OBJETIVO

Establecer las políticas generales a contemplar en el uso de los recursos y servicios de tecnologías de Información y Comunicaciones, para asegurar la integridad y disponibilidad de la infraestructura tecnológica, garantizar la seguridad digital y la confidencialidad e integridad de la información y mitigar riesgos de incidentes cibernéticos o filtración de datos personales o sensibles, en la Caja de Compensación Familiar de la Guajira.

ALCANCE

Aplica para la protección de la información generada, procesada y almacenada de forma electrónica y digital en los diferentes sistemas de información que soportan los procesos misionales de la corporación y las prácticas en cuanto a manejo de la información en toda la organización por parte de las partes interesadas.

DEFINICIONES

- **Activo**: Cualquier cosa que tenga valor para la organización (información).
- **Confidencialidad**: La propiedad que un activo esté disponible y no sea divulgado a personas, entidades o procesos no autorizados**.**
- **Integridad**: Propiedad de salvaguardar la exactitud e integridad de los activos.
- **Datos personales:** Son toda aquella información que se relaciona con nuestra persona y que nos identifica o nos hace identificables. Nos dan identidad, nos describen y precisan: Nuestra edad. Domicilio
- **Disponibilidad**: La propiedad de un activo de estar disponible y utilizable cuando lo requiera una persona, entidad o proceso autorizados.
- **Evento de seguridad de la información**: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.
- **Incidente de seguridad de la información**: Un solo, o una serie, de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer los procesos y amenazan la seguridad de la información.
- **Usuario**: Persona que usa una cosa con cierta limitación.
- **Cuenta de usuario**: Una instancia que permite identificar al usuario de un sistema informático para hacer uso del mismo.
- **Servidor**: Unidad informática que proporciona diversos servicios a computadoras conectadas con ella a través de una red.
- **Disponibilidad de la información:** La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.
- **Hábeas Data:** Recurso legal a disposición de todo individuo que permite acceder a un banco de información o registro de datos que incluye referencias informativas sobre sí mismo.

- **Integridad:** Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento los cuáles deben ser exactos.
- **Información**. Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.
- **Información pública reservada**. Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
- **Incidente de Seguridad:** Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad.
- **Malware:** El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicaciones populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.
- **Protección de datos personales:** Disciplina jurídica frente al peligro que supone la colección y el empleo indiscriminado de datos personales, entendiendo como semejantes a toda aquella información que es parte integrante de nuestra esfera privada y que puede ser usada para valorar ciertos aspectos de nuestra personalidad
- **Seguridad de la información:** Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información.
- **Servicio:** Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.
- **Sistemas de Información:** Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

CONTENIDO

CONTENIDO

CONTENIDO

1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

En COMFAGUAJIRA consideramos la información como un activo indispensable para la operación de los procesos y la prestación de los servicios a nuestros afiliados, por tal motivo nos comprometemos a proteger la información bajo los términos de confiabilidad, disponibilidad e integridad, acorde con la normatividad legal vigente aplicable y las buenas prácticas de seguridad de la información.

A través de esta política Comfaguajira se compromete a:

- Promover y orientar una cultura corporativa desde la alta dirección, enfocada a la protección de la información y su seguridad.
- Evaluar y proponer estrategias y mecanismos de control para el tratamiento de riesgos que afecten los activos de información de la corporación y apoyen la continuidad de las operaciones.
- Promover la mejora continua en materia de gestión de la seguridad de la información de la corporación y tomar las acciones pertinentes de manera oportuna.

2. MARCO LEGAL Y NORMATIVO.

La normatividad legal vigente aplicable en temas de seguridad se tiene identificada y controlada conforme a los lineamientos establecidos en el procedimiento elaboración y revisión de documentos legales GJU-PTO-003, quien establece como instrumento de control la matriz de requisitos legales del área de gestión de la tecnología GTI-DES-003.

3. POLÍTICAS GENERALES Y ESPECÍFICAS APLICADAS A LA SEGURIDAD DE LA INFORMACIÓN.

Estas políticas se conforman de una serie de pautas sobre aspectos específicos de la Seguridad de la Información que incluyen los siguientes criterios:

- Gestión de activos.
- Control de acceso.
- Criptografía.
- Seguridad física y del entorno.
- Seguridad de las operaciones.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Seguridad en el recurso humano.
- Relación con proveedores.
- gestión de incidentes de la seguridad de la información.
- Aspectos de la seguridad de la información.
- Cumplimiento.

CONTENIDO

4. EXCEPCIONES.

Las excepciones a cualquier cumplimiento de Política de Seguridad de la Información deberán ser aprobadas por la alta dirección. Todas las excepciones a la Política deben ser formalmente documentadas.

5. SANCIONES PREVISTAS POR INCUMPLIMIENTO

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido, determinado por el reglamento interno de trabajo y el procedimiento de cargos y descargos para funcionarios y el procedimiento de acciones judiciales para el caso de terceros.

6. ORGANIZACIÓN DE LA SEGURIDAD.

6.1. RESPONSABILIDADES DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CORPORATIVA.

a) **De la Alta Dirección:** Conformado por el Comité de buen gobierno en cabeza del director administrativo, le proceden las siguientes responsabilidades:

- Facilitar los recursos necesarios para el funcionamiento y mejora de la seguridad de la información
- Asignar las responsabilidades en materia de seguridad de la información.
- Participar en el proceso de revisión por la dirección.

b) **Del responsable de la Seguridad de la Información:** El responsable de la Seguridad de la Información tendrá las siguientes responsabilidades:

- Velar por la efectiva implantación de las medidas de seguridad seleccionadas.
- Detectar necesidades de formación y emprender las acciones adecuadas.
- Mantener actualizados los elementos que dan soporte a la seguridad de la información

c) Del Responsable de Sistemas: El responsable de sistemas tendrá entre sus responsabilidades:

- Implantar las medidas de seguridad seleccionadas para mitigar los riesgos.
- Supervisar el funcionamiento de los activos de información y de las medidas de seguridad aplicadas sobre los mismos.

d) Del personal: El personal de toda la corporación tendrá las siguientes responsabilidades:

- Respetar y seguir las normas y procedimientos definidos en el manual de políticas de seguridad de la información.
- Hacer un buen uso de los activos de la organización.

- Respetar la legislación y regulación vigentes.
- Notificar al responsable de seguridad de las anomalías o incidentes de seguridad, así como las situaciones sospechosas.

e) Del Comité técnico de Seguridad de la Información: Objetivos del Comité Técnico de Seguridad de la Información:

- El Comité Técnico de Seguridad de la Información será el órgano colegiado de la Corporación, responsable de gestionar las actividades en materia de seguridad de la información.
- Este Comité será responsable de analizar y preparar propuestas en los temas de su competencia, para someterlos a aprobación del director y del Comité de Buen Gobierno.

Integrantes

El Comité Técnico de Seguridad de la Información estará conformado por los siguientes miembros permanentes, con voz y voto:

- El Subdirector de Gestión Estratégica y Tecnológica.
- El Jefe de la Oficina Administrativa, o su delegado.
- El Jefe de la Oficina Jurídica, o su delegado.
- El Jefe del Departamento de Sistemas, o su delegado.
- El Jefe del equipo de Gestión de la Calidad, o su delegado.
- El jefe del equipo de Riesgos formará parte de este Comité, en calidad de miembro permanente, con voz pero sin voto.

Cualquier líder de procesos de la Caja, podrá participar en el Comité, en calidad de invitado, con voz pero sin voto, de acuerdo con el tema a tratar.

Funciones del comité de seguridad de la información

- Proponer políticas, proyectos y mejores prácticas, relacionadas con la Seguridad de la información, someterlas a consideración del Comité de Buen Gobierno y verificar e informar sobre su ejecución o cumplimiento.
- Revisar periódicamente informes de eventos e incidentes relacionados de la seguridad de la información.
- Evaluar y proponer estrategias y mecanismos de control para el tratamiento de riesgos que afecten los activos de información de la corporación.
- Proponer soluciones a los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables de procesos y/o entre diferentes áreas de la Organización.
- Definir y solicitar a la Dirección Administrativa, los recursos necesarios para respaldar las iniciativas para mejorar la seguridad de la información.
- Promover la mejora continua en materia de gestión de la seguridad de la información de la corporación y

Proponer planes y programas para mantener la concientización del personal de la empresa en estos temas.

