital.

Es responsabilidad del Equipo de Respuesta a Incidentes de Seguridad y Privacidad de la Información:
- Reunirse y definir acciones conjuntas que permitan llegar a una respuesta eficaz y oportuna cuando se presente un incidente que afecte de manera considerable los activos de información del GECC.
- Informar a los titulares de la información sobre la situación presentada y sus consecuencias cuando estén relacionadas con Protección de Datos Personales, a través de los canales definidos por la organización.

Es responsabilidad de la Gerencia Corporativa de Riesgo, la Gerencia Corporativa de Gestión Humana y las áreas que hagan sus veces en el GECC:
- Difundir y dar a conocer la política de gestión de incidentes de seguridad y privacidad de la información definida para los dirigentes, administradores, colaboradores, proveedores y contratistas del GECC.
- Proveer a dirigentes, administradores, colaboradores, proveedores y contratistas de una sensibilización que incluya la identificación y reporte de los eventos que afectan la seguridad y privacidad de la información.

5.13.3.2. Reporte de eventos y debilidades de seguridad y privacidad de la información

Es responsabilidad de los dirigentes, administradores, colaboradores, contratistas y proveedores de las empresas y unidades del GECC:
- Detectar y reportar a través de los medios establecidos por la organización los eventos e incidentes de seguridad y privacidad de la información que son ocasionados por accidentes, errores o actos maliciosos intencionados, robo, apropiación indebida, extorsión, fraude, espionaje o eventos ambientales; de tal forma que la Gerencia Corporativa de Riesgo o quienes hagan sus veces en el GECC gestionen de manera eficaz y oportuna la solución y respuesta de los mismos.
- Preservar la confidencialidad de la información relacionada con el manejo, investigación y seguimiento de los incidentes de seguridad y privacidad de la información.

Es responsabilidad de las áreas de Seguridad Física de la GCR o quien haga sus veces en el GECC, reportar al **Equipo de Seguridad de la Información de la GCR** o quien haga sus veces, todos los incidentes seguridad física reportados y relacionados con los equipos e infraestructura tecnológica que atenten contra la seguridad y privacidad de la información, con el fin de iniciar la gestión del incidente de manera conjunta tanto para la parte administrativa como para la de seguridad y privacidad de la información.

5.13.3.3. Evaluación de eventos de seguridad y privacidad de la información

Es responsabilidad del Equipo Seguridad de la Información de la GCR o quien haga sus veces en el GECC:

- Revisar y analizar los eventos reportados para las empresas que están bajo la supervisión de la GCR, con el fin de iniciar la gestión y categorización sobre aquellos que realmente puedan considerarse como un incidente de seguridad y privacidad de la información.
- Analizar los eventos reportados por los usuarios internos y externos del GECC, y definir si estos efectivamente representan un incidente de seguridad y privacidad de la información para el trámite correspondiente de los mismos. En caso de ser necesario, los Analistas de Seguridad de la Información validarán los incidentes reportados con el Jefe Corporativo o Coordinador de Seguridad de la Información para definir su categorización como incidente de seguridad y privacidad de la información.
- Documentar en forma detallada el incidente, con el fin dar respuesta al mismo. Cuando sea requerido, el Jefe Corporativo o Coordinador de Seguridad de la Información, apoyarán el proceso de documentación con el fin de agilizar el tratamiento del incidente registrado.
- Categorizar el incidente documentado para el manejo estadístico correspondiente.

5.13.3.4. Respuesta a incidentes de seguridad y privacidad de la información

Es responsabilidad del Equipo Seguridad de la Información de la GCR o quien haga sus veces en el GECC:

- Dar respuesta a los incidentes de seguridad y privacidad de la información dentro de los tiempos acordados según su la prioridad (Crítico – 2 horas, Moderado – 4 horas, Menor – 8 horas).
- Acordar con el usuario o área afectada el tiempo requerido para gestionar el incidente de seguridad y privacidad de la información; siempre y cuando éste no afecte la disponibilidad de los servicios tecnológicos corporativos.
- Garantizar la recuperación del negocio ante el incidente presentado.

