Cámara de Comercio de Bogotá

Lineamientos y prácticas Gestión de Seguridad de la Información

INTRODUCCIÓN

La **Cámara de Comercio de Bogotá (CCB)** reconoce y declara la información como un activo que tiene valor y es indispensable para la consecución de los objetivos definidos por la estrategia de la Entidad, por esta razón es necesario establecer un marco en el cual se asegure que la información es protegida y tratada de una manera adecuada, independientemente de la forma en la que ésta sea procesada, transportada o almacenada.

Los lineamientos incluidos en este documento son parte fundamental del proceso ***Gestión de Seguridad de la Información*** y se convierten en la base para implementar controles eficaces para proteger la información de la Entidad.

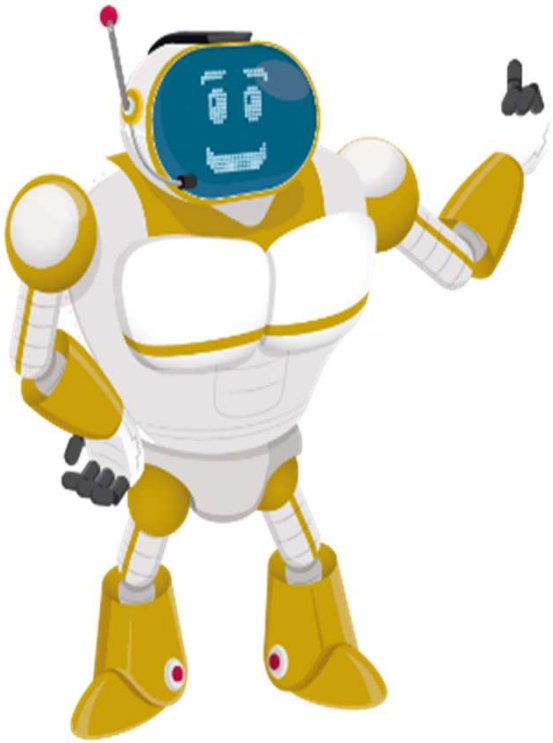
La Seguridad de la Información es una prioridad para la Entidad y por tanto es responsabilidad de todos sus **colaboradores, proveedores y aliados** sin excepción, que tengan algún tipo de acceso físico a las sedes de la CCB, acceso lógico o físico a la información de la Entidad y sean responsables y/o encargados de los activos de información, velar porque todas las actividades que se realicen cumplan con la esencia y el espíritu de cada uno de sus lineamientos.

OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

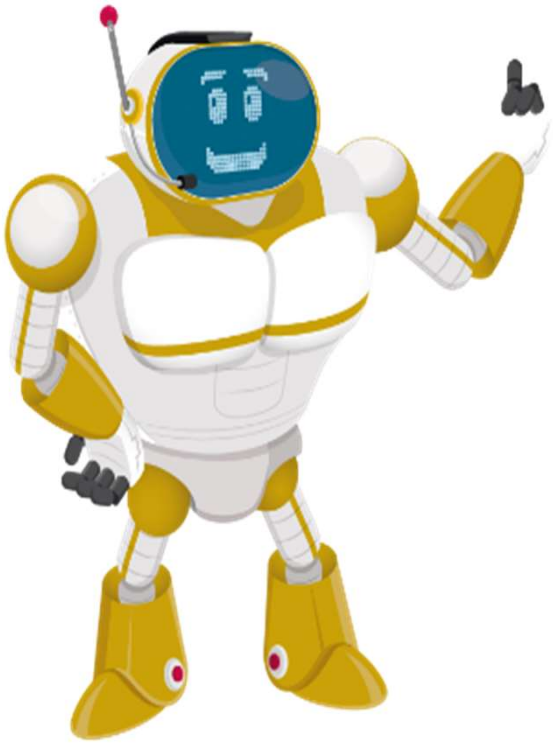
El objetivo del proceso de ***Gestión de Seguridad de la Información*** es facilitar el logro de los objetivos organizacionales mediante la implementación de las prácticas de seguridad y el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información. Para el logro de este objetivo, la Entidad se asegura de:

- Establecer el marco de trabajo que permita i) identificar los riesgos de Seguridad de la Información, considerando posibles causas, vulnerabilidades y amenazas e ii) implementar medidas y controles para la mitigación a lo largo del ciclo de vida de la información.
- Generar una cultura perceptible y medible en Seguridad de la Información en los colaboradores, inmersa en sus funciones y actividades del día a día.
- Gestionar oportunamente incidentes de Seguridad de la Información que puedan impactar las actividades y operaciones de la Entidad a partir de la notificación y análisis de eventos que permitan la mejora de los controles.
- Contribuir al cumplimiento de la legislación vigente sobre la seguridad y protección de información pública y personal, propiedad intelectual, transparencia, entre otras, para brindar tranquilidad a los empresarios de la CCB sobre el cuidado de su información.
- Alinear el esquema de gestión de la Seguridad de la Información con las actividades de los procesos de ***Gestión por procesos***, ***Gestión de riesgos*** y continuidad de negocio, garantizando el cumplimiento de los planes y acciones (preventivas o correctivas) generadas en el seguimiento interno, la revisión por la Alta Dirección y/o las auditorías internas o externas.

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



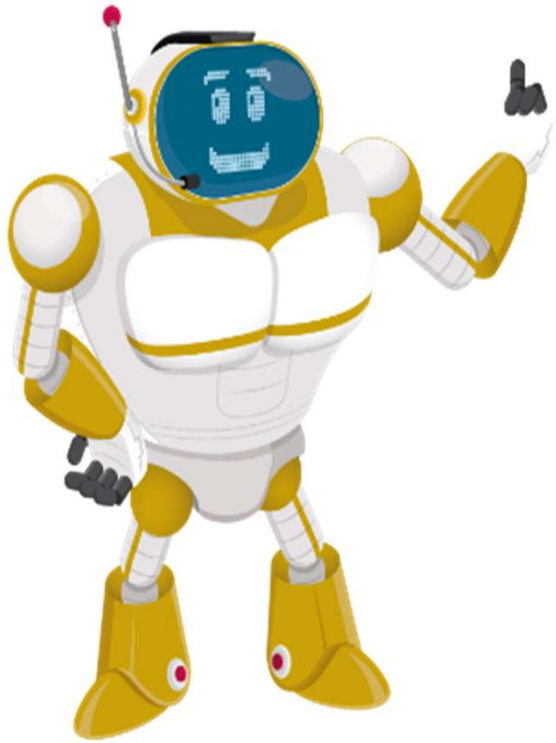
LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información aprobada por el **Comité de Buen Gobierno, Riesgos y Auditoría** (**CBGRA**) de la Entidad se encuentra publicada en el sistema de información de gestión como parte de las políticas organizacionales.

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



MODELO DE GOBIERNO

MODELO DE GOBIERNO

- Asegurar que se disponga de un adecuado proceso de gestión de riesgos, considerando riesgos de Seguridad de la Información.
- Reglamentar el funcionamiento del Comité de Buen Gobierno, Riesgos y Auditoría (**CBGRA**).
- Prevenir y asegurar que se gestionen las situaciones críticas.
- Exigir que las Políticas de Riesgos y Seguridad de la Información se traduzcan en reglas de conducta y procedimientos que orienten la actuación de la CCB, las personas destinatarias y relacionadas.
- Las demás establecidas en el Código de Ética y Buen Gobierno y las políticas organizacionales.

MODELO DE GOBIERNO

- Proveer lineamientos para la gestión de riesgos y Seguridad de la Información, siendo una instancia de direccionamiento a la gestión que realiza la Junta Directiva.
- Aprobar las políticas y metodologías de riesgos y Seguridad de la Información y presentarlas a la Junta Directiva.
- Exigir que las políticas de riesgos y Seguridad de la Información se traduzcan en reglas de conducta y procedimientos que orienten la actuación de la CCB, las personas destinatarias y relacionadas.
- Realizar seguimiento a la implementación, funcionamiento y operación de la gestión de riesgos y Seguridad de la Información.
- Las demás establecidas en el Código de Ética y Buen Gobierno y las políticas organizacionales.

MODELO DE GOBIERNO

- Evaluar temas de Seguridad de la Información que debido a su criticidad y alto impacto requieren acción inmediata.
- Recomendar cambios a la política y lineamientos de Seguridad de la Información.
- Auspiciar la gestión y la cultura de riesgos de Seguridad de la Información en todos los procesos de la Entidad.

MODELO DE GOBIERNO

- Asegurar la actualización de los lineamientos y prácticas de Seguridad de la Información.
- Coordinar el cierre de brechas de las oportunidades de mejora en los procesos, así como promover la gestión de riesgos de Seguridad de la Información.
- Validar que los planes de tratamiento de riesgos de Seguridad de la Información cumplen unos mínimos requeridos.
- Liderar la implementación de los controles exigidos por la ley y la normatividad vigente en relación a Seguridad de la Información.

MODELO DE GOBIERNO

- Asegurar la actualización de la política, lineamientos y prácticas de Seguridad de la Información.
- Liderar la implementación de los controles exigidos por la ley y la normatividad vigente en relación a Seguridad de la Información.
- Asesorar en la adecuada identificación, definición, redacción y generación de planes para el tratamiento de riesgos de Seguridad de la Información.
- Validar que los planes de tratamiento diseñados por los dueños de los procesos cumplen con los lineamientos establecidos por la línea de Gestión de riesgos.
- Asesorar a la organización en la gestión de eventos de riesgos de Seguridad de la Información.
- Presentar los avances y resultados de la gestión de riesgos de Seguridad de la Información a la instancia de aprobación y decisión que lo solicite.

MODELO DE GOBIERNO

Roles y Responsabilidades

- Participar en las mesas de trabajo para la identificación, evaluación, control y seguimiento de las situaciones de riesgo de Seguridad de la Información identificadas.
- Promover la asistencia a las capacitaciones que se programan sobre la gestión de riesgos de Seguridad de la Información.
- Liderar la gestión de riesgos de Seguridad de la Información en los proyectos velando por el cumplimiento de la política y lineamientos, cuando se desempeñe como gerente de proyecto.
- Diseñar, elaborar, desarrollar y ejecutar los planes de tratamiento para los riesgos de Seguridad de la Información.
- Coordinar la labor de los gestores de riesgo frente a los planes de tratamiento de riesgos de Seguridad de la Información.
- Reportar los incidentes de Seguridad de la Información que identifiquen.