- Proponer y actualizar las Políticas y Procedimientos de seguridad de la información.
- Informar regularmente del estado de la seguridad de la información al Comité de Buen Gobierno.
- Proponer convenios con especialistas en seguridad de la información para recibir asesoría.

Funciones de la Presidencia

- Presidente del Comité Técnico de Seguridad de la Información será el responsable de la ejecución de las gestiones relacionadas con la seguridad de la información.
- Será el vocero del Comité Técnico de Seguridad de la Información, ante la Alta Dirección y los órganos de Control (Dirección Administrativa, Comité de Buen Gobierno, Consejo Directivo, Comité de Auditoría, Revisoría Fiscal y Auditoría Interna).
- Designará a la persona responsable de ejercer la Secretaría del Comité, de entre los miembros del mismo.

Funciones de la Secretaría del Comité:

La Secretaría de este Comité será responsable de:

- Coordinar las actividades y reuniones del Comité Técnico de Seguridad de la información.
- Coordinar y solicitar a la Secretaría del Comité de buen gobierno, la inclusión de los temas de seguridad de la información, en la agenda de trabajo de este último, cuando se considere conveniente.
- Elaborar y custodiar las actas de las reuniones.

Reuniones

- El Comité Técnico de Seguridad De La Información se reunirá libremente, de acuerdo con la necesidad de tratar los temas de su competencia, por solicitud de cualquiera de sus miembros, mediante convocatoria de la Presidencia a través de la Secretaría.
- De todas las reuniones se realizarán actas.

7. POLÍTICAS.

7.1. GESTIÓN DE ACTIVOS.

Los activos de la corporación relacionados con la información deben estar inventariados y clasificados con el fin de identificar los riesgos asociados y definir controles efectivos que eviten su pérdida o fuga.

7.1.1. Responsabilidad sobre los activos.

a. Inventario de activos.

CONTENIDO

- Los activos de información de la corporación deben ser relacionados en un inventario de activos corporativos.
- El inventario de los activos de información tipo tecnológico se revisará como mínimo 1 vez año, por parte del departamento de Sistemas.

b. Propiedad de los activos.

- A cada activo de información se le debe asignar un propietario, el cual autorizará las acciones requeridas sobre este activo.
- La información contenida dentro de cada equipo de cómputo es propiedad de Comfaguajira. Ningún archivo tendrá carácter personal.
- A cada activo de información se le debe asignar un custodio el cual velará por salvaguardar el acceso al activo.

c. Uso aceptable de los activos.

- Todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de Comfaguajira, son responsables de cumplir y acoger con integridad la presente política de uso aceptable de los activos y recursos para dar un uso racional y eficiente los recursos asignados.
- Los activos de información podrán ser utilizados para la ejecución de funciones o responsabilidades contractuales de los colaboradores o terceros que dentro de su vínculo contractual lo requiera.
- Los trabajadores deben utilizar los recursos tecnológicos provistos por la organización.
- Los activos de información provistos por Comfaguajira solo deben ser utilizados para los fines establecidos en el vínculo contractual.
- En los dispositivos físicos está prohibido el almacenamiento de música, videos, fotos y demás archivos los cuales no tengan relación con las funciones del cargo.

d. Devolución de activos

- Todo colaborador o tercero que tengan en su posesión o responsabilidad un activo de información deberá devolver una vez termine su vinculación con la organización.
- En el momento en que un colaborador o tercero se desvincule de la empresa, el propietario del activo de información debe retirar todo permiso o propiedad sobre él.
- En caso de que se autorice el uso externo de un activo, este debe ser devuelto de acuerdo con la finalización de la actividad autorizada.
- Para los activos que deban disponerse se tiene en cuenta lo dispuesto en el procedimiento de baja de activos fijos de la Corporación.

CONTENIDO

7.1.2. Clasificación de la información.

a) Metodología de clasificación de activos.

Para asegurar que los activos de información reciben el nivel de protección adecuado, el proceso de gestión documental es responsable de definir la metodología de clasificación de activos de información, estos se deben clasificar según la necesidad, las prioridades y el grado de protección esperado en el manejo de estos.

b) Directrices de clasificación.

Todo activo de información inventariado debe ser clasificado según su confidencialidad, disponibilidad e integridad, lo anterior partiendo de su valor, requisitos legales, sensibilidad y criticidad de la corporación. Partiendo de la confidencialidad se debe clasificar en información pública reservada, información pública clasificada, información pública. Seguidamente para la disponibilidad se debe clasificar en alta, media y baja. Por último, con respecto a su integridad se clasifica en alta, media o baja.

c) Etiquetado y manipulado de la información.

- Los colaboradores que crean o actualizan información son los responsables de escoger la clasificación apropiada de la información y etiquetarla. Esta etiqueta debe ser consistente con las decisiones tomadas por áreas productoras de la información. La etiqueta aplicada debe también ser consistente con los estándares de clasificación de datos de la entidad y la creación del tipo documental debe ser comunicada al proceso de gestión documental.

- La elaboración de copias adicionales, o la impresión de copias extras de información pública reservada, información pública clasificada, no se debe realizar sin el permiso anticipado del propietario de la información.

7.1.2.1. Manipulación de activos.

- Con anterioridad a enviar cualquier información pública reservada o pública clasificada a terceros para copiar, imprimir, formatear, o cualquier otro manejo, los terceros deben firmar con la entidad acuerdos de no divulgación.

- La información pública reservada o pública clasificada enviada por el correo electrónico debe remitirse como Confidencial.

- El documento con información pública reservada se debe enviar por correo certificado o por mensajería de

confianza según los lineamientos del proceso de gestión documental.

- Los funcionarios que custodian la información pública reservada de la entidad deben asegurar que esos materiales no están disponibles para personas no autorizadas.

7.1.3. Manejo de los soportes de almacenamiento

a) Gestión de soportes extraíbles.

- Los funcionarios no deben almacenar información pública reservada o pública clasificada, en medios de almacenamiento como USB, discos duros externos u otros medios de almacenamiento removible.
- El uso de los dispositivos de almacenamiento extraíbles dentro de la organización dependerá de la necesidad del cargo o quehacer diario, para dicho uso el líder del proceso debe solicitar al departamento de sistemas la habilitación de los puertos del PC a cargo del colaborador, que por defecto deben estar deshabilitados.
- Todo soporte de almacenamiento extraíble debe ser correctamente removido del computador.

b) Eliminación de soportes.

- Toda aquella información contenida en un mecanismo de almacenamiento debe ser borrada del dispositivo una vez se tenga la autorización del propietario que dicha información no se volverá a utilizar.
- A los equipos que se dan de baja se debe hacer un borrado de información segura, de manera que esta no sea recuperable, con el fin evitar divulgar información pública reservada y clasificada de la corporación.

7.2. CONTROL DE ACCESO.

Definir el acceso a la información es fundamental para su seguridad, por lo anterior es importantes establecer medidas de control con el objetivo de monitorear y controlar los accesos a los medios de información teniendo en cuenta la estructura organizativa.

7.2.1. Requerimiento del negocio para el control del acceso.

a) Política de control del acceso

- El Departamento de Sistemas establecerá los criterios para controlar la definición de perfiles y la asignación de derechos de acceso a los usuarios. Dichos criterios deben cubrir todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación del registro a quienes no necesiten el acceso. Se debe brindar atención y seguimiento especial, donde sea apropiado, a la necesidad del control de asignaciones de accesos privilegiados.
- Separación de las Políticas de acceso de información específica: solo se asignarán usuarios y contraseñas a los nuevos trabajadores y a aquellos que hayan cambiado de cargo o funciones de forma temporal o permanente,

de acuerdo a la información relacionada en su respectivo perfil del cargo, con el nivel de acceso correspondiente.