- Reportar de forma inmediata a los titulares de la información (clientes, colaboradores, contratistas y proveedores) los incidentes presentados sobre sus datos personales, las consecuencias asociadas a los mismos y los mecanismos que podría adoptar para disminuir el daño potencial.
- Reportar de forma oportuna a la Superintendencia de Industria y Comercio (SIC) los incidentes presentados sobre los datos personales de los titulares de la información; los cuales deberán contener como mínimo la siguiente información: tipo de incidente, fecha y hora de ocurrencia, fecha y hora de descubrimiento, causa, tipo de datos personales comprometidos y cantidad de datos personales de los titulares afectados. El reporte descrito previamente debe ser realizado a través del aplicativo RNBD dispuesto por la SIC https://rnbd.sic.gov.co/sisi/login.
- Recolectar información del incidente para soportar el reporte correspondiente ante la SIC.

5.13.3.5. Aprendizaje obtenido de los incidentes de seguridad y privacidad de la información

Es responsabilidad del Equipo Seguridad de la Información de la GCR o quien haga sus veces en el GECC:

- Documentar las lecciones aprendidas resultantes del proceso de gestión de incidentes, con el objetivo de garantizar la base de conocimiento.
- Realizar como mínimo una (1) vez al año la revisión y mejora de los procesos de gestión de riesgos y gestión de incidentes de seguridad y privacidad de la información apoyados en las lecciones aprendidas que han sido documentadas.

5.13.3.6. Recolección de evidencia

Es responsabilidad del Equipo Seguridad de la Información de la GCR o quien haga sus veces en el GECC, cuando sea requerido, coordinará la contratación y realización de una Investigación Forense que permita identificar a detalle el origen, responsable y comportamiento del incidente. De igual forma, garantizará la cadena de custodia correspondiente en caso que el incidente tenga un tratamiento judicial.

5.14. Aspectos de seguridad de la información de la gestión de continuidad del negocio

5.14.1. Objetivo

Preservar los requisitos de seguridad de la información en los procesos de continuidad de negocio y recuperación de desastres durante todas las fases de planeación, respuesta y recuperación.

5.14.2. Alcance

Estas políticas y responsabilidades aplican para todos los procesos críticos del GECC, para los cuales se debe contar o estar en proceso de desarrollo los planes de continuidad de negocio y recuperación de desastres.

5.14.3. Políticas y responsabilidades

5.14.3.1. Continuidad de seguridad de la información

Es responsabilidad de los líderes de los procesos con el apoyo de la Gerencia Corporativa de Riesgo:

- Determinar los requisitos de seguridad de la información durante el desarrollo de los planes de continuidad de negocio y planes de recuperación de desastres.

- Establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

- Establecer, implementar y mantener controles de seguridad de la información alternos cuando los controles definidos en situación normal no garanticen la seguridad de la información en situaciones adversas.

- Desarrollar y aprobar los planes de respuesta y recuperación donde se detalle como la organización gestionará un evento perturbador y mantenga la seguridad de la información en un nivel aceptable con base en los objetivos definidos en la fase de planificación.

- Revisar los controles de continuidad de la seguridad de la información definidos e implementados, con el objetivo de corroborar que son válidos y eficaces durante situaciones adversas, se recomienda realizar estas pruebas junto con las pruebas de continuidad de negocio y recuperación de desastres.

- **Es responsabilidad de la Gerencia Corporativa de Riesgo y la Auditoría Corporativa,** revisar los controles de continuidad de la seguridad de la información definidos e implementados, con el objetivo de corroborar que son válidos y eficaces durante situaciones adversas a través de auditorías de sistemas.

5.14.3.2. Redundancias

- **Es responsabilidad de los líderes de los procesos o propietarios de la información,** contemplar soluciones de redundancia para los sistemas de apoyo a los procesos críticos con el fin de garantizar los requisitos de disponibilidad.

- **Es responsabilidad de la Dirección de Servicios de TI CSA** con la autorización de los líderes de proceso involucrados, realizar pruebas periódicas de los sistemas de información que cuenten con redundancia para asegurar que después de una falla, el paso de operación de un componente a otro funcione de manera correcta.

- Implementar mecanismos que permitan la continuidad de la operación en los centros de procesamiento de información del GECC ante eventos adversos, siempre conservando los niveles de seguridad de la información suficientes para el cumplimiento de la política de seguridad y privacidad de la información.