MODELO DE GOBIERNO

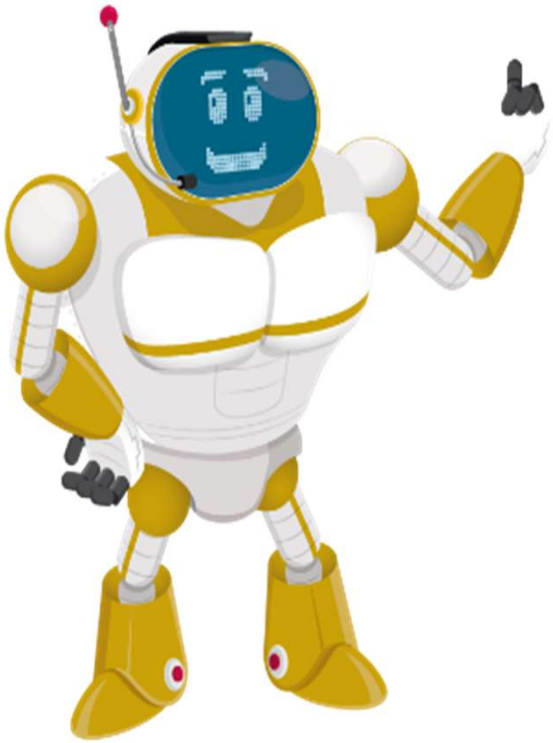
Roles y Responsabilidades

- Cumplir con las políticas y lineamientos de la gestión de riesgos de Seguridad de la Información.
- Incorporar el autocontrol en la gestión de riesgos de Seguridad de la Información.
- Apropiar y poner en práctica la cultura de gestión de riesgos de Seguridad de la Información.
- Aplicar los controles diseñados en los procesos a su cargo que presenten algún factor de riesgo de Seguridad de la Información.
- Asistir y participar activamente a las capacitaciones de gestión de riesgos de Seguridad de la Información, a las cuales sea convocado.
- Reportar los incidentes de Seguridad de la Información que identifiquen.
- Las demás establecidas en el Código de Ética y Buen Gobierno y las políticas organizacionales.

MODELO DE GOBIERNO

- Realizar el mantenimiento y actualización de la política, lineamientos y prácticas de Seguridad de la Información.
- Asesorar en la adecuada identificación, análisis y generación de planes para el tratamiento de riesgos de Seguridad de la Información.
- Validar que los planes de tratamiento diseñados por los dueños de los procesos cumplen con los lineamientos establecidos por la línea de gestión de riesgos.
- Coordinar el programa de toma de conciencia en riesgos y Seguridad de la Información, para que los colaboradores conozcan y tengan herramientas para gestionar los riesgos a los que está expuesta la Entidad.
- Consolidar la información de riesgos y Seguridad de la Información para la generación de reportes de gestión a las instancias de gobierno.

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



GESTIÓN DE ACTIVOS Y RIESGOS

Lineamiento General

Definición, implementación y alcance

La **CCB** establece las prácticas y procedimientos para la gestión de activos de información y los riesgos de Seguridad de la Información asociados; su validación y la definición de medidas de protección para mitigar estos riesgos.

Los dueños de procesos son los responsables de la identificación y clasificación de los activos de información de los procesos a su cargo, así como de la identificación y valoración de los riesgos de Seguridad de la Información y la definición e implementación de los planes de tratamiento para su mitigación.

La gestión de activos y riesgos de seguridad aplica para todos los procesos de la Entidad.

Prácticas que soportan el lineamiento

GESTIÓN DE ACTIVOS Y RIESGOS

Generación inventario activos de información

Objetivo

Identificar los activos de información críticos de los procesos.

Alcance y responsables

- Dueños de procesos
- Jefe de gestión de riesgos
- Todos los procesos

Referencias asociadas

- ***Guía para gestionar los activos de información***
- Formato ***Inventario de activos de la información***

- El Jefe de gestión de riesgos y el Coordinador de gestión de riesgos establecen el plan de trabajo para la actualización del inventario de los activos de información de cada proceso, con periodicidad de 2 años o antes si es requerido por cambios en los procesos y las líneas.

- El inventario de activos de información se realiza conjuntamente con los dueños de proceso utilizando el formato ***Inventario de activos de la información*.**

- El dueño del proceso es el responsable del activo y debe asegurar que el mismo esté clasificado de manera apropiada.

- Para el inventario de activos de información deben tenerse en cuenta los siguientes elementos:
  - Listado maestro de registros: nombres, ubicación, responsable.
  - Bases de datos de protección de datos personales: nombre, finalidad, cargo de responsable, área responsable.

GESTIÓN DE ACTIVOS Y RIESGOS

Clasificación de activos de información

Objetivo

Clasificar los activos de información en función de los requisitos legales, valor y susceptibilidad a divulgación o modificación no autorizada.

Alcance y responsables

- Dueños de procesos
- Oficina de gestión de riesgos
- Activos de información de los procesos

Referencias asociadas

- ***Guía para gestionar los activos de información***
- Formato ***Inventario de activos de la información***

- La Oficina de gestión de riesgos, como parte del plan de trabajo para la actualización del inventario de los activos de información, asesora la actualización de la clasificación de los activos, con periodicidad de 2 años o antes si es requerido por cambios en los procesos.

- La clasificación de los activos de información se realiza conjuntamente con los dueños de proceso utilizando el formato ***Inventario de activos de la información*****.** Para la clasificación de los activos se considera la ***Guía para gestionar los activos de información***.

- El responsable del proceso tendrá la propiedad de los activos y debe asegurar esté clasificados de manera apropiada.

- Los activos de información deben ser etiquetados de acuerdo con la clasificación establecida.

GESTIÓN DE ACTIVOS Y RIESGOS

Análisis riesgos Seguridad de la Información

Objetivo

Identificar los riesgos de Seguridad de la Información a los cuales están expuestos los activos de información críticos de los procesos.

Alcance y responsables

- Dueños de procesos
- Oficina de gestión de riesgos
- Activos información críticos de los procesos

Referencias asociadas

- ***Guía para gestionar los riesgos operacionales y de seguridad de la información***
- ***Matriz de riesgos operacionales y seguridad de la información***

- El análisis de riesgos de Seguridad de la Información se realiza en conjunto con los dueños de proceso utilizando el formato ***Matriz de riesgos operacionales y seguridad de la información.*** La periodicidad de la revisión es anual o antes si es requerido por cambios en los procesos.

- Los dueños de procesos deben definir y desarrollar planes de tratamiento para todos los riesgos identificados como de alta severidad. Los riesgos de severidad media serán sujeto de tratamiento de acuerdo con lo definido por los dueños de los procesos.

- Se debe hacer el seguimiento periódico (definido de acuerdo con lo definido en cada plan) a la ejecución de los planes de tratamiento con los dueños de proceso, responsables de los riesgos.

- A los planes de trabajo de riesgos debe tener acceso la Oficina de gestión de riesgos, para su respectiva revisión y conocimiento.

- Para los proyectos, se debe establecer un plan de gestión de riesgos (que incluya riesgos de seguridad) el cual puede estar contenido en el cronograma del proyecto.

GESTIÓN DE ACTIVOS Y RIESGOS

Uso aceptable de los activos

Objetivo

Indicar las responsabilidades de los involucrados en el manejo de activos de información.

Alcance y responsables

- Colaboradores
- Oficina de gestión de riesgos
- Todos los procesos

Referencias asociadas

- ***Cláusula de autorización de tratamiento y cumplimiento de la seguridad de la información y la protección de datos personales***
- ***Guía para gestionar los riesgos operacionales y de seguridad de la información***

- El acceso a los activos de información que se proporcionan a colaboradores y terceros autorizados para cumplir con el propósito de la Entidad, está determinado por las restricciones del tipo de información de acuerdo con la clasificación dada a ésta en la ***Guía para gestionar los activos de información***.

- Todos los colaboradores y terceros con acceso a información deben firmar una ***Cláusula de autorización de tratamiento y cumplimiento de la seguridad de la información y la protección de datos personales***, donde se comprometan a no divulgar, usar o explotar la información a la que tengan acceso, respetando los niveles establecidos de clasificación y que cualquier violación a lo establecido en esta práctica es considerado como un incidente de seguridad.

GESTIÓN DE ACTIVOS Y RIESGOS

Uso aceptable de los activos

Frente al acceso a internet, no está permitido:

- El acceso a páginas web que vayan en contra del Código de Ética y Buen Gobierno Corporativo, las leyes vigentes o las políticas y lineamientos establecidos en la CCB.
- El intercambio no autorizado de información de propiedad de la CCB, de sus clientes y/o de sus colaboradores con terceros no autorizados.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución (shareware, freeware), información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la seguridad de la infraestructura tecnológica. Ante dudas con esta práctica o frente a la autorización, los colaboradores deben consultar con la Oficina de gestión de riesgos para recibir asesoría. De igual forma, la Oficina de gestión de riesgos puede realizar monitoreo de la navegación realizada por los colaboradores con el fin de evaluar riesgos de seguridad.
- Dar uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros y la legislación vigente.

GESTIÓN DE ACTIVOS Y RIESGOS

Uso aceptable de los activos

- Frente al uso del correo electrónico:
  - La cuenta de correo electrónico corporativo debe ser usada para el desempeño de las funciones asignadas, de manera ética, razonable, responsable y no abusiva. El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo corporativo.
  - Los mensajes y la información contenida en los buzones de correo corporativos son propiedad de la Entidad. Cada usuario como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
  - El tamaño de los buzones de correo es determinado e implementado por la Vicepresidencia de tecnología de acuerdo con las necesidades de cada usuario y previa autorización del Jefe inmediato.
  - No se permite el uso del correo electrónico corporativo para enviar mensajes que atenten contra la dignidad y la productividad de las personas, el normal desempeño del servicio de correo electrónico y que vayan en contra del Código de Ética y Buen Gobierno Corporativo.
  - Las líneas que manejan correo masivo hacia clientes internos y externos, deben gestionar los permisos con Relacionamiento con el cliente a través de los procedimientos de esta línea.
  - Toda información generada con los diferentes programas computacionales (Ejemplo. Office, Project, Access, WordPad, entre otros.), que requiera ser enviada fuera de la Entidad, y que por sus características de integridad deba ser protegida, debe estar en formatos no editables o debidamente protegida para modificaciones (contraseñas o cifrado).
  - Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad y protección de datos personales.