7.2.2. Gestión de acceso del usuario

a) Registro del usuario

- Requerimiento de Identificación válida para el uso del sistema: Todos los usuarios deben estar identificados y validados antes de poder usar recurso de tecnología por medio de sus credenciales de acceso.
- Usuario y Contraseña requerido para conectarse al computador de la red: Todos los usuarios deben tener su identidad verificada mediante un usuario y una contraseña
- Requerimiento de Usuario único y de password: Todos los usuarios deben tener un usuario único y una contraseña secreta. Este usuario y contraseña serán requeridos para tener acceso a los recursos de tecnología de la Corporación.
- Mensajes de advertencia de seguridad en el sistema de acceso: Todo proceso de logeo para computadores debe incluir una advertencia especial. Esta advertencia debe indicar: (1) el sistema es para ser usado solamente por usuarios autorizados, y (2) el continuo uso del sistema por el usuario indica que el / ella es un usuario autorizado.
- Prohibición de sesiones simultáneas múltiples en línea: A menos que se tenga un permiso especial concedido por el administrador del sistema, los sistemas del computador no deben permitir que ningún usuario maneje simultáneamente sesiones múltiples cuando esté en línea.
- Uso personal del computador y sistemas de comunicación: Los computadores de la Caja y los sistemas de comunicación deben usarse solamente para asuntos de negocios o actividades exclusivas de la Corporación. Se permite su uso para fines personales por solicitud del jefe inmediato del colaborador. El uso personal ocasional puede permitirse si : (a) no se consume más que una cantidad mínima de los recursos que podrían, en otra forma, usarse para asuntos de negocios, (b) no interfiere con la productividad del trabajador, y (c) no se apropia de ningún tipo de actividad comercial.
- Usos permitidos de información de la entidad: La información de la empresa debe usarse solamente con fines comerciales expresamente autorizados por la Corporación.
- Los permisos de acceso a los sistemas de información se terminan cuando el colaborador se retira de la entidad: Todos los permisos de acceso para el uso de los sistemas de información de la empresa deben terminar inmediatamente después de que el colaborador o el contratista cesa de prestar sus servicios a la Corporación.
- Transferencia de las tareas una vez el funcionario deja su cargo: Cuando un colaborador deja su cargo con la Caja, tanto los archivos digitales como los de papeles, los debe recibir el jefe inmediato, para determinar a quién se los asigna, delegando específicamente la responsabilidad sobre ellos.

b) Gestión de privilegios

CONTENIDO

- Restricción privilegiada basada en la necesidad de saber: El computador y los privilegios del sistema de comunicación de todos los usuarios, sistemas, y programas deben ser restringidos basados en la necesidad de saber, relacionados a la función a desarrollar dentro de su cargo.
- Restricción de privilegios especiales del sistema: El uso de perfil administrador en los recursos tecnológicos debe ser exclusivo del Departamento de sistemas.
- Gestión inapropiada y revocación de privilegios de acceso: El Departamento de Sistemas se reserva el derecho de revocar los privilegios de cualquier usuario en cualquier momento. No se permitirá que la gestión que interfiera con el funcionamiento normal y apropiado de los recursos tecnológicos de la entidad.
- Privilegios para modificar la información generada en los procesos en el ambiente de producción: Los lideres funcionales de cada sistema de información son los encargados de otorgar privilegios de modificación de la información generada en el ambiente de producción, para preservar la integridad de la información y ejecutándose en forma controlada.
- Actualización de datos en el ambiente de producción para áreas de soporte o control: Los privilegios definidos en el sistema de información para el personal que no pertenezca al proceso de responsable de la información, será con perfil de consulta únicamente. (auditores internos, administradores de seguridad de información, programadores, operarios del computador, etc.) no se les permitirá modificar directamente los datos en el ambiente de producción.
- Privilegios del personal del departamento de sistemas en los sistemas en producción: Los privilegios del Departamento de Sistemas en los sistemas de información, serán del perfil de seguridad (administración de usuarios), no es permitido realizar transacciones de los procesos.
- Separación de actividades y datos de usuario-a-usuario: El líder de cada proceso debe definir los privilegios del usuario para que usuarios comunes no puedan lograr acceso, o de otra forma interferir con actividades individuales o datos privados de otros usuarios.
- Reflejo en los Log de auditoría sobre la actividad de los administradores: Las transacciones realizadas por los usuarios administradores debe quedar registrado en los logs de auditoria

c) Gestión de las claves secretas de los usuarios

- Protección de contraseñas enviadas a través del correo: Los usuarios y contraseñas se deben enviar por medios diferentes, pueden ser correo y chat corporativo y/o mensajería de texto. Esta comunicación no debe tener ninguna marca indicando la naturaleza del contenido.
- Cambio de códigos claves proporcionados por el fabricante (palabras default): Todas las contraseñas de fábrica proporcionadas por el fabricante se deben cambiar antes que la Corporación utilice cualquier sistema de computación o de comunicaciones para sus negocios.
- Entrega de los códigos de identificación de usuarios: Todos los usuarios deben tener en sus contratos laborales firmados, una cláusula de acuerdo con la Caja sobre la confidencialidad con el manejo de la

información y el acatamiento con las normas de seguridad del sistema, se incluye el manejo de los códigos de identificación de usuario para ingresar a los sistemas de la Corporación.

d) Revisión de los derechos de acceso del usuario

- Revisión periódica y reevaluación de los privilegios de acceso del usuario: El Departamento de Sistemas en conjunto con los líderes funcionales de los sistemas de información debe reevaluar el otorgamiento de los privilegios del sistema a todos los usuarios como mínimo 1 vez al año. Esto se confirmará por acta o comunicación formal.
- Prohibición de la reutilización de códigos de identificación de usuario en los sistemas de información: Cada usuario de acceso en los sistemas de información debe ser único y solamente habilitarse al colaborador que se le fue asignado. Después que un colaborador se retira de la Caja, no se debe volver a usar ninguno de los códigos asignados anteriormente.

7.2.3. Responsabilidades del usuario

a) Uso de claves secretas

- Cambio obligatorio de contraseña al acceder por primera vez el sistema: Los activos de información críticos deben obligar que todos los usuarios cambien sus contraseñas al menos una vez cada 3 meses.
- Control de acceso a la red usuario individuales para cada colaborador: El acceso a cada aplicativo, es responsabilidad plena del usuario que ingresa y que es dueño de las contraseñas, las responsabilidades administrativas, civiles, laborales, sociales y penales recaerán sobre la persona dueña de dicho usuario en caso de su mala manipulación o uso compartido inadecuado.
- Cambio de clave cuando se sospecha o detecte que ha sido descubierta: Todas las contraseñas se deben cambiar tan pronto como se sospeche o detecte que han sido descubiertas o que podrían conocerlas personas no autorizadas.
- Cambios de contraseñas después del mantenimiento a un computador o un sistema de información: Una vez finalizado el mantenimiento preventivo y/o correctivos el usuario debe cambiar la contraseña de acceso a la red.
- Escribir contraseñas (passwords) y dejarlas en donde otros pueden descubrirlas: No se deben escribir las contraseñas (passwords) y dejarlos en lugares donde personas no autorizadas pueden descubrirlos o usarlos.
- Escribir passwords usando técnicas secretas: Los usuarios no deben escribir sus passwords al menos que: (1) ellos hayan realmente ocultado estos passwords en un número de teléfono o con otros caracteres aparentemente no relacionados, o (2) que ellos hayan usado un sistema de código propio para ocultar el password.
- Prohibición de contraseñas (passwords compartido): No importa las circunstancias, las contraseñas (paswords) nunca deben ser compartidas o reveladas a nadie más que al usuario autorizado. Al hacerlo el usuario autorizado se responsabiliza de las acciones que otras personas hagan con la contraseña. Si los

usuarios necesitan compartir información permanente del computador, ellos deben usar correo electrónico, carpetas o recursos compartidos en la red u otras herramientas colaborativas autorizadas

- Usuarios responsables de todas las actividades involucrando su código de identificación de usuario: Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario. Los códigos de identificación de usuario no pueden ser utilizados por nadie más, sino por aquellos a quienes se les ha expedido. Los usuarios no deben permitir que otros realicen ninguna actividad con sus códigos de identificación de usuario. Asimismo, se les prohíbe a los usuarios que realicen cualquier actividad con códigos de identificación de usuario que pertenezcan a otros usuarios.
- No se deben almacenar ni usar juegos y/o aplicaciones de entretenimiento en los computadores de la entidad: No deben almacenarse, ni usarse juegos y/o aplicaciones de entretenimiento en ninguno de los computadores de la Corporación.
- Códigos de identificación de usuarios que identifiquen únicamente a un usuario en particular: El software contenido en cada computador o sistema de comunicación es responsabilidad de su dueño asignado, tanto los aplicativos como el sistema operativo y computador están registrados en el control de inventarios.

b) Equipo del usuario desatendido.