5.15. Cumplimiento

5.15.1. Objetivo

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad y privacidad de la información y de cualquier requisito de seguridad.

5.15.2. Alcance

Estas políticas y responsabilidades aplican a todos los dirigentes, administradores, colaboradores y contratistas del GECC que tienen la responsabilidad de garantizar el cumplimiento de las políticas, normas y procedimientos de seguridad y privacidad de la información.

5.15.3. Políticas y responsabilidades

5.15.3.1. Cumplimiento de requisitos legales y contractuales

Es responsabilidad de la Gerencia Corporativa de Riesgo o quien haga sus veces dentro de las empresas del GECC:

- Identificar los requisitos legales, estatutarios, reglamentarios y contractuales aplicables a las empresas y unidades del GECC en materia de seguridad y privacidad de la información con el fin de garantizar el cumplimiento de los mismos.

- Definir y comunicar los procedimientos que garanticen la privacidad de la información de los dirigentes, administradores, colaboradores, proveedores, contratistas y clientes de las empresas y unidades del GECC por parte de los responsables y encargados del tratamiento de datos personales de la organización.

- Definir e implementar una política de protección de datos personales corporativa que cumpla los requisitos legales.

- Definir e implementar un aviso de privacidad que comunique a los Titulares de los datos personales, las finalidades del tratamiento de acuerdo a los requisitos legales.

- Establecer las finalidades del tratamiento de los datos personales de los grupos de interés del GECC.

- Establecer y habilitar los medios para el ejercicio de los derechos de los Titulares de datos personales.

- Determinar los procedimientos necesarios para el tratamiento de los datos personales de categoría especial (datos sensibles y de menores de edad) que permitan garantizar su seguridad.

- **Es responsabilidad de la Gerencia Corporativa de Riesgo, la Gerencia Corporativa Jurídica o quien haga sus veces en el GECC,** definir y comunicar los procedimientos que garanticen el cumplimiento de los derechos de propiedad intelectual y el uso de software legal por parte de los colaboradores, proveedores y contratistas del GECC.

- **Es responsabilidad de la Dirección de Servicios de TI CSA,** garantizar la adquisición de software a través de proveedores autorizados para garantizar el respeto a los derechos de autor.

Es responsabilidad de la Gerencia Corporativa de Gestión Humana:

- Definir, comunicar y aplicar sanciones frente al incumplimiento de derechos de propiedad intelectual y uso de software legal por parte de los colaboradores y contratistas de las empresas y unidades del GECC.

- Definir, comunicar y aplicar sanciones a los colaboradores y contratistas frente al incumplimiento de los procedimientos que garantizan la protección de datos personales al interior de la organización.

Es responsabilidad de la Dirección de Servicios de TI CSA:

- Definir los procedimientos necesarios que garanticen la adecuada administración de los activos de software de las empresas y unidades del GECC, al igual que emisión de reportes periódicos (mensuales) sobre el estado de legalidad de software de las empresas.

- Garantizar el uso de controles criptográficos dentro de los procesos transporte, procesamiento y almacenamiento de información sensible dentro de la red corporativa; al igual que en los procesos de intercambios de información con terceros.

Es responsabilidad de los Oficiales de Protección de Datos Personales del GECC:

- Velar para que, en el uso, captura, recolección y tratamiento de datos personales, se garantice la calidad y veracidad de la información.

- Verificar que se adopten las medidas tecnológicas y administrativas necesarias para evitar la adulteración, modificación, pérdida, consulta, uso o acceso no autorizado a los registros y repositorios del GECC.

- Identificar los requisitos legales, estatutarios, reglamentarios y contractuales aplicables a las empresas y unidades del GECC en materia de seguridad y privacidad de la información con el fin de garantizar el cumplimiento de los mismos.

- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.

- Establecer los lineamientos mínimos requeridos para garantizar una adecuada administración y protección de la información contenida en las bases de datos, así como de la determinación de las estrategias para la protección de datos personales.

- Monitorear y hacer seguimiento a la normatividad expedida en materia de protección de la información y hacer recomendaciones de ajustes al interior del GECC.