GESTIÓN DE ACTIVOS Y RIESGOS

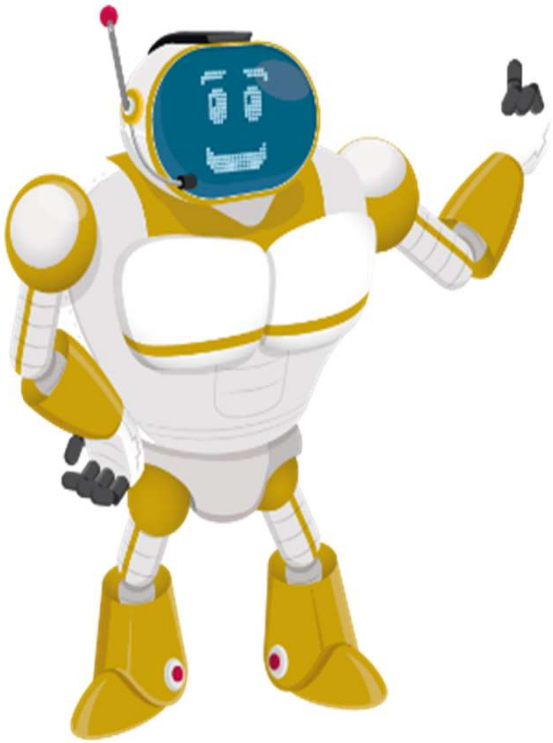
Uso aceptable de los activos

- La Gerencia de recursos humanos es la responsable de informar a la Vicepresidencia de tecnología, Gerencia de relacionamiento con el cliente, Vicepresidencia administrativa y financiera y línea de Gestión por procesos sobre el retiro de un colaborador para que procedan a remover de manera oportuna los privilegios de acceso a los recursos tecnológicos. El bloqueo de privilegios de acceso también debe realizarse cuando los colaboradores se encuentren en vacaciones o en incapacidad.

- En el uso de escritorio y pantalla limpia:

  - Todos los colaboradores y terceros que tengan un vínculo con la CCB deben mantener la información restringida o confidencial bajo llave en sus escritorios y/o sitios de trabajo, aun cuando se retiren temporalmente de sus puestos de trabajo o en horas no laborales. Esto incluye: documentos impresos, CD's, dispositivos de almacenamiento USB y medios removibles.
  - La información sensible que se envía a las impresoras debe ser recogida inmediatamente.
  - Todos los colaboradores son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá puede desbloquear sólo con la contraseña del usuario.
  - Todas las estaciones de trabajo deben usar el papel tapiz corporativo y el protector de pantalla predefinido por la Vicepresidencia de tecnología, el cual se activará automáticamente una vez se bloquee la estación o después de cinco (5) minutos de inactividad, la cual se podrá puede desbloquear únicamente con la contraseña del usuario.

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



GESTIÓN DE INCIDENTES DE SEGURIDAD

Lineamiento General

Definición, implementación y alcance

La **CCB** cuenta con prácticas y procedimientos para la gestión de incidentes de Seguridad de la Información, en pro de su identificación oportuna, evaluación, y atención, con el fin de minimizar los efectos adversos para la Entidad.

Todos los colaboradores son responsables de identificar y reportar los incidentes de seguridad. La atención de los incidentes está a cargo de la Oficina de gestión de riesgos y la Vicepresidencia de tecnología (Mesa de Servicio) como grupos de primera respuesta. Dependiendo del tipo de incidente, puede ser requerido el apoyo de otras líneas de la Entidad.

Prácticas que soportan el lineamiento

GESTIÓN DE INCIDENTES DE SEGURIDAD

Reporte de incidentes de seguridad

Objetivo

Guiar las actividades y criterios para reportar un incidente de Seguridad de la Información de forma oportuna.

Alcance y responsables

- Colaboradores
- Oficina de gestión de riesgos
- Todos los procesos

Referencias asociadas

- ***Guía para gestionar eventos de riesgo operacionales e incidentes de seguridad***

- Los colaboradores deben reportar los eventos que sean considerados como posibles incidentes de Seguridad de la Información a través del correo electrónico incidentesdeseguridad@ccb.org.co incluyendo la siguiente información:
  - Nombre de quien reporta.
  - Cargo - Extensión - Correo electrónico – Piso/Módulo de quién reporta.
  - Fecha y hora del reporte del evento.
  - Equipo, sistema afectado, piso afectado, posible colaborador afectado por el evento.
  - Descripción del evento.

- En caso de eventos que se consideren de atención inmediata, los colaboradores pueden reportarlos a las extensiones **2624, 2631, 2658, 2479**.

- Los incidentes de Seguridad de la Información, son escalados por el Jefe o Coordinador de gestión de riesgos vía correo electrónico a las líneas de la Entidad de acuerdo con su tipología (Seguridad física, Calidad de vida, Infraestructura tecnológica).

GESTIÓN DE INCIDENTES DE SEGURIDAD

Reporte de incidentes de seguridad

Objetivo

Guiar las actividades y criterios para evaluar y tratar un incidente de Seguridad de la Información de forma oportuna.

Alcance y responsables

- Equipo Oficina de gestión de riesgos
- Equipo Vicepresidencia de tecnología
- Equipo Talento humano
- Equipo Seguridad física

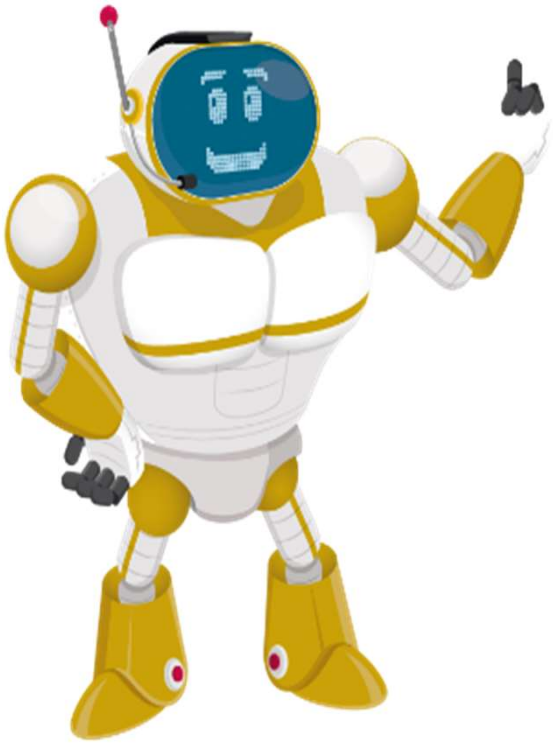
Referencias asociadas

- ***Guía para gestionar eventos de riesgo operacionales e incidentes de seguridad***

- La Coordinación de gestión de riesgos registra el evento y determina si se trata de un incidente de Seguridad de la Información para proceder con su gestión de acuerdo con la ***Guía para gestionar eventos de riesgo operacionales e incidentes de seguridad.***

- La Oficina de gestión de riesgos coordina la atención del incidente reportado y orienta la elaboración del plan a seguir con las líneas de trabajo involucradas, donde se considera:
  - Analizar el incidente.
  - Valorar el impacto y criticidad del incidente.
  - Gestionar las comunicaciones pertinentes con las líneas de trabajo y/o entes externos (por ejemplo: CAI Virtual, CSIRT, CCOC, Colcert).
  - Recolectar las pruebas, evidencias y documentación y almacenarlas de manera física y/o digital según corresponda.
  - Realizar un seguimiento a los planes de acción definidos para la atención del incidente.
  - Gestionar las lecciones aprendidas del incidente
  - Generar los reportes para las instancias superiores (Gerente de Planeación e Innovación y/o Comité de Seguridad de la Información)
  - Registrar los incidentes

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



SEGURIDAD EN RECURSOS HUMANOS

Lineamiento General

Definición, implementación y alcance

La **CCB** dispone de prácticas en procura de contar con procesos y condiciones de vinculación, desarrollo del empleo y terminación de la relación laboral bajo estándares de seguridad, para contar con personal confiable en la Entidad**.**

La Gerencia de recursos humanos es la responsable de asegurar que los procesos a su cargo cumplan con las prácticas de Seguridad de la Información. La Oficina de gestión de riesgos valida el cumplimiento de estas prácticas y lidera el programa de cultura organizacional en Seguridad de la Información.

Todos los colaboradores deben participar en las actividades de capacitación de Seguridad de la Información a las cuales sean convocados.

Prácticas que soportan el lineamiento

SEGURIDAD EN RECURSOS HUMANOS

Seguridad en la selección y vinculación

Objetivo

Verificar los antecedentes de los posibles candidatos para ser vinculados cumplen con las leyes, reglamento interno de trabajo y manual de ética desarrollado por la Entidad.

Alcance y responsables

- Equipo Gerencia talento humano
- Aplica a todos los candidatos a la **CCB**

Referencias asociadas

- ***Lineamientos para la gestión del talento humano***

- La vinculación laboral se rige por las leyes de la República de Colombia y por lo dispuesto en el Código sustantivo del trabajo.

- Todo colaborador contratado por la CCB es seleccionado adecuadamente, de acuerdo con los requerimientos de cada cargo y siguiendo los ***Lineamientos para la gestión del talento humano*** que se encuentran en el sistema de información de gestión.

- Como parte de las validaciones de antecedentes se debe considerar:
  - Antecedentes judiciales / penales / disciplinarios
  - Validaciones en *Risk* (Validaciones realizadas por Seguridad física)
  - Hoja de vida respecto a referencias laborales y académicas

- Los terceros que realicen procesos de selección en nombre de la CCB deben cumplir los lineamientos de Seguridad de la Información. La Gerencia de recursos humanos es la responsable de asegurar que este requerimiento se incluya en los respectivos contratos. La Oficina de gestión de riesgos prestará la asesoría sobre los contenidos a incluir en los contratos.

- La Gerencia de recursos humanos verifica la información brindada durante el proceso de vinculación de los colaboradores y el cumplimiento de las políticas de selección de personal.

SEGURIDAD EN RECURSOS HUMANOS

Seguridad en la vinculación laboral

Objetivo

Establecer las responsabilidades del colaborador contratado y las de la Entidad relacionadas con Seguridad de la Información.