- Proceso automático de Log-Off: Si no ha habido actividad en un computador durante 10 minutos, el sistema automáticamente debe bloquear y suspender sesión. El restablecimiento de la sesión debe hacerse solamente después de que el usuario haya proporcionado la contraseña.
- Abandonar los sistemas sensitivos sin ejecutar cierre de sesión: Si el sistema del computador al cual los usuarios están conectados contiene información sensible o valiosa, éstos no deben abandonar el computador (PC) sin hacer primero el cierre de sesión.
- Log-Off de los computadores personales conectados a las redes: Si los computadores están conectados a una red, cuando no estén en uso deben siempre tener la sesión cerrada o bloqueada (ctr+alt+supr)

c) Política de escritorio y pantalla limpios

- Visualización de contraseñas: Las contraseñas en pantalla, impresas o manuscritas no se deben visualizar, esto con el fin de evitar que personas no autorizadas las puedan observar o recuperarlas.
- Los usuarios deberán tener los escritorios físicos y virtuales limpios y evitar la disposición de información corporativa que puedan ser accedida por personas no autorizadas.

7.2.4. Control de acceso a la red.

CONTENIDO

Las conexiones no seguras a los servicios de red pueden afectar a toda la empresa, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos. Las reglas de acceso a la red a través de los puertos, estarán basadas en la remisa "todo está restringido, a menos que este expresamente permitido".

a) Uso de los servicios de la red.

- Indicación de pautas para un usuario-ID particular usando todas las plataformas: Los funcionarios de la Caja deben solamente tener un código de identificación de usuario para el acceso al dominio y al correo corporativo, está relacionado con el cargo. Para los accesos a los sistemas de información el estándar de acceso se establece por medio de documento de identidad del colaborador.
- Permisos restrictivos para accesos a los recursos tecnológicos: Los permisos de control de acceso a los recursos de tecnología de la Caja deben fijarse de manera restrictiva para poder bloquear el acceso a usuarios no autorizados.

b) Autenticación del usuario para las conexiones externas.

- La conexión entre sistemas internos de la empresa y otros de terceros debe ser explícitamente aprobada y certificada por el departamento de sistemas
- En la autenticación de usuarios para conexiones externas el Departamento de Sistemas contempla como servicios de conexiones externas SSL, VPN y primarios para funcionarios que requieran conexión remota a la red de datos institucional.
- Conceder acceso a los recursos de tecnología a usuarios externos desconocidos: No se puede conceder, o dar cierto tipo de prerrogativas al acceso a los recursos tecnológicos de la Caja a personas que no tengan ningún vínculo laboral o comercial con la Corporación, que no sean empleados, contratistas, o consultores, a menos que primero se obtengan la aprobación por escrito del supervisor del contrato y del Administrador y/o Encargado del Sistema de Información.

c) Identificación del equipo en las redes.

- Administración para todos los computadores de la red: Las configuraciones y parámetros instituidos para todos los equipos adscritos a la red de la Caja, deben cumplir con las políticas y normas sobre el manejo administrativo, operativo y de control de las seguridades en tecnología de información.

d) Protección del puerto de diagnóstico y configuración remoto

- Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, estará restringido a los administradores de red o servidores.

- Los usuarios finales deberán permitir tomar el control remoto de sus equipos para el área de soporte técnico, teniendo en cuenta, no tener archivos con información sensible a la vista, no desatender el equipo mientras que se tenga el control del equipo por un tercero.

e) Segregación en redes.

- Organizar recursos de información en segmentos de acuerdo a su prioridad de recuperación o disponibilidad: El departamento de sistemas debe establecer un esquema lógico para segmentar los recursos de información de acuerdo a su prioridad de recuperación o disponibilidad, esto permitirá recuperar primero los recursos más críticos.

f) Control de conexión a la red

- El Departamento de Sistemas controlará e identificará los equipos conectados a su red, mediante el uso de controladores de dominio, asignación manual de IP y portal cautivo para la conexión WIFI.
- Sincronización del reloj para un Log adecuado de eventos en la red: Todas los computadores multi-usuarios conectados a la red interna de la Caja deben tener la hora exacta reflejada en el reloj interno, esta debe estar sincronizada con la hora legal colombiana, http://horalegal.inm.gov.co/

g) Control de routing de la red.

- La conexión remota a la red de área local de Comfaguajira debe ser hecha a través de una conexión VPN segura suministrada por el Departamento de Sistemas.
- La creación de las VPN se realizará por autorización de jefe inmediato del colaborador, el cual debe definir el acceso al sistema información requerido y durante que tiempo se le otorgará el permiso.

7.2.5. Control del acceso al sistema operativo.

7.2.5.1. Procedimientos para un registro seguro.

- Límite de intentos consecutivos fallidos para ingresar la contraseña: Después de cinco intentos consecutivos y fallidos de ingreso de la contraseña, el sistema debe suspender el acceso del usuario hasta que el administrador del sistema lo habilite nuevamente o inhabilitarlo temporalmente por lo menos de 1 hora.

a) Identificación y autenticación del usuario.

- Contraseñas con caracteres alfabéticos y no alfabéticos: Todas las contraseñas deben tener al menos un carácter alfabético y uno no alfabético; se consideran caracteres no alfabéticos los números y los signos de

puntuación, no se deben utilizar caracteres de control y otros caracteres no impresos porque involuntariamente pueden causar problemas de transmisión en la red o sin intención llamar ciertos servicios del sistema. La longitud de la clave se recomienda que sea mínimo de ocho (8) caracteres.

- Incorporación de contraseñas dentro del software: Las contraseñas no se deben incorporar dentro de los programas de software, esto para que las claves se pueden cambiar en el momento que sea necesario.
- Las cuentas de correo que se utilizan para envío de correspondencia masiva: Las contraseñas de los correos utilizados para envío de correspondencia masiva se configuran para que no pidan cambio de clave.

b) Sistema de gestión de claves secretas.

- Prohibición para explorar vulnerabilidades de los sistemas de seguridad: Los usuarios no deben explorar vulnerabilidades o deficiencias en la seguridad de los sistemas de información para dañar sistemas o información, para obtener recursos mayores a los que han sido autorizados, para tomar recursos de otros usuarios, o para tener acceso a otros sistemas a los cuales no se les ha otorgado una autorización apropiada. Todas estas vulnerabilidades y deficiencias deben ser reportadas inmediatamente al Departamento de Sistemas. La protección de la información y de los datos se regulará mediante la aplicación de ley colombiana 1273 de 2009.
- Capacidades del usuario para el acceso de archivos y su implicación en cuanto al uso: Los usuarios no deben leer, modificar, borrar, o copiar un archivo que pertenezca a otro sin obtener primero permiso del propietario del archivo. A menos que el acceso general haya sido claramente proporcionado, la habilidad para leer, modificar, borrar, o copiar un archivo que pertenezca a otro usuario no implica que el usuario tenga permiso para realizar estas actividades.

c) Uso de las utilidades del sistema.

- Herramientas de seguridad del sistema: Todo sistema multi-usuario debe contener suficientes herramientas automatizadas que ayuden al Departamento de Sistemas en la verificación del estado de seguridad de los sistemas automatizados. Estas herramientas deben contener mecanismos que sirvan para detectar, informar y corregir problemas de seguridad.
- Prohibición para explorar vulnerabilidades de los sistemas de seguridad: Los usuarios no deben explorar vulnerabilidades o deficiencias en la seguridad de los sistemas de información para dañar sistemas o información, para obtener recursos mayores a los que han sido autorizados, para tomar recursos de otros usuarios, o para tener acceso a otros sistemas a los cuales no se les ha otorgado una autorización apropiada. Todas estas vulnerabilidades y deficiencias deben ser reportadas inmediatamente al Departamento de Sistemas. La protección de la información y de los datos se regulará mediante la aplicación de ley colombiana 1273 de 2009.
- Capacidades del usuario para el acceso de archivos y su implicación en cuanto al uso: Los usuarios no deben

leer, modificar, borrar, o copiar un archivo que pertenezca a otro sin obtener primero permiso del propietario del archivo.A menos que el acceso general haya sido claramente proporcionado, la habilidad para leer, modificar, borrar, o copiar un archivo que pertenezca a otro usuario no implica que el usuario tenga permiso para realizar estas actividades.

d) Cierre de una sesión por inactividad

- Inactividad de credenciales de acceso por inactividad: El responsable del procedimiento de infraestructura lógica estará pendiente de la revocación de privilegios para los usuarios que presentan inactividad superior a treinta (30) días, esta revocación puede ser automática o manual.
- Las sesiones de red en las estaciones de trabajo se bloquearán después de 10 minutos de inactividad y su reactivación deberá ser con la contraseña del usuario.

e) Limitación del tiempo de conexión

- Al finalizar la jornada laboral, los trabajadores deben apagar los equipos de cómputo (CPU, Monitores, Portátiles e Impresoras).