- Iniciar y dirigir internamente las investigaciones relacionadas con la administración de la información al interior de la empresa.

- Definir e implementar controles del Programa Integral de Gestión de Datos Personales (PIGDP).

- Actuar como coordinador con las demás áreas de las empresas que conforman el GECC para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.

- Conservar un inventario de las bases de datos personales en poder del GECC.

- Solicitar ante la Superintendencia de Industria y Comercio las declaraciones de conformidad cuando esto sea requerido.

- Revisar los contenidos de los contratos de transmisiones nacionales e internacionales.

- Diseñar un programa capacitación y sensibilización en protección de datos personales específico para cada cargo de la empresa, según el nivel y tipo de datos personales que deba conocer o usar.

- Realizar el entrenamiento necesario a los nuevos empleados (inducción), que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.

- Integrar las políticas de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call center y gestión de proveedores, etc.).

- Atender las consultas e inquietudes relacionadas con el tratamiento de información personal que titulares, funcionarios y personas o entidades con los que se comparte la información puedan manifestar.

- Mantener documentación actualizada de los procedimientos usados por el GECC para la recolección, almacenamiento, uso, circulación y supresión de información.

- Valorar los incidentes de seguridad de la información relacionados con información personal con el fin de establecer las medidas correctivas que ameriten y su posterior comunicación a la Superintendencia de Industria y Comercio y los titulares, en caso de considerarlo necesario.

- Adelantar los análisis correspondientes a la manera como se manejan los datos personales por parte de la empresa y proponer el marco metodológico más apropiado para la administración de riesgos.

- Impartir directrices para el relacionamiento con terceros encargados del tratamiento de datos personales, medir la participación y calificar el desempeño de los empleados en materia de protección de datos personales.

- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio.

- Realizar seguimiento al Programa Integral de Gestión de Datos Personales.

- Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio.

5.15.3.2. Revisiones de seguridad de la información

Es responsabilidad de la Gerencia Corporativa de Riesgo o quien haga sus veces en las empresas del GECC:

- Definir las políticas, normas y procedimientos de seguridad y privacidad de la información para las empresas y unidades del GECC, al igual que garantizar su actualización de manera periódica.

- Definir los mecanismos internos para reportar a la organización (dirigentes, administradores, accionistas, socios, etc.) el seguimiento y ejecución del Programa de Seguridad y Privacidad de la Información.

- Definir con la Auditoría Corporativa o Auditoría Interna de las empresas los planes de auditoría periódicos (semestrales o anuales) para verificar el cumplimiento de los políticas, lineamientos y procedimientos de seguridad y privacidad de la información establecidos por la organización.

- Generar informes periódicos (semestrales, anuales o por demanda) para los dirigentes, administradores, accionistas, socios, etc., que presenten el estado del programa de seguridad y privacidad de la información.

- **Es responsabilidad de la Dirección de Servicios de TI CSA**, garantizar la definición e implementación de controles técnicos que soporten las políticas de seguridad y privacidad de la información definidas para las empresas y unidades del GECC.

- **Es responsabilidad de los Directivos de las empresas y unidades del GECC,** garantizar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información por parte de los colaboradores y contratistas que están a su cargo.

- **Es responsabilidad de la Auditoría Corporativa,** validar la eficacia de los controles de seguridad de la información implementados por la Dirección de Servicios de TI CSA para dar respuesta a las políticas de seguridad y privacidad de la información definidas por la Gerencia Corporativa de Riesgo.

6. Acogimiento de las Políticas y responsabilidades

6.1. Medición de cumplimiento

- La Gerencia Corporativa de Riesgo o quien haga sus veces en el **GECC,** puede verificar el cumplimiento de esta política a través de varios métodos, incluyendo, pero no limitado a; generador de reportes, resultados de auditorías internas y externas e inspecciones directas.

6.2. Excepciones

- Cualquier excepción a la política debe ser aprobada por Gerencia Corporativa de Riesgo o quien haga sus veces en el GECC.

6.3. Incumplimiento

- Cualquier colaborador y contratista del **GECC** que incumpla con estas políticas puede estar sujeto a acciones disciplinarias, lo cual puede llevar a la terminación del contrato.