Alcance y responsables

- Equipo Gerencia talento humano
- Equipo Oficina gestión de riesgos
- Aplica a todos los candidatos a la **CCB**

Referencias asociadas

- ***Lineamientos para la gestión del talento humano.***
- ***Cláusula de autorización de tratamiento y cumplimiento de la seguridad de la información y la protección de datos personales***.

- Todos los colaboradores y terceros que tengan acceso a la información de la CCB o a la infraestructura tecnológica, deben cumplir con la ***Cláusula de autorización de tratamiento y cumplimiento de la seguridad de la información y la protección de datos personales*** establecida por la Entidad.
- Sin importar el mecanismo de vinculación, todo colaborador recibe, comprende y acepta la Política de Seguridad de la Información y se acoge a las definiciones del Código de Ética y Buen Gobierno Corporativo y el Reglamento interno de trabajo.
- La Oficina de gestión de riesgos lidera el programa de cultura organizacional en Seguridad de la información y es responsable de su mantenimiento así como realizar su seguimiento para identificar oportunidades de mejora. El programa de cultura debe ser planeado con periodicidad anual.
- Sin excepción, todos los colaboradores deben atender las disposiciones referentes al entrenamiento, concientización y sensibilización que les permita el manejo apropiado para la protección de la información de la Entidad.

SEGURIDAD EN RECURSOS HUMANOS

Seguridad en la vinculación laboral

- Frente al teletrabajo:

  - Es responsabilidad de la Gerencia de recursos humanos reportar las solicitudes de teletrabajo a la Oficina de gestión de riesgos para contar con el análisis desde Seguridad de la Información sobre las implicaciones de la solicitud.

  - Cualquier colaborador autorizado que requiera tener acceso a la información de la CCB desde redes externas, podrá acceder remotamente mediante conexión segura provista a partir de la configuración de una VPN en el equipo de cómputo. La configuración de VPNs se encuentra a cargo de la Vicepresidencia de tecnología.

  - En caso que ocurra pérdida o hurto de un equipo en el cual se lleven actividades de teletrabajo, está a cargo del teletrabajador responsable informar el evento de forma inmediata al correo electrónico incidentesdeseguridad@ccb.org.co o a las extensiones **2624, 2631, 2658, 2479.**

- Frente al uso de medios removibles:

  - El uso de medios removibles (CDs, DVDs, USBs, discos duros externos) está autorizado para aquellos colaboradores cuyo perfil del cargo y funciones lo requiera de mutuo acuerdo entre los dueños de las líneas y la Oficina de gestión de riesgos.

SEGURIDAD EN RECURSOS HUMANOS

Seguridad en la vinculación laboral

- Frente al uso de medios removibles:

  - La Vicepresidencia de tecnología es responsable de implementar los controles necesarios para asegurar que sólo los colaboradores autorizados pueden hacer uso de los medios de almacenamiento removibles.

  - El colaborador a quién se autorice el uso de un medio removible se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información corporativa que éste contiene.

SEGURIDAD EN RECURSOS HUMANOS

Seguridad en la terminación laboral

Objetivo

Proteger los intereses de la Entidad como parte del proceso de cambio y/o terminación del contrato laboral.

Alcance y responsables

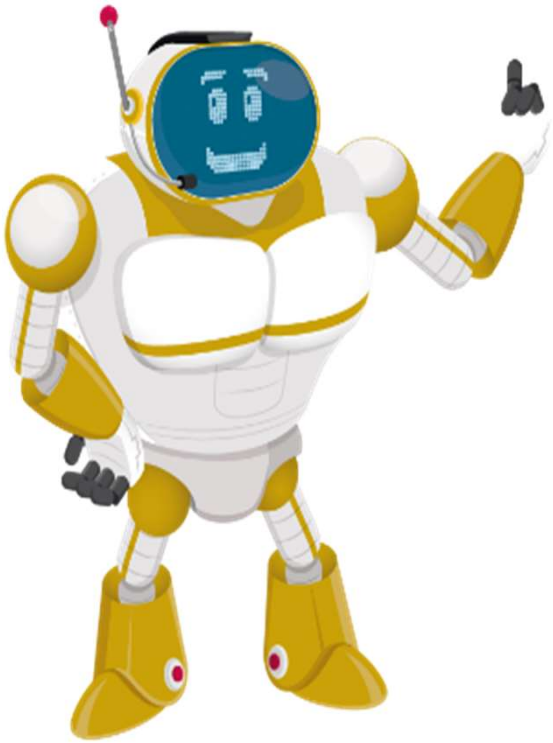
- Gerencia talento humano
- Vicepresidencia de tecnología
- Oficina gestión de riesgos
- Aplica a todos los candidatos a la **CCB**

Referencias asociadas

- ***Lineamientos para la gestión del talento humano.***

- Cuando un colaborador se retira o cambia de funciones, la solicitud de retiro o modificación de accesos (lógicos y físicos) y activos debe ser realizada por la Gerencia de recursos humanos. Es responsabilidad de esta Gerencia remitir estas novedades de personal a la Vicepresidencia de tecnología, Vicepresidencia administrativa y financiera, Gerencia de relacionamiento con el cliente y Línea de Gestión por procesos para que realicen el bloqueo de los accesos y la entrega de activos. La notificación de novedades deben ser copiados a la Oficina de gestión de riesgos.
- La Oficina de gestión de riesgos es la responsable de validar que los accesos físicos y lógicos sean eliminados cuando un colaborador se retira de la Entidad o cambia sus funciones.
- Cuando un colaborador se retira debe entregar la información utilizada y generada durante el ejercicio de sus funciones a su Jefe inmediato. El Jefe inmediato solo firmará el paz y salvo por retiro de la Entidad una vez reciba esta información.
- Ante devolución de equipos por terminación del empleo o reasignación de los mismos, la Vicepresidencia de tecnología es responsable de realizar el respaldo de la información del equipo y realizar el borrado seguro de información. Este proceso debe ser aplicable a equipos que se den de baja, sean devueltos al proveedor o sean reasignados a otro colaborador.

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



SEGURIDAD FÍSICA

Lineamiento General

Definición, implementación y alcance

La **CCB** dispone de mecanismos de control de acceso electrónico en sus sedes y controles de seguridad física para proteger los bienes de la Entidad. El mantenimiento e implementación de estos mecanismos de protección son de responsabilidad del Jefe de seguridad física y su equipo de trabajo.

Todos los colaboradores de planta, temporales o terceros deben portar en un lugar visible la tarjeta de control de acceso que es entregada al vincularse con la Entidad o en el caso de visitantes la tarjeta de control y/o el sticker entregado en la recepción al momento del ingreso.

Prácticas que soportan el lineamiento

SEGURIDAD FÍSICA

Control de acceso físico

Objetivo

Presentar los controles que se deben seguir para el ingreso y salida de personal (interno y/o externo) y bienes de propiedad de la **CCB**.

Alcance y responsables

- Equipo seguridad física
- Aplica a todas las sedes

Referencias asociadas

- ***Lineamientos de seguridad física***
- ***Lineamientos operacionales operación centro de cómputo***

- Los visitantes se deben registrar en la recepción de la Entidad para la autorización de ingreso y deben portar una escarapela que los identifique dentro de las instalaciones; siempre deben estar acompañados por un colaborador.

- En todos los casos se deben seguir los ***Lineamientos de seguridad física*** y los ***Lineamientos operacionales operación centro de cómputo*** disponibles en el sistema de información de gestión.

- El centro de cómputo es un área restringida y sólo tienen acceso a ella los colaboradores de la Vicepresidencia de tecnología definidos en los ***Lineamientos operacionales operación centro de cómputo***. Para el ingreso se cuenta con un control biométrico para validación del ingreso de cada colaborador autorizado.

- Otros colaboradores y terceros que requieran ingreso al centro de cómputo deben estar autorizados y acompañados por los colaboradores autorizados y registrarse en la bitácora de visitantes.

- Los colaboradores deben portar en un lugar visible su carnet durante su permanencia en las instalaciones y no debe ser compartido con otros.

SEGURIDAD FÍSICA

Protección contra amenazas externas y ambientales

Objetivo

Presentar los controles que se deben seguir para la protección de la infraestructura tecnológica.

Alcance y responsables

- Equipo seguridad física
- Equipo Vicepresidencia de tecnología

Referencias asociadas

- N/A

- En la implementación de la infraestructura tecnológica se deben considerar las amenazas ambientales a las que puede estar expuesta y prever planes de mitigación y de contingencia para las amenazas identificadas y de mayor riesgo de ocurrencia. Estos aspectos deben ser tenidos en cuenta frente a la infraestructura contratada como servicio y ser considerados en los acuerdos contractuales con proveedores.
- Los computadores sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos.
- En las áreas debe contarse con equipos para la extinción manual o automática de incendios. En el centro de cómputo se deben establecer controles ambientales para detectar y mitigar incendios y problemas de humedad.
- Las salidas de emergencia de la Entidad, deben estar plenamente identificadas y libres de obstáculos, con el fin de poder realizar evacuaciones rápidas en caso de presentarse algún incidente.
- Se deben adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

SEGURIDAD FÍSICA

Servicios de suministro y cableado

Objetivo

Presentar los controles que se deben seguir para la protección de equipos tecnológicos.

Alcance y responsables

- Equipo seguridad física
- Equipo Vicepresidencia de tecnología

Referencias asociadas

- N/A

- Los servidores y estaciones de trabajo deben protegerse contra picos de energía eléctrica con filtros eléctricos, supresores de picos de corriente y en lo posible, eliminadores de corriente estática. En los servidores deben usarse fuentes de poder ininterrumpido de potencia (UPS).
- Ningún usuario deberá conectar equipos diferentes a computadores y portátiles, al circuito de corriente regulada, los cuales se encuentran debidamente identificados y marcados en color naranja.
- Se debe asegurar el suministro de energía eléctrica mediante un mecanismo de generación de energía eléctrica, como es el caso de las plantas eléctricas, en caso de falla del suministro de la red externa.
- Todo el cableado estructurado de energía y la red de datos debe estar debidamente instalado y protegido por canaletas, de la misma manera debe estar etiquetado y correctamente identificado.
- La Vicepresidencia de tecnología es responsable del mantenimiento preventivo de los componentes que conforman la infraestructura tecnológica. Para ello debe programar de forma periódica el mantenimiento y soporte correspondiente.