7.2.6. Control de acceso a la aplicación y la información

- El control de acceso a la información a través de una aplicación, se realizará a través de roles que administren los privilegios de los usuarios dentro del sistema de información.
- El control de acceso a información física o digital, se realizará teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información

a) Restricción del acceso a la información.

- Responsabilidad por daño a información y a programas por negligencia: La Corporación usa controles de acceso y otras medidas de seguridad para proteger la veracidad, integridad y disponibilidad de la información manejada en los computadores y sistemas de información. Para mantener estos objetivos, la administración tiene la autoridad para: (1) restringir o derogar cualquiera de los privilegios del usuario, (2) inspeccionar, copiar, remover, o bien alterar algún dato, programa, u otro sistema que pueda socavar estos objetivos, y (3) tomar cualquier otra acción que estime necesaria para manejar y proteger sus sistemas de información. Esta autoridad puede emplearse con o sin notificación a los usuarios. La Caja no se hace responsable por pérdida o daño a la información personal o software que resulte de sus esfuerzos para lograr estos objetivos de seguridad de la información corporativa.

CONTENIDO

- Regulación por el control de acceso a los sistemas del software: El acceso a los sistemas de información debe ser controlado desde el inicio de sesión al dominio por medio de la validación de credenciales de acceso, una vez ingresado al dominio deberá ingresar al sistema de información correspondiente con sus credenciales de acceso, los permisos otorgados en estos serán los prevalentes en el sistema de información.
- El acceso no autorizado por medio de los sistemas de información de la entidad: Se prohíbe a los colaboradores que usen los sistemas de información de la Caja, para tener acceso no autorizado a cualquier otro de los sistemas de información o de cualquier forma dañar, alterar, o desbaratar las operaciones de estos sistemas. Del mismo modo se les prohíbe capturar o de otra forma obtener contraseñas, claves encriptadas o cualquier otro mecanismo de control de acceso que pueda permitirles un acceso no autorizado.
- Logs en los sistemas de aplicación que contengan Información sensitiva: Todos los sistemas de aplicación en producción que contengan información sensitiva de la Caja deben generar Logs o evidencias que indiquen cada adición, modificación, borrado de esta información.
- Utilización de los log´s de los sistemas de información: Los archivos de Logs que contienen eventos relevantes de seguridad deben proporcionar suficiente información para apoyar el monitoreo, control y auditorías sobre la efectividad y cumplimiento con las medidas de seguridad implementadas en la Caja.
- Contenido de Logs en los sistemas de aplicaciones en ambiente de producción: Todo software aplicativo habilitado en ambiente de producción de la Caja debe incluir archivos Logs que registren como mínimo la siguiente información:

  - ✔ (1) el usuario que ingreso al sistema
  - ✔ (2) cambios realizados en la información
  - ✔ (3) fecha y hora del cambio.
- Períodos de retención de los Logs: Los Logs que contienen los registros de los eventos relevantes de los diferentes sistemas de información deben retenerse por un periodo mínimo de un año y se estarán sacando copias de forma permanente se acuerdo con la política de copias de seguridad, a esta información solo tendrá acceso el jefe del Departamento de Sistemas y el dueño del procedimiento de infraestructura lógica.
- Información que se sospecha como crimen informático o abuso del Computador: Para proporcionar evidencia en investigaciones y tomar acciones administrativas y de carácter legal, se debe obtener la información necesaria de, los archivos de seguridad “Logs”, los estados del sistema actual y las copias de los archivos (back-up) y de todos los demás potencialmente involucrados, cuando se sospecha que ha ocurrido un crimen informático o abuso en el computador. La información debe custodiarse por el jefe del departamento de Sistemas y/o por el Director de la Caja.
- Personas autorizadas para consultar los Logs: Solo el Departamento de Sistemas debe tener acceso a los Logs de los sistemas de información.
- Revisiones regulares a los Logs del sistema: El administrador del sistema, deben periódicamente revisar los diferentes registros de los Logs con el fin de verificar las violaciones a las seguridades o mal uso de la información en las máquinas multi-usuario y en los sistemas de información, presentando a la administración

informes periódicos de tal comportamiento.

b) Aislar el sistema confidencial.

- Asignación de pertenencia de la información: La administración debe claramente especificar por escrito la asignación de las responsabilidades de pertenencia para bases de datos, archivos principales, y otra información compartida. Estas declaraciones deben también indicar los individuos a quienes se les ha dado autoridad para originar, modificar, o borrar tipos específicos de información encontrada en estos conjuntos.
- Permisos para tener acceso a información delicada no leída: Los colaboradores a quienes se les ha autorizado ver información clasificada de un cierto delicado nivel se les debe permitir el acceso solamente a información a este nivel o a niveles menos delicados.
- Permisos para tener acceso a información delicada no escrita: Los colaboradores nunca deben tener autorización para mover información clasificada de un cierto nivel delicado a un menor nivel a menos que sea parte del proceso aprobado de desclasificación.
- Los usuarios de red con privilegios de administrador son exclusivos para el Departamento de Sistemas y Director Administrativo

7.2.7. Computación y trabajo-remoto móvil.

a) Computación y comunicaciones móviles.

Los colaboradores, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la corporación, tales como escritorios y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros, atendiendo las siguientes directrices:

I. El dispositivo móvil debe estar en el bolsillo, maletín o lugar no visible en partes públicas.

- El dispositivo móvil debe estar configurado para bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como contraseña, patrón huella dactilar, reconocimiento de voz, entre otras.
- Uso de aplicación de antivirus.
- El acceso a servicios de la corporación desde el exterior de la misma debe realizarse según las condiciones seguras determinadas por el Departamento de Sistemas.
- La persona autorizada para acceder a los servicios de la corporación de forma externa o desde un equipo que no pertenece a la corporación, solo debe remitirse a ejecutar las acciones por las cuales está autorizado.
- Uso de canales seguros y cifrados cuando se conecte a redes compartidas de acceso libre, no seguras.

II. Se debe desactivar la opción de autoguardado de contraseñas en los diferentes navegadores web.

- No dejar claves en ningún sistema de almacenamiento de información web.
- Creación de contraseñas seguras, no incluir información personal como nombres, fechas de nacimiento, otros.
- Cerrado de sesión de escritorio virtual cuando no esté en uso.
- Se prestará especial cuidado para asegurar que no se comprometa la información del negocio, teniendo en cuenta los riesgos que conlleva el trabajar con el equipo móvil en entornos desprotegidos. La utilización de los servicios móviles conectados a las redes, debe tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil, sólo debería tener lugar después de la identificación y autenticación exitosa y con el establecimiento de los mecanismos adecuados del control del acceso.

b) Trabajo remoto.

- El trabajo remoto solo será autorizado por el responsable del área a de la cual dependa el funcionario que solicite el permiso.

7.3. CRIPTOGRAFÍA.

Establecer el uso de controles criptográficos es fundamental para garantizar la confidencialidad, autenticidad o integridad de la información. De esta manera es posible proteger claves de acceso a sistemas, datos y servicios.

7.3.1. Controles criptográficos.

a) Empleo de controles criptográficos.

- El Departamento de Sistemas debe verificar los sistemas o aplicaciones que realicen y/o permitan la transmisión de información pública reservada o información pública clasificada (privada o semiprivada), lo realicen mediante herramientas de cifrado de datos.
- El Departamento de Sistemas proveerá la herramienta de encriptación de datos a los usuarios, previa solicitud formal.
- La persona titular de las firmas digitales son las responsables de su custodia y el uso adecuado de esta.
- Las personas titulares de la firma deberán solicitar al departamento de sistemas la renovación de la firma como mínimo 30 días antes de su vencimiento para realizar el trámite ante la entidad encargada.
- Todo sistema de información que maneje información sensible o de protección debe contener las contraseñas encriptadas.

b) Gestión de claves.

- Todo dispositivo con claves criptográficas (Token o firmas digitales) están bajo la responsabilidad del colaborador que lo opera.
- La persona titular de las firmas digitales son las responsables de su custodia y el uso adecuado de esta.