SEGURIDAD FÍSICA

Retiro de activos y equipos

Objetivo

Presentar los controles que se deben seguir para la protección de equipos tecnológicos**.**

Alcance y responsables

- Equipo seguridad física
- Equipo Vicepresidencia de tecnología

Referencias asociadas

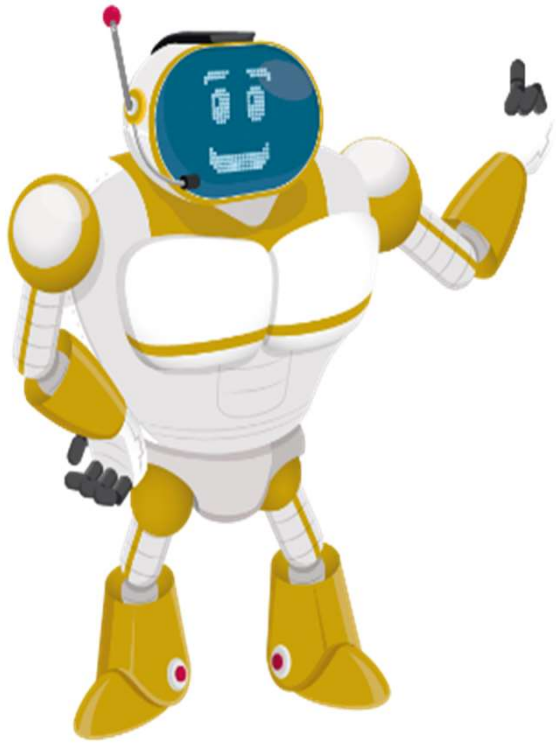
- N/A

- Bajo ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista. (Ejemplo, cuando están siendo transportados en un vehículo).

- Los equipos de infraestructura deben ser transportados con las medidas de seguridad apropiadas, que garanticen la integridad física de los dispositivos. Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

- En caso de pérdida o robo de un equipo corporativo, se debe informar inmediatamente al Jefe inmediato y reportar el incidente al correo electrónico incidentesdeseguridad@ccb.org.co o las extensiones **2624, 2631, 2658, 2479.**

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



CUMPLIMIENTO Y PRIVACIDAD

Lineamiento General

Definición, implementación y alcance

La **CCB** cumple con la reglamentación de propiedad intelectual, privacidad y protección de datos personales vigente en el país asegurando la protección de sus signos distintivos, validando que ante requerimientos de cambios en estos o el requerimientos de nuevos signos distintivos se estén respetando los derechos de propiedad intelectual de terceros, e implementando los controles de protección requeridos sobre datos personales.

La Oficina de gestión de riesgos vigila la implementación de los controles de Seguridad de la Información definidos o exigidos por la ley y las normas aplicables en materia de derechos de propiedad intelectual, privacidad y protección de datos; con el soporte prestado por la Vicepresidencia jurídica como área que sigue las iniciativas normativas que pueden impactar a la CCB.

Todos los colaboradores se acogen al cumplimiento de la ley y normas aplicables en materia de Seguridad de la Información, derechos de propiedad intelectual y privacidad y protección de datos personales.

Prácticas que soportan el lineamiento

CUMPLIMIENTO Y PRIVACIDAD

Derechos de propiedad intelectual

Objetivo

Garantizar la protección intelectual de cualquier material que se desarrolle y/o se utilice dentro de la CCB.

Alcance y responsables

- Equipo Vicepresidencia de tecnología

Referencias asociadas

- ***Lineamientos gestión de la propiedad industrial***

- Los derechos de propiedad intelectual incluyen códigos fuente, documentos generados como parte del conocimiento del negocio, propuestas comerciales, información publicitaria y comercial que involucre la imagen corporativa de la Entidad. Deben existir acuerdos contractuales claramente definidos entre la CCB y cualquier proveedor, en los cuales se especifiquen los compromisos de preservación de los derechos de propiedad intelectual.

- La Vicepresidencia de tecnología es responsable por mantener y administrar el inventario y control de todas las licencias, así como los medios y contratos que se relacionan con la actividad comercial de compra de software y hardware para la Entidad.

- Está prohibido el uso de software ilegal o no licenciado. Los colaboradores son responsables por la instalación y utilización de software no autorizado en sus estaciones de trabajo y en las plataformas tecnológicas.

- En todos los casos se deben seguir los ***Lineamientos de gestión de la propiedad industrial***.

CUMPLIMIENTO Y PRIVACIDAD

Privacidad y protección de datos personales

Objetivo

Garantizar la protección de los datos personales que estén bajo la administración y custodia de la CCB.

Alcance y responsables

- Equipo Oficina gestión de riesgos
- Equipo Vicepresidencia de tecnología

Referencias asociadas

- ***Políticas organizacionales (Política de protección de datos personales)***

- Las acciones en el uso y manejo de la información de datos personales considera lo dispuesto en la ***Políticas organizacionales***.
- La información personal de los colaboradores y/o contratistas es de carácter confidencial, por lo cual se establecen los controles necesarios para su protección y en ningún momento puede ser divulgada a terceras partes a menos que cuente con la autorización formal del colaborador y/o contratista o en los casos en que la normatividad lo permita.
- La información de clientes considerada como personal es de carácter confidencial y está sujeta a los controles de protección definidos por la Oficina de gestión de riesgos.
- Los controles de acceso a información de carácter personal son los establecidos a nivel de control de acceso físico y lógico para la información clasificada como confidencial.
- Deben existir acuerdos contractuales claramente definidos entre la CCB y cualquier proveedor, en los cuales se especifiquen los compromisos frente a privacidad y protección de datos personales.

CUMPLIMIENTO Y PRIVACIDAD

Protección de registros de auditoria

Objetivo

Garantizar la protección de los registros de auditoría de las operaciones y transacciones críticas.

Alcance y responsables

- Equipo Vicepresidencia de tecnología
- Equipo Oficina gestión de riesgos

Referencias asociadas

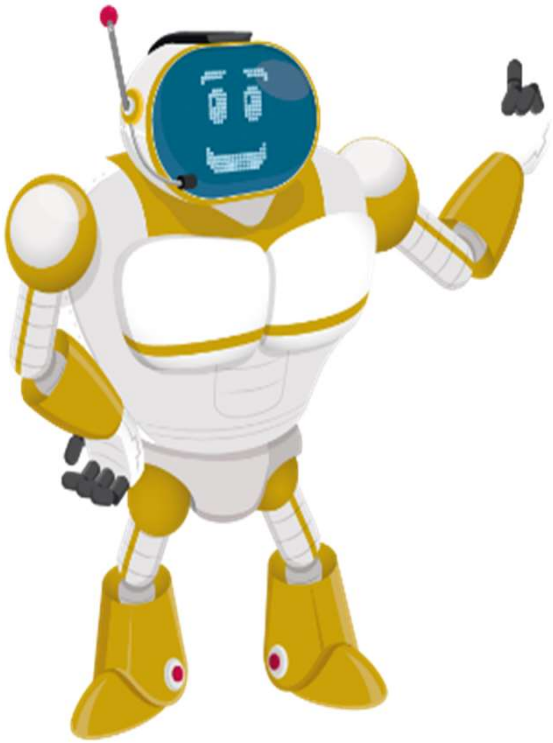
- N/A

- Las aplicaciones y sistemas críticos de la Entidad deben tener implementados registros de auditoría que permitan establecer la trazabilidad de una operación o transacción y sirvan como mecanismo para la detección de fallas, posibles eventos de fraude o violaciones a la seguridad.

- Los registros de auditoría de los sistemas y aplicaciones se deben proteger y almacenar de acuerdo con los requerimientos de la Entidad. Estos tiempos deben ser establecidos entre la Vicepresidencia de tecnología y la Oficina de gestión de riesgos.

- La responsabilidad del mantenimiento de los registros de auditoría es de la Vicepresidencia de tecnología.

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



SEGURIDAD CON PROVEEDORES

Lineamiento General

Definición, implementación y alcance

En la **CCB** se establecen los controles de Seguridad de la Información frente al acceso de los proveedores y contratistas a la información de la Entidad, así como disposiciones sobre recuperación, contingencia y continuidad de los servicios contratados con los contratistas. La Entidad en la relación con proveedores, protege los datos recolectados de estos en la base de datos de la Entidad.

La Dirección de planeación y gestión contractual es la responsable de establecer los lineamientos para asegurar el cumplimiento de los controles de Seguridad de la Información frente a información de proveedores potenciales registrada en la base de datos de la CCB.

La Oficina de gestión de riesgos informa y asesora a los colaboradores involucrados en los procedimientos de contratación sobre los lineamientos y prácticas de Seguridad de la Información.

Todos los proveedores y contratistas con acceso a información de la CCB se acogen al presente lineamiento.

Prácticas que soportan el lineamiento

- **Protección de la información de proveedores**
- **Tratamiento de la seguridad dentro de los acuerdos con contratistas**

SEGURIDAD CON PROVEEDORES

Protección de la información de proveedores

Objetivo

Establecer los controles frente a la información recolectada de terceros cuando se registran como proveedores.

Alcance y responsables

- Director de planeación y gestión contractual
- Administradores de contratos

Referencias asociadas

- ***Lineamientos para la administración de la base de datos de proveedores potenciales***

- La Dirección de planeación y gestión contractual como parte de los estudios de mercado realizados**,** exige en los casos que aplique, a los proveedores invitados acogerse a las disposiciones sobre confidencialidad de la información de la Entidad a la que puedan tener acceso como parte del estudio de mercado.

- La Oficina de gestión de riesgos y la Dirección de planeación y gestión contractual disponen los controles para proteger la información administrada en la base de datos de proveedores potenciales.

- La Dirección de planeación y gestión contractual es la responsable de la implementación de los controles para proteger los expedientes (digitales o en físico) de los proveedores potenciales de la Entidad.

SEGURIDAD CON PROVEEDORES

Tratamiento de la seguridad dentro de los acuerdos con contratistas

Objetivo

Identificar y exigir controles de Seguridad de la Información específicamente en el acceso de los contratistas a la información de la CCB.

Alcance y responsables

- Dirección de contratación
- Supervisores de contratos

Referencias asociadas

- ***Estatuto de contratación***
- ***Manual de procedimiento de contratación***

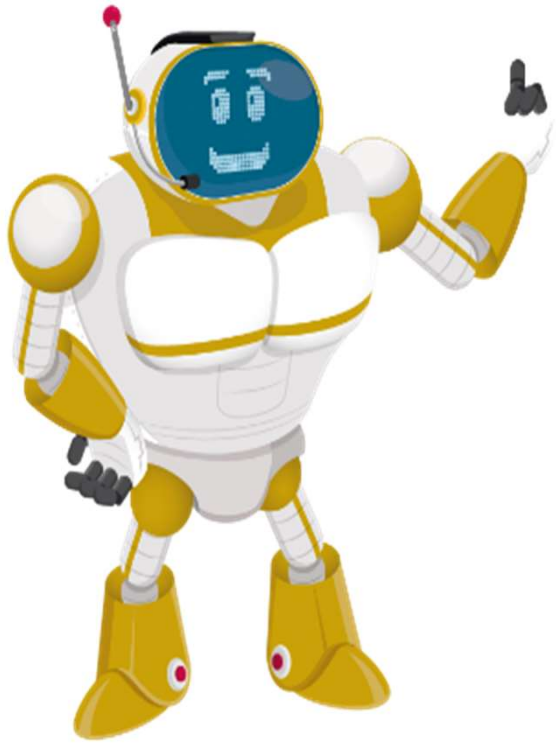
- El supervisor de contrato es el responsable de definir los siguientes controles en los acuerdos con los contratistas:
  - Los tipos de acceso a la información que se permitirán al contratista y el seguimiento en su uso.
  - Las disposiciones sobre privacidad y protección de datos que debe cumplir el contratista en la prestación de servicios.
  - Las disposiciones sobre recuperación, contingencias y continuidad de los servicios prestados a la CCB, para asegurar la disponibilidad de la información procesada o el servicio suministrado por el contratista.

  El supervisor del contrato debe informar a la Dirección de contratación estas disposiciones para que sean incluidas en el contrato respectivo.

- La Dirección de contratación es la responsable de la implementación de los controles para proteger los expedientes contractuales durante su alistamiento, digitalización, archivo y consulta.

- Cualquier incidente relacionado con la información de los contratos debe ser tratado de acuerdo con lo establecido en la ***Guía de gestión de eventos operacionales e incidentes de seguridad de la información*****.**

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



RED Y COMUNICACIONES

Definición, implementación y alcance

La CCB cuenta con prácticas en procura de contar con controles de seguridad en redes y comunicaciones. El área de Infraestructura tecnológica de la Vicepresidencia de tecnología debe identificar e implementar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de los servicios de red utilizados por la Entidad.

Prácticas que soportan el lineamiento

RED Y COMUNICACIONES

Control de acceso lógico

Objetivo

Definir los requisitos para el acceso lógico a los activos de información disponibles en red por parte de colaboradores y terceros de acuerdo con sus derechos de acceso.

Alcance y responsables

- Vicepresidencia de tecnología
- Equipo Oficina de gestión de riesgos
- Colaboradores
- Terceros con acceso a recursos en red

Referencias asociadas

- ***Administración de usuarios, roles y perfiles de los sistemas de información***
- ***Administración de usuarios, roles y perfiles ERP SAP***

- La Vicepresidencia de tecnología y la Gerencia de relacionamiento con el cliente asignan los accesos a plataformas, sistemas de información, servicios y segmentos de red de acuerdo con procesos formales de autorización de los dueños de procesos o sistemas de información, los cuales deben ser revisados periódicamente por la Oficina de gestión de riesgos.

- Los dueños de procesos o sistemas de información deben determinar los privilegios de acceso que se pueden otorgar a los colaboradores y terceros de acuerdo con los requerimientos de acceso para el cumplimiento de la operación y las funciones de estos.

- El acceso lógico está determinado por el suministro de usuarios y mecanismos de autenticación únicos por colaborador. Esta actividad está a cargo de la Vicepresidencia de tecnología y la Gerencia de relacionamiento con el cliente con el monitoreo de la Oficina de gestión de riesgos.

- Los colaboradores y terceros con acceso a los servicios de red son responsables del uso de la información de autenticación.

- En todos los casos se deben seguir lo descrito en los procedimientos de ***Administración de usuarios, roles y perfiles de los sistemas de información diferentes del ERP SAP y Administración de usuarios, roles y perfiles ERP SAP*** disponibles en el sistema de información de gestión.

RED Y COMUNICACIONES

Control de acceso lógico

- Considerando que el acceso lógico está basado en la gestión de usuarios y mecanismos de autenticación (contraseñas), se establece:

  - Las contraseñas iniciales otorgadas deben servir únicamente para el primer ingreso del usuario al sistema, en ese momento el sistema debe obligar al usuario a cambiar su contraseña.
  - El sistema debe limitar el número de intentos consecutivos de introducir una contraseña válida. Después de tres (3) intentos fallidos el identificador del usuario debe ser bloqueado.
  - Las contraseñas deben ser cambiadas al momento que exista sospecha de una posible falla de seguridad.

- Para la calidad de las contraseñas se considera:
  - Deben estar compuestas por tres de las siguientes las siguientes categorías:
    - Letras mayúsculas (de la A la Z).
    - Letras minúsculas.
    - números de 0 a 9.
    - Caracteres no alfanuméricos (caracteres especiales): (~! @ # $% ^ & * _- + = `| \ () {} [] :;" '<>,.? /)y caracteres especiales tales como ¡%$@.
    - Cualquier carácter de Unicode que se clasifica como un carácter alfabético pero no está en mayúsculas o minúsculas. Esto incluye caracteres Unicode de idiomas asiáticos.
  - Deben tener como longitud mínima 8 caracteres
  - El historial de contraseñas debe ser de las últimas 5 contraseñas utilizadas por el usuario
  - La vigencia de la contraseña es de 40 días, tiempo a partir del cual debe expirar y solicitar el cambio de contraseña
  - El usuario debe recibir notificación previa del vencimiento de su contraseña para que realice el cambio correspondiente

RED Y COMUNICACIONES

Seguridad en la transferencia de información

Objetivo

Mantener la Seguridad de la Información transferida dentro de la CCB y con cualquier entidad externa.

Alcance y responsables

- Vicepresidencia de tecnología
- Equipo Oficina de gestión de riesgos
- Colaboradores
- Terceros con acceso a recursos en red

Referencias asociadas

- N/A

- La CCB establece acuerdos de confidencialidad con los colaboradores, clientes y terceros que por diferentes razones requieran conocer o intercambiar información de la Entidad. En estos acuerdos quedan especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deben firmar antes de permitir el acceso o uso de dicha información.

- Todo colaborador es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

- Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma.

- Los controles sobre transferencia de información se aplican para datos personales.

RED Y COMUNICACIONES

Seguridad en la red

Objetivo

Definir los requisitos para la gestión de seguridad en la red.

Alcance y responsables

- Vicepresidencia de tecnología
- Equipo Oficina de gestión de riesgos
- Colaboradores
- Terceros con acceso a recursos en red

Referencias asociadas

- N/A

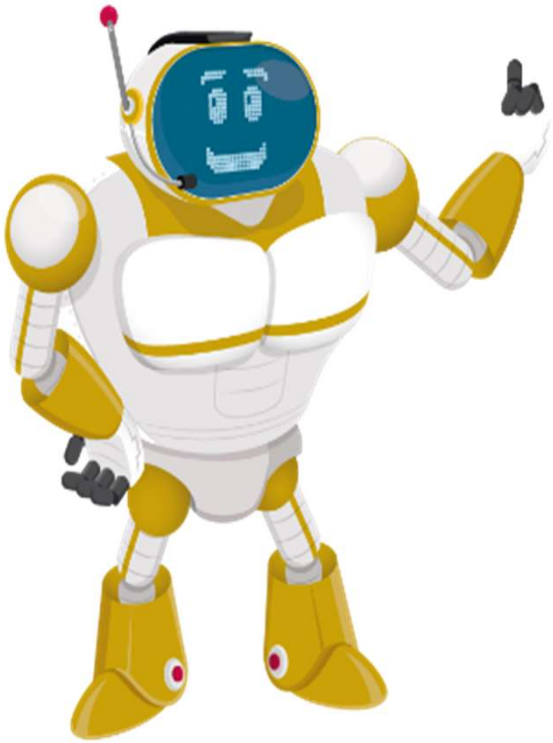
- La Vicepresidencia de tecnología está a cargo de implementar controles para la protección de la información electrónica, tales como aseguramiento de equipos de red, empleo de firewall, listas de control de acceso, entre otros.

- La plataforma tecnológica que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La Vicepresidencia de tecnología es el área encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos partiendo de un análisis de riesgos.

- Es responsabilidad de la Vicepresidencia de tecnología garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar restringidos y monitoreados con el fin de prevenir accesos no autorizados.

- El usuario que requiera acceso remoto a la red siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



ADQUISICIÓN Y DESARROLLO DE SOFTWARE

Lineamiento General

Definición, implementación y alcance

En la CCB, la implementación de un nuevo software, así como la actualización del mismo debe estar planeada, administrada, y formalmente documentada asegurando que los riesgos de Seguridad de la Información asociados sean mitigados.

Para todo el software de la Entidad desarrollado internamente, a través de un tercero o adquirido, la Vicepresidencia de tecnología es la responsable de implementar los requerimientos en materia de Seguridad de la Información, privacidad y protección de datos personales desde el inicio del proceso de diseño del software hasta su puesta en producción con la asesoría de la Oficina de gestión de riesgos.

Prácticas que soportan el lineamiento

ADQUISICIÓN Y DESARROLLO DE SOFTWARE

Análisis y especificación de los requerimientos de seguridad

Objetivo

Asegurar la inclusión de los requisitos relacionados con Seguridad de la Información en las especificaciones para nuevos aplicativos software o para mejoras en los existentes.

Alcance y responsables

- Vicepresidencia de tecnología
- Proveedores de desarrollo externos
- Equipo Oficina de gestión de riesgos

Referencias asociadas

- N/A

- La Vicepresidencia de tecnología y la Oficina de gestión de riesgos son los responsables de realizar el análisis y especificar los requisitos en materia de Seguridad de la Información, privacidad y protección de datos personales con los cuales deben cumplir los desarrollos.
- El desarrollo de software debe estar basado en metodologías y prácticas seguras determinadas de común acuerdo entre la Vicepresidencia de tecnología, el proveedor de desarrollo (si es externo) o el equipo de desarrollo interno y el equipo de la Oficina de gestión de riesgos.
- Los requerimientos de Seguridad de la Información mínimos que se deben observar en la adquisición y desarrollo de software son:
  - Procesos de identificación, autenticación y autorización de usuarios.
  - Análisis de roles, perfiles y privilegios de acceso; que den origen a una matriz para su gestión.
  - Los requerimientos de protección para datos personales que puedan manejarse como parte de los desarrollos (Ejemplo, Manejo de datos en ambientes de desarrollo) y cómo es diseñado el software para la posterior administración de estos datos.
  - El análisis sobre el manejo de logs de acuerdo con tipo de aplicación, su criticidad y funcionalidad.