7.4. SEGURIDAD FÍSICA Y DEL ENTORNO.

Establecer controles claros para la seguridad física y del entorno es de vital importancia para minimizar los riesgos de daños e interferencias a la información y a los servicios de la organización.

7.4.1. Áreas seguras.

Se definen las políticas de seguridad física y ambiental para la protección de áreas seguras y controladas que contienen información y las instalaciones de procesamiento de información sensible o crítica, dentro de las cuales se encuentran Computadores, Centro de Datos, Cuarto de UPS, Cableado estructurado y Gabinetes de comunicaciones.

a) Perímetros de seguridad física.

- En el instructivo de control de espacios restringidos se detalla la estructura del perímetro, terrenos circundantes de las instalaciones, entrada al edificio, pisos y corredores de acceso a los pasillos, la descripción de zonas controladas, áreas seguras y las áreas restringidas.
- Las oficinas y las áreas de trabajo que contienen información sensible deben ser físicamente restringidas con un método de control apropiado de acceso mediante ventanas, puertas de seguridad, cerraduras, alarmas, muros, chapas metálicas, vigilancia privada y/o recepcionistas, entre otros; El jefe encargado de cada área determina los niveles de protección del perímetro y los elementos de control a utilizar.
- Las instalaciones de procesamiento de información sensible o crítica deben estar ubicados en áreas aseguradas y restringidas para prevenir manipulaciones, alteraciones y usos no autorizados; protegidos con barreras de acceso físico, monitoreo y vigilancia.
- Los perímetros de seguridad de las áreas seguras y zonas controladas deben ser físicamente sólido, no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una intrusión. Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados.
- Se debe verificar que las puertas y ventanas de las áreas seguras estén cerradas con llave cuando no hay supervisión o estén desocupadas.

CONTENIDO

b) Controles físicos de entrada.

- Se debe controlar el acceso a las áreas en donde se procesa o almacena información sensible y restringir el acceso únicamente a personas autorizadas.
- El acceso a las oficinas de la entidad por parte de visitantes u otras personas a áreas que contengan computadoras y/o información sensible debe estar controlada por vigilantes, recepcionistas u otras personas del área técnica. A los visitantes y demás no se les debe permitir el uso de las entradas de los empleados u otras vías de acceso no controladas a áreas que contienen información sensible.
- Los trabajadores deben portar el carné de identificación en un lugar visible. Para las sedes que cuenten con control de visitantes, estos deberán portar la escarapela en un lugar visible.
- Los distintivos de ingresos de los trabajadores de la entidad perdidos o robados deben ser reportados inmediatamente a la Oficina administrativa. Así mismo las tarjetas RFID, tarjetas inteligentes con contraseñas dinámicas, tarjetas de crédito, etc.) que hayan sido pérdidas o robadas o que se sospeche que hayan sido pérdidas o robadas, deben ser reportados inmediatamente al área responsable de la corporación para su suspensión.
- Los controles de acceso físicos para los edificios de la entidad están restringidos para personal no autorizado. Los colaboradores no deben permitir que personas no autorizadas o desconocidas ingresen a través de puertas, compuertas y otras entradas a áreas restringidas.
- El personal de vigilancia debe establecer mecanismos para inspeccionar y examinar los morrales, bolsos, cajas, etc. de los colaboradores o visitantes que ingresen y salen de las instalaciones.
- Registrar en una bitácora o sistema de información el ingreso y retiro de todo equipo de cómputo, servidores, equipos activos de red, entre otros, en caso de que estos equipos sean propiedad de la organización, deberán contar con orden de salida autorizada por el jefe encargado del área.
- Los derechos de acceso a áreas seguras se deben revisar y actualizar con regularidad y ser revocados cuando sea necesario.

c) Seguridad de oficinas, despachos y recursos.

- Las zonas de acceso controlado deben estar ubicadas de modo que se evite el acceso no autorizado.
- Las oficinas deben ser discretas y no tener indicaciones sobre su propósito, sin señales obvias, fuera o dentro de ellas, que identifiquen la presencia de actividades de procesamiento de información sensible, crítica o confidencial.
- Supervisar las actividades de limpieza en las áreas seguras, especialmente: centro de datos y centros de cableado, brindando las recomendaciones al personal de limpieza acerca de las precauciones mínimas a

seguir durante el proceso de limpieza.

d) Protección contra las amenazas externas y ambientales.

- Se deben aplicar medidas de protección físicas y medioambientales necesarias como sistemas de control ambiental de temperatura y humedad, sistemas de detección de humo, entre otros para certificar la protección y correcta operación de la gestión de la información y de los recursos de la plataforma tecnológica. Estos sistemas se deben monitorear de manera permanente.
- Mantener en buen estado la infraestructura física de los gabinetes de comunicaciones, cableado, centros de datos, y en general de las áreas seguras, tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, sensores, entre otros.
- Se debe asegurar que el centro de cómputo o de cableado, se encuentre separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones o incendios.
- Se deben elaborar e implementar los planes de contingencia, de emergencia y de continuidad del negocio, suministrar equipo apropiado contra incendios y ubicarlo adecuadamente.

e) El trabajo en áreas seguras.

- En las áreas aseguradas y restringidas de tecnología solo se permite el acceso para el desarrollo de operaciones tecnológicas, tareas de aseo (monitoreado por personal del área), almacenamiento de equipos (inactivos), implementación o mantenimiento de los controles ambientales bajo supervisión y autorización previa.
- Las áreas seguras vacías deben tener bloqueo físico y se debe revisar periódicamente.
- Las disposiciones para el trabajo en áreas seguras incluyen controles para los empleados, contratistas.
- Se debe asegurar que las labores de mantenimiento para los centros de cableado y/o cuarto eléctricos sean realizadas por personal idóneo y apropiadamente; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

f) Áreas de acceso público, carga y descarga.

- Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se debe controlar y mantener aislado de los servicios de procesamiento de información para evitar el acceso no autorizado.
- Restringir el acceso al área de despacho y de carga desde el exterior de la edificación únicamente al personal identificado y autorizado.

- Registrar el material que ingresa de acuerdo con los procedimientos de gestión de activos al entrar al sitio.

7.4.2. Seguridad de los equipos

a) Emplazamiento y protección de equipos.

- Se debe asegurar que los equipos de cómputo asignados a los colaboradores cuenten con las condiciones adecuadas para su funcionamiento.
- Se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.
- La protección del equipo, incluyendo el utilizado por fuera, es necesaria para reducir el riesgo de acceso no autorizado a la información y para proteger contra pérdida o daño.
- Los equipos de procesamiento de la información que manejan información sensible y confidencial deben ser ubicados de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso.
- Se deben establecer lineamientos sobre comer, beber y fumar en la proximidad de los equipos de procesamiento de información.

b) Instalaciones de suministro:

- Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.
- Se debe asegurar que la plataforma tecnológica (Hardware, software y comunicaciones) cuente con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.
- Se debe aplicar protección contra rayos en las edificaciones donde se encuentren las áreas aseguradas y restringidas que manejan información sensible o procesamiento de información.
- Todos los servicios públicos de soporte; como electricidad, suministro de agua, desagüe, calefacción/ventilación y aire acondicionado; deben ser adecuados para los sistemas que soportan. Los servicios públicos de soporte deben ser inspeccionados regularmente y, conforme sea apropiado, probados para asegurar su adecuado funcionamiento y para reducir cualquier riesgo por un mal funcionamiento o falla.
- Se recomienda un dispositivo de suministro de energía ininterrumpido (UPS) para garantizar el funcionamiento continuo de las operaciones.
- Se debe asegurar la operación permanente de los servidores alojados en los centros de cómputo, de igual forma proteger la información almacenada en los sistemas de almacenamiento, para que esté segura y

disponible.

c) Seguridad del cableado.

- Se debe proteger contra interceptación, interferencia o daño el cableado de energía y el cableado estructurado que porta datos o soporta servicios de información.
- Los cables de potencia deben estar separados de los cables de comunicaciones para evitar interferencia.
- Se debe asegurar que los centros de cableado y/o cuarto eléctrico tengan las condiciones físicas y medioambientales.
- Mantener organizado e identificado el cableado en los gabinetes de los centros de cableado y centro de datos.
- El cableado de la red debiera estar protegido contra intercepciones no autorizadas o daños.

d) Mantenimiento de los equipos.