ADQUISICIÓN Y DESARROLLO DE SOFTWARE

Seguridad en el desarrollo y soporte de software

Objetivo

Establecer y aplicar reglas para los procesos de desarrollo y soporte de software, ya sean realizados por la CCB o por terceros.

Alcance y responsables

- Vicepresidencia de tecnología
- Proveedores de desarrollo externos
- Equipo Oficina de gestión de riesgos

Referencias asociadas

- ***Construcción y mantenimiento de software***

- Los desarrollos o modificaciones de software deben ser implementados en el ambiente de producción después de un protocolo de pruebas que involucre aspectos funcionales, no funcionales y de Seguridad de la Información de acuerdo con los requerimientos propios de cada aplicación (tales como manejo de excepciones, control de acceso, validación de entrada y salida de datos, entre otros).
- Los ambientes de desarrollo, pruebas y producción deben encontrarse separados. La Vicepresidencia de tecnología es la responsable de administrar el acceso sobre estos ambientes asegurando que se mantiene la segregación de funciones.
- Los administradores de las plataformas de producción son los responsables de controlar el acceso a las aplicaciones, así como de coordinar y/o ejecutar las actualizaciones programadas.
- El acceso de los proveedores a los sistemas de producción sólo es permitido para realizar labores de soporte o mantenimiento, previa autorización del administrador de la plataforma y con el respectivo monitoreo por parte de este. Cuando la administración se tercerice, los lineamientos y controles de seguridad requeridos serán indicados como parte del contrato.

ADQUISICIÓN Y DESARROLLO DE SOFTWARE

Seguridad en el desarrollo y soporte de software

- En todos los casos se deben seguir el procedimiento de ***Construcción y mantenimiento de software*** disponible en el sistema de información de gestión.

- Para todo desarrollo de software realizado por terceros a ser utilizado por la Entidad, se deben especificar cuáles son las condiciones de utilización del código fuente y cuáles son los derechos de propiedad que deben ser tenidos en cuenta.

- La Vicepresidencia de tecnología debe llevar un proceso de control de cambios y versiones, utilizado para controlar las modificaciones, cambios y documentación del software de la Entidad.

- Todo cambio y/o actualización en los aplicativos e infraestructura que los soporta y que se encuentren en producción, debe cumplir con el proceso de control de cambios. La Oficina de gestión de riesgos participará en el análisis realizado por el Comité de cambios y configuraciones para llevar a cabo un cambio o actualización en los aplicativos e infraestructura que los soporta previo a su puesta en producción.

ADQUISICIÓN Y DESARROLLO DE SOFTWARE

Pruebas de Seguridad de la Información

Objetivo

Establecer los requisitos para realizar pruebas de Seguridad de la Información a los desarrollos nuevos o a las mejoras realizadas sobre los existentes.

Alcance y responsables

- Vicepresidencia de tecnología
- Proveedores de desarrollo externos
- Equipo Oficina de gestión de riesgos

Referencias asociadas

- N/A

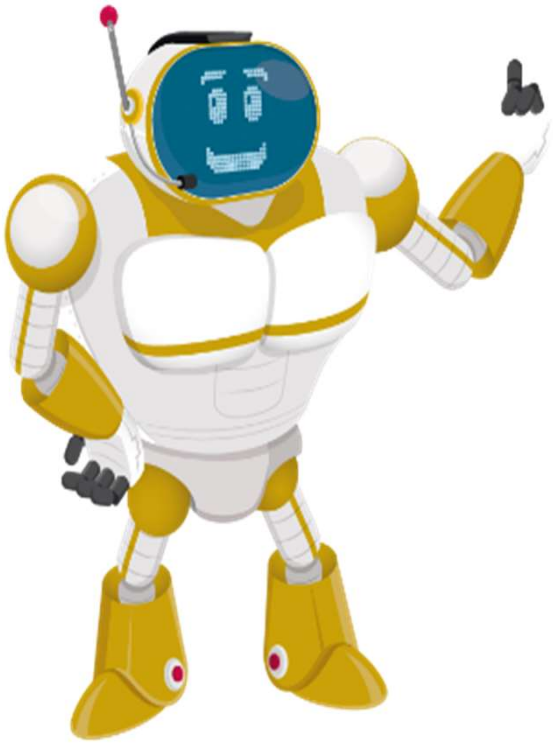
- Para nuevo software a ser implantado, sea desarrollado en la Entidad o por terceros, La Oficina de gestión de riesgos evaluará la necesidad de realizar pruebas de Seguridad de la Información y pruebas de vulnerabilidad del software, de tal forma que se tengan niveles adecuados de seguridad aceptados por la Entidad.

- La Oficina de gestión de riesgos es la responsable de validar la ejecución y aceptación de las pruebas de Seguridad de la Información. La ejecución de las pruebas está bajo la responsabilidad de la Oficina de gestión de riesgos y de la Vicepresidencia de tecnología.

- Las pruebas de Seguridad de la Información deben estar basadas en metodologías y prácticas de desarrollo seguro determinadas de común acuerdo entre la Vicepresidencia de tecnología, el proveedor de desarrollo (si es externo) o el equipo de desarrollo interno y el equipo de la Oficina de gestión de riesgos.

- En caso que se requiera contar con datos de prueba sacados de ambiente de producción, se deberán implementar mecanismos de enmascaramiento de datos de acuerdo con el tipo de datos, los requerimientos del negocio y las posibilidades de cada aplicación.

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



SEGURIDAD EN OPERACIONES

Lineamiento General

Definición, implementación y alcance

La CCB promueve prácticas para asegurar que las operaciones en la Entidad se realizan bajo parámetros seguros, considerando aspectos para la gestión de cambios, la protección contra malware, el respaldo de la información y la gestión de vulnerabilidades técnicas.

La Vicepresidencia de tecnología y los dueños de los procesos son los responsables de la aplicación de los controles de Seguridad de la Información que soportan los aspectos mencionados.

Prácticas que soportan el lineamiento

SEGURIDAD EN OPERACIONES

Control de cambios

Objetivo

Gestionar las solicitudes de cambio sobre software y hardware que soportan las operaciones.

Alcance y responsables

- Vicepresidencia de tecnología
- Responsables de líneas
- Equipo Oficina de gestión de riesgos

Referencias asociadas

- ***Gestión de cambios y configuración***

- Todo cambio que se realice sobre la infraestructura tecnológica debe ser controlado, gestionado, sometido a una evaluación que permita identificar riesgos asociados que pueden afectar la operación del negocio y autorizado por los niveles correspondientes según la infraestructura afectada.

- Los cambios que puedan afectar los controles de Seguridad de la Información en ambiente de producción pueden ser revisados por el Comité de seguridad de la información, cuando esta instancia considere pertinente su análisis para evaluar impactos adversos en las operaciones del negocio.

- Entre los aspectos que debe considerar el control de cambios están:
  - La planeación y pruebas de los cambios
  - El análisis del impacto por el cambio, incluyendo el impacto en la Seguridad de la Información
  - Las actividades de *rollback* y las actividades de recuperación considerando imprevistos en los cambios.

- En todos los casos se deben seguir el procedimiento de ***Gestión de cambios y configuración*** disponible en el sistema de información de gestión.

SEGURIDAD EN OPERACIONES

Gestión de la capacidad tecnológica

Objetivo

Establecer los requerimientos de monitoreo y proyección de la capacidad de los recursos tecnológicos para asegurar su desempeño.

Alcance y responsables

- Vicepresidencia de tecnología

Referencias asociadas

- Proceso ***Gestión de infraestructura tecnológica***

- La Vicepresidencia de tecnología mantendrá un proceso continuo de monitoreo, análisis y evaluación del rendimiento y capacidad de la infraestructura tecnológica, con el fin de identificar y controlar el consumo de recursos y prever el crecimiento de forma planificada asegurando la integridad y disponibilidad de la infraestructura tecnológica.

SEGURIDAD EN OPERACIONES

Controles contra malware

Objetivo

Establecer mecanismos de control y protección contra software malicioso.

Alcance y responsables

- Vicepresidencia de tecnología

Referencias asociadas

- N/A

- La CCB establece que los equipos de cómputo y servidores deben estar protegidos mediante herramientas y software de seguridad, como antivirus, *antispam*, *antispyware* y otras aplicaciones que brinden protección contra código malicioso.

- La Vicepresidencia de tecnología es responsable de establecer controles para detectar, prevenir y recuperar posibles fallos causados por código malicioso, con el apoyo en su análisis por la Oficina de gestión de riesgos.

- Todos los equipos de cómputo de usuarios final deben contar con software de seguridad habilitado y con bases de firmas actualizadas.

- Ante ataques por *malware*, la Vicepresidencia de tecnología y la Oficina de gestión de riesgos son responsables de la contención y remediación, considerando las actividades de recuperación necesarias.

SEGURIDAD EN OPERACIONES

Respaldo de información

Objetivo

Contar con copias de respaldo de información de las aplicaciones y las bases de datos que soportan las operaciones.

Alcance y responsables

- Vicepresidencia de tecnología

Referencias asociadas

- Proceso ***Gestión de infraestructura tecnológica***

- La Vicepresidencia de tecnología es la responsable de generar y mantener los respaldos de información que soportan la operación de las líneas de la CCB, de acuerdo con lo definido en la caracterización del proceso ***Gestión de Infraestructura tecnológica***, considerando las condiciones para su realización, retención y protección.

- Los respaldos de información deben tener un proceso periódico de realización basado en el análisis de criticidad de la información y los requerimientos de recuperación dados desde continuidad de negocio.

- Los respaldos de información deben tener un proceso de validación, con el fin de garantizar que no han sufrido ningún deterioro y que se podrán utilizar en el momento en que se requieran para recuperar información.

- Los *backups* en medios magnéticos, cartuchos, y discos utilizados para mantener los respaldos, deben mantenerse almacenados bajo condiciones ambientales de temperatura y humedad que permitan conservar la información. Las copias deben estar almacenadas externamente garantizando que cualquier evento adverso que afecte físicamente las sedes de procesamiento de información de la CCB no vaya a afectar las copias de respaldo.

SEGURIDAD EN OPERACIONES

Gestión de vulnerabilidades técnicas

Objetivo

Establecer los requisitos para gestionar las vulnerabilidades técnicas sobre la infraestructura tecnológica.

Alcance y responsables

- Vicepresidencia de tecnología
- Oficina de gestión de riesgos

Referencias asociadas

- N/A

- La Oficina de gestión de riesgos es responsable de identificar las vulnerabilidades técnicas del conjunto de plataformas tecnológicas, de comunicaciones y de seguridad que soporten la operación.

- La Oficina de gestión de riesgos debe elaborar y ejecutar un plan anual de pruebas de vulnerabilidades para las plataformas tecnológicas del negocio cuya viabilidad técnica y de administración lo permita.

- La Vicepresidencia de tecnología es responsable de implementar los planes de remediación que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas.

- La Oficina de gestión de riesgos es responsable de la supervisión sobre la implementación de los planes de remediación.

- La implementación de los planes de remediación debe considerar la definición de responsables de su aplicación, y tiempos límites de subsanación (según la criticidad que se determine para la vulnerabilidad), las condiciones de negocio, así como limitaciones tecnológicas.

SEGURIDAD EN OPERACIONES

Restricciones sobre la instalación de software

Objetivo

Controlar la instalación de software no autorizado en los equipos de cómputo y sobre plataforma tecnológica.

Alcance y responsables

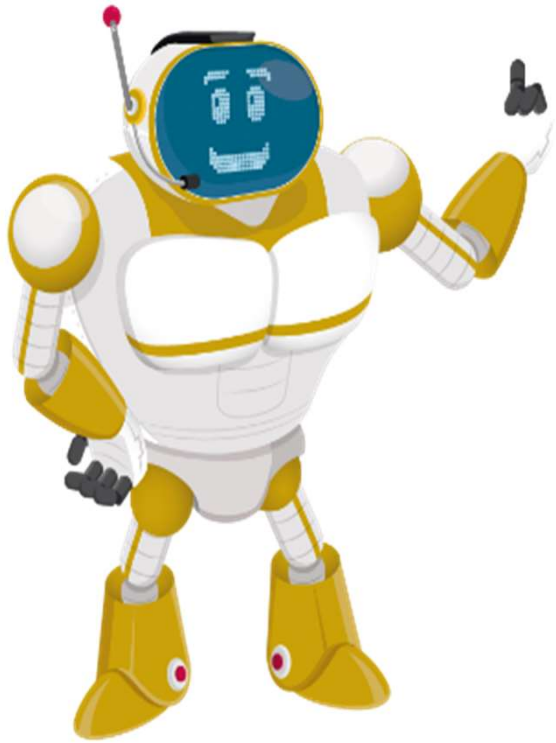
- Vicepresidencia de tecnología
- Colaboradores
- Oficina de gestión de riesgos

Referencias asociadas

- N/A

- El software que emplee la CCB para el desarrollo de sus actividades debe ser legal y contar con licencia de uso.
- Es responsabilidad de la Vicepresidencia de tecnología validar que el software instalado en los equipos de cómputo y servidores sea original y debidamente licenciado. En los casos en que el software sea de distribución libre, esta condición deberá ser verificada y autorizada previamente.
- Se prohíbe la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por la Vicepresidencia de tecnología.
- La Vicepresidencia de tecnología debe establecer cuál es el software autorizado en la Entidad y validar su implementación en los equipos de cómputo y servidores.
- La Oficina de gestión de riesgos puede validar la legalidad del software de acuerdo con los requerimientos del negocio.

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



CRIPTOGRAFÍA

Lineamiento General

Definición, implementación y alcance

Con el fin de proteger la confidencialidad, integridad, autenticidad y no repudio de la información, la CCB establece el uso de protocolos y controles criptográficos para transferencia de información, enlaces de comunicaciones y acceso remoto.

La administración de claves criptográficas y certificados digitales estará a cargo de la Vicepresidencia de tecnología.

Prácticas que soportan el lineamiento

Controles criptográficos

CRIPTOGRAFÍA

Controles criptográficos

Objetivo

Establecer los requisitos para el uso de criptografía como control de Seguridad de la Información.

Alcance y responsables

- Vicepresidencia de tecnología
- Oficina de gestión de riesgos

Referencias asociadas

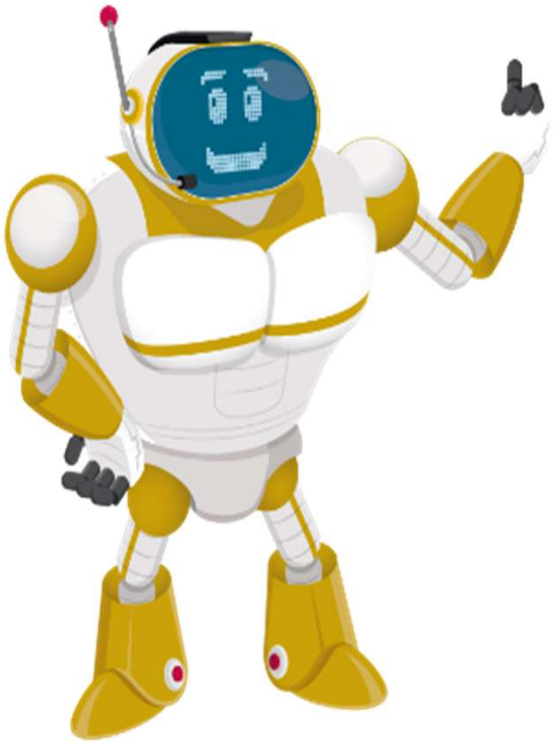
- N/A

- Las herramientas utilizadas para implementar protocolos y controles criptográficos deben estar incluidas en el listado de software autorizado. No está autorizado el uso de herramientas o mecanismos de cifrado de información diferentes a los autorizados por la Vicepresidencia de tecnología.

- Los datos de autenticación en el software desarrollado por o para la CCB deben cifrarse. Se deben utilizar algoritmos de cifrado de datos cuando la Vicepresidencia de tecnología y la Oficina de gestión de riesgos analicen y lo consideren necesario.

- La Oficina de gestión de riesgos es la responsable de validar que el uso de algoritmos de criptografía consideren los estándares de seguridad del mercado basado en el análisis de vulnerabilidades al respecto para el momento en que se requiera su implementación; para lo cual la Vicepresidencia de tecnología al momento de realizar su implementación debe consultar a la Oficina de gestión de riesgos.

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN



SEGURIDAD Y CONTINUIDAD DE NEGOCIO

Lineamiento General

Definición, implementación y alcance

La CCB cuenta con prácticas referentes a la continuidad de las operaciones críticas a partir de la planificación, implementación, revisión y evaluación de actividades de contingencia, continuidad y recuperación. Como parte de continuar operando ante un evento adverso que interrumpa las operaciones, se establecen los requerimientos de continuidad para el proceso de ***Gestión de Seguridad de la Información*** de la Entidad con el fin de mantener los niveles mínimos de seguridad para el negocio ante un evento de interrupción.

Prácticas que soportan el lineamiento

SEGURIDAD Y CONTINUIDAD DE NEGOCIO

Gestión de la continuidad para la Seguridad de la Información

Objetivo

Determinar los requisitos de continuidad a nivel de Seguridad de la Información en eventos de interrupción.

Alcance y responsables

- Vicepresidencia de tecnología
- Oficina de gestión de riesgos

Referencias asociadas

- N/A

- Los sistemas, aplicativos e infraestructura de Seguridad de la Información críticos de la Entidad deben contar con una estrategia de contingencia y/o continuidad para continuar operando en caso de un evento de interrupción que afecte la CCB.

- El plan para la recuperación ante desastres (DRP) debe considerar la infraestructura de Seguridad de la Información (*firewalls*, herramientas de monitoreo, sistemas de autenticación, entre otros) que permita que sistemas y equipos de cómputo críticos puedan estar operativos en la eventualidad de un desastre.

- Es responsabilidad de la Oficina de gestión de riesgos y de la Vicepresidencia de tecnología la inclusión de la infraestructura tecnológica de Seguridad de la Información en el DRP.

- Las pruebas sobre el DRP deben incluir la infraestructura tecnológica de Seguridad la Información, siendo realizadas periódicamente. Su planeación será realizada por la Vicepresidencia de tecnología con el monitoreo por la Oficina de gestión de riesgos.

CONTACTO CON LAS AUTORIDADES Y GRUPOS DE INTERÉS

La CCB establece y mantiene una relación cercana con entidades del Sistema Distrital de Prevención y Atención de Emergencias (SDPAE), así como con grupos de interés o foros de especialistas en Seguridad de la Información, para que puedan ser contactados de manera oportuna en caso de que se presente un incidente de Seguridad de la Información.

Los grupos de interés son los siguientes:

- **CCOC**: Comando Conjunto Cibernético
- **ColCert**: Grupo de Respuesta a Emergencia Cibernéticas de Colombia. www.colcert.gov.co
- **CSIRT**: Centro de Coordinación Seguridad Informática Colombia. www.csirt-ccit.org.co
- **Centro Cibernético Policial (CAI Virtual)**: Ciberseguridad en Colombia comandado por la Policía Nacional. www.policia.gov.co
- **MINTIC**: Ministerio de las Tecnologías y las Comunicaciones www.mintic.gov.co

VIGENCIA Y ACTUALIZACIÓN

La actualización de los lineamientos y prácticas de Seguridad de la Información es responsabilidad del **Gerente de planeación e innovación y el Jefe de gestión de riesgos** con la debida aprobación del Comité de seguridad de la información y se realizará anualmente o ante requerimientos de cambio.

En las revisiones periódicas se deben tener en cuenta factores como:

- Requerimientos de ley
- Mapa de riesgos de la Entidad
- Incidentes de Seguridad de la Información
- Nuevas vulnerabilidades detectadas
- Cambios en la infraestructura organizacional y/o tecnológica
- Cambios en la estrategia, objetivos y/procesos de la Entidad.

La versión oficial de este documento será la que se encuentre publicada y aprobada en el sistema de información de gestión.