- Se debe asegurar que se les efectúe mantenimiento preventivo a los equipos adecuadamente con el objeto de garantizar su disponibilidad e integridad continua.
- Se debe asegurar el correcto funcionamiento de los equipos de cómputo, concretando tiempos de mantenimiento de los equipos con el Departamento de Sistemas y el responsable de cada equipo de cómputo.
- Los miembros del departamento de sistemas y terceros autorizados por el Jefe departamento de Sistemas puede brindar mantenimiento y llevar a cabo reparaciones en los equipos.
- Se deben mantener registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo realizado a los equipos.

e) Seguridad de los equipos y activos fuera de las instalaciones.

- Los equipos portátiles que contengan información clasificada como confidencial o reservada, cuenten con controles de seguridad que garanticen la confidencialidad de la información.
- Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En caso de viaje siempre se debe llevar como equipaje de mano.
- Informar inmediatamente al Departamento de Sistemas en caso de pérdida o robo de un equipo portátil, el responsable del equipo debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de esta.

CONTENIDO

- Asegurar con una guaya los equipos portátiles cuando se encuentren desatendidos, dentro o fuera de las instalaciones.
- Registrar todos los equipos de cómputo al ingreso y al retirarse de las instalaciones, según las indicaciones relacionadas con los activos de la corporación.

f) Reutilización o retirada segura de dispositivos de almacenamiento.

- Realizar la copia de respaldo de la información que se encuentre almacenada en los equipos de cómputo, por medio de las herramientas dispuestas por la corporación.
- El almacenamiento de la información corporativa debe ser resguardada por los usuarios en las herramientas dispuestas para su fin.
- Cuando un equipo de cómputo sea reasignado o dado de baja, posteriormente, debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

g) Equipo informático de usuario desatendido.

- No se permite retirar equipo, información o software sin autorización previa del Departamento de Sistemas.
- Cerrar las sesiones activas cuando hayan terminado su trabajo y bloquear la pantalla cuando se ausente de su puesto de trabajo.
- Los usuarios de las diferentes tecnologías deben salir de las aplicaciones o servicios de red cuando ya no los necesiten.

h) Política de puesto de trabajo despejado y bloqueo de pantalla.

- Siempre que cualquier trabajador se ausente de su puesto de trabajo, deberá guardar en un lugar seguro y bajo llave cualquier documento físico, medio magnético u óptico que contenga información sensible, crítica o reservada.
- Los colaboradores que estén ubicados en oficinas de atención al público, al ausentarse de sus puestos de trabajo, deberán guardar los documentos y medios que contengan información sensible, crítica o reservada.
- Los usuarios de las diferentes tecnologías no deben mostrar información en la pantalla cuando el equipo no esté en uso y el escritorio del computador debe estar libre de archivos o enlaces de acceso a archivos, estos deben ubicarse en carpetas diferentes al escritorio.
- Dependiendo de la clasificación de los documentos en papel y la cultura de la organización, el papel y los medios extraíbles deben asegurarse cuando no estén en uso.
- Los documentos que contengan información sensible, crítica o reservada, cuando se impriman se deberán retirar inmediatamente de las impresoras.

- Todos los equipos de cómputo y dispositivos portátiles deberán tener aplicado el cierre de sesión por inactividad.

7.5. SEGURIDAD DE LAS OPERACIONES.

El necesario para la protección de la información corporativa establecer políticas que puedan controlar los procedimientos existentes sobre las operaciones, el desarrollo y mantenimiento de documentación actualizada relacionada.

7.5.1. Responsabilidades y procedimientos de operación

a) Procedimientos documentados de operación

-
- Identificación los requerimientos de seguridad antes del desarrollo o adquisición de un sistema: Antes de que un nuevo sistema de información, se adquiera o se desarrolle, el responsable dentro del departamento de sistemas de la infraestructura lógica de la Caja, deberá haber especificado los requerimientos de seguridad necesarios y validará el cumplimiento de estos criterios antes durante el procedimiento de adquisición de tecnología.
- Documentación estandarizada para toda la tecnología que se encuentre en el ambiente de producción: Cada usuario que desarrolle o implemente software o hardware para ser usado por la Caja en las actividades propias del negocio, deberá documentar el sistema de acuerdo con el avance de la Implementación. La documentación deberá ser escrita para que el sistema pueda ser utilizado por personas no familiarizadas con él. La documentación deberá cubrir usuarios finales operativos y técnicos.
- La funcionalidad permitida en los sistemas desarrollados o implementados: las funciones descritas en el documento aprobado de especificaciones de la solución tecnológica podrán ser incluidas o implementadas en las funcionalidades de los sistemas, será responsabilidad del desarrollador su no cumplimiento.
- La incorporación o modificación del software en el ambiente de producción: Todos los sistemas de información incluyendo aplicaciones deberán ser provistos de software licenciado y deberán estar registrados en un inventario de licencias de software bajo la responsabilidad del delegado en el equipo del departamento de sistemas.
- Instrucciones formales dadas por el proveedor sobre la integridad: Cuando la adquisición del software se realiza a terceros, el responsable del procedimiento de adquisición de la tecnología deberá gestionar la inclusión en el contrato una cláusula de integridad donde el proveedor garantice el aseguramiento de que el software en cuestión no contiene indocumentadas características técnicas, no contiene mecanismos ocultos que puedan ser usados para comprometer la seguridad del software, y no requiere de la modificación o debilitamiento de controles del software del sistema aplicativo y operativo bajo el cual corre.

b) Gestión de cambios

- Todos los sistemas de información que se encuentren en producción deberán cumplir con el procedimiento formal de control de cambios: Cada responsable técnico de sistemas de información será el responsable del control de cambios, y llevará el registro de los mismos donde se evidencia de forma clara el origen, el cambio, el motivo, la fecha, la supervisión o autorización y la conclusión de los cambios realizados en el aplicativo.
- Todo desarrollo de software debe tener requerimientos formales: Se deberán definir previamente las especificaciones o requerimientos formales para todo desarrollo de software. Estas especificaciones deberán ser parte integral de un acuerdo entre los dueños de la información involucrada y los programadores del software, ya sean internos o externos. El acuerdo deberá ser completado y aprobado antes de comenzar el desarrollo o personalización del código del aplicativo.
- Todo software que ha sido primero probado externamente por terceros también debe ser probado por la entidad: Los programas ejecutables (código objeto de software) provistos por entidades externas, deberán probarse por la Caja antes de la instalación en el ambiente de producción. Cada prueba y examen deberán ser consistentes con los estándares de la Caja y deberá tener la documentación estándar mínima requerida.
- Desarrollo de aplicaciones de usuario final e implementación en el ambiente de producción: Todo software que maneje información sensible, crítica, o valiosa, desarrollado para los usuarios finales y que se deba comenzar a usar en el ambiente de producción, deberá tener la autorización de su uso por parte del jefe de departamento de sistemas y del dueño del proceso propietario del sistema de información.
- Procedimientos para el regreso a una versión anterior del software en producción: Procedimientos para el regreso a una versión anterior "back off" deberán ser desarrollados para todos los cambios al software que se encuentre en producción. Ellos permiten a las actividades de procesamiento de datos un rápido y conveniente regreso a la anterior versión del software o estado de datos, para que las operaciones del negocio puedan continuar.
- Cuando se pase al ambiente de producción un nuevo software o uno significativamente modificado, se requieren procedimientos contingentes especiales para evitar considerables pérdidas en la entidad. Los líderes de los procesos deberán preparar un plan de contingencia de conversión que refleje las diferentes formas o maneras de asegurar la continuidad del servicio a los usuarios que potencialmente se puedan ver afectados.

c) Gestión de la capacidad

- Programas que consumen excesivos recursos del sistema: Los usuarios del sistema no deberán escribir o

ejecutar ningún programa o proceso automático que consuma demasiados recursos de máquina y que puedan afectar el normal rendimiento de los trabajos de la Caja.

d) Separación de los ambientes para desarrollo, prueba y operación

- No ejecutar pruebas al software con información confidencial: No es permitido ejecutar pruebas al software aplicativo con datos o información real del ambiente de producción, cuando ésta sea específicamente secreta o confidencial.
- Eliminación todas las rutas de acceso no autorizadas en los ambientes de producción: Antes de trasladar al ambiente de producción el software desarrollado, los programadores o personal técnico del departamento de sistemas deberán eliminar todas las rutas de acceso especiales o privilegiadas, para que solamente puedan ser obtenidas de acuerdo con los procedimientos corporativos normales de seguridad. Todos los privilegios de usuarios especiales que se concedieron para el desarrollo del software no deberán ser permitidos en el ambiente de producción, los privilegios serán controlados por el responsable del procedimiento de control de acceso.
- Utilización de convenciones estándar para nombrar los archivos en el ambiente de producción: Se deberán utilizar convenciones estándar para nombrar los archivos del ambiente de producción, que permitan diferenciarlos claramente de los respectivos archivos utilizados en los ambientes de desarrollo, pruebas o con propósitos de entrenamiento.
- Las etapas de sistemas deben mantener los ambientes de producción, desarrollo, pruebas o con propósitos de entrenamiento, de forma separada o independiente tanto para las aplicaciones y bases de datos, los permisos de acceso y funciones dependerán de la etapa en que se encuentren; la asignación de estos permisos se contrala según el procedimiento de control de acceso.
- Utilización de convenciones estándar para nombrar los archivos en el ambiente de producción: Se deberán utilizar convenciones estándar para nombrar los archivos del ambiente de producción, que permitan diferenciarlos claramente de los respectivos archivos utilizados en los ambientes de desarrollo, pruebas o con propósitos de entrenamiento.
- El personal de desarrollo de sistemas no debe ser el responsable de las pruebas formales del software: Los colaboradores que estén vinculados específicamente con el desarrollo del software no deberán ser los responsables del resultado de las pruebas formales ni de la operación diaria de la solución tecnológica.

7.5.2. Protección contra código malicioso.

a) Controles ante software malicioso.

- Los usuarios deben notificar la presencia de virus en el computador: Si los usuarios sospechan que hay infección por un virus, ellos deben inmediatamente parar de usar el computador, desconectarlo de todas las redes y reportar el caso al Departamento de Sistemas.
- Proceso para examinar el Software obtenido a través de internet: Antes de usar el software obtenido a través de internet los usuarios deben cerrar todas las sesiones activas en los sistemas de información, servidores y otras conexiones en red; debe evaluarse la presencia de virus informáticos antes de ejecutarse. Si un virus es detectado debe notificarse inmediatamente al Departamento de Sistema, quienes divulgarán un mensaje de alerta vía correo electrónico a todos los usuarios de la red para que se abstengan de bajar este software infectado a través de internet.
- Se requieren instalar programas de chequeo de virus en PCs y servidores LAN: El Departamento de Sistemas, debe contar con programas automáticos para examinar virus e instalarlo y ejecutarlo continuamente en todos los servidores de red de área local (LAN) y en los diferentes computadores que se conectan a la red institucional.
- Los usuarios del sistema no deben incluir virus en el software: Los usuarios del sistema que hagan o pretendan escribir, generar, compilar, copiar, propagar, ejecutar, o intentar introducir intencionalmente cualquier código malicioso al computador, que haya sido diseñado para causar daño o impedir la normal actuación de la memoria de la máquina, archivos de datos o programas, sistemas operativos o software aplicativo; se les aplicará lo contemplado en la ley 1273 de 2009, ley de la protección de la información y de los datos.
- Pruebas de virus antes de usar los programas en la entidad: Para prevenir la infección por virus en los computadores, los funcionarios de la Caja no deben usar ningún software proporcionado externamente por una persona u organización que no sea un proveedor conocido y confiable. La única excepción a esto es cuando el software ha sido primero probado y aprobado por el Departamento de Sistemas.

7.5.3. Copias de seguridad.

a) Respaldo de la información

- Control de acceso a usuarios finales en el proceso de restauración de información: Si a los usuarios finales les está permitido restaurar sus propios archivos de información, se les debe restringir la capacidad para restaurar la información de otros usuarios o inclusive mirar que archivos de otros usuarios han sido respaldados.
- Que datos se deben respaldar y con qué frecuencia: Toda la información de valor, confidencial y crítica de la entidad, debe ser periódicamente respaldado en medio digital. Este proceso de respaldo debe ser realizado al menos mensualmente.
- Respaldos periódicos y complementarios requeridos para computadores portátiles: Los usuarios que usen computadores portátiles deben hacer respaldo de su información crítica antes de ser llevados fuera del lugar de trabajo. Estos respaldos deben permanecer en el sitio de trabajo o virtual y deben ser hechos en forma adicional a los procedimientos de respaldo preestablecidos.
- Inscripción de los datos de respaldo que se archiven en sitios fuera de la entidad: Toda información de valor,

confidencial o crítica que sea respaldada y almacenada en un lugar externo a la entidad debe ser respaldada en forma encriptada para prevenir que esta sea divulgada o usada en forma no autorizada por otras entidades o personas.

- Almacenamiento de backup en un sitio externo: Los backups de información de alto valor, sensitiva y crítica deben ser almacenados en un repositorio documental destinado para este fin.
- Los funcionarios de tipo administrativo: Los funcionarios responsables de cada área administrativa deben identificar y mantener una lista completa de los registros vitales de su área en caso de un proceso de restauración después de un desastre.
- Los propietarios de los sistemas de información deberán indicar la frecuencia de realización de las copias de seguridad y tiempo de resguardo según las TRD de cada proceso, para que estas sean incluidas en la programación de las copias de seguridad.
- Las copias de seguridad de los sistemas de información serán realizadas según lo contemplado en el plan de copias de seguridad GTI-DES-007.

7.5.4. Registro de actividad y supervisión

a) Registro de eventos

- Logs en los sistemas de aplicación que contengan Información sensitiva: Todos los sistemas de aplicación en producción que contengan información sensitiva de la Caja deben generar Logs o evidencias que indiquen cada adición, modificación, borrado de esta información.
- Contenido de Logs en los sistemas de aplicaciones en ambiente de producción: Todo software aplicativo habilitado en ambiente de producción de la Caja debe incluir archivos Logs que registren como mínimo la siguiente información: (1) el usuario que ingreso al sistema, (2) cambios realizados en la información, (3) fecha y hora del cambio.
- Revisiones regulares a los Logs del sistema: El administrador del sistema o el responsable del procedimiento de infraestructura lógica de la Caja, deben periódicamente revisar los diferentes registros de los Logs con el fin de verificar las violaciones a las seguridades o mal uso de la información en las máquinas multi-usuario y en los sistemas de información, presentando a la Administración informes periódicos de tal comportamiento.

b) Protección de la información de registros (logs).

- Períodos de retención de los Logs: Los Logs que contienen los registros de los eventos relevantes de los diferentes sistemas de información deben retenerse por un periodo mínimo de un año y se estarán sacando copias de forma permanente se acuerdo con la política de copias de seguridad, a esta información solo tendrá acceso el jefe del Departamento de Sistemas y el dueño del procedimiento de infraestructura

lógica.

- Personas autorizadas para consultar los Logs: El Departamento de Sistemas, entes de control y los miembros de la alta dirección tendrán acceso a los Logs de los sistemas de información en caso de requerirlos.

c) Registros del administrador y operador

- Reflejo en los Log de auditoría sobre la actividad de los administradores: Las transacciones realizadas por los usuarios administradores debe quedar registrado en los logs de auditoria.

d) Sincronización de relojes

- Sincronización del reloj para un Log adecuado de eventos en la red: Todos los computadores multi-usuario conectados a la red interna de la Caja deben tener la hora exacta reflejada en el reloj interno, esta debe estar sincronizada con la hora legal colombiana, http://horalegal.inm.gov.co/.

7.5.5. Control del software en explotación.

a) Instalación de software en los sistemas operativos.

- El uso de medios de almacenamiento para los sistemas de utilidades residentes en ambientes de producción: Los discos y otros medios de almacenamiento en línea usados en los servidores de producción y servidores web, no deberán contener compiladores, ensambladores, editores de texto, procesadores de palabra u otras utilidades de propósito general que puedan utilizarse para comprometer la seguridad del sistema.
- Prohibición a los usuarios finales de la instalación de software en sus equipos o computadoras personales: Los usuarios finales no deberán instalar software en sus equipos de cómputo, servidores de red, u otras máquinas sin la autorización del Jefe del Departamento de Sistemas o el responsable del procedimiento de gestión de operaciones.
- Se prohíbe instalar programas externos en las computadoras interconectadas en red: Los usuarios no podrán instalar ningún programa o software desarrollado fuera de la entidad en sus estaciones de trabajo, en servidores de la red, o en computadoras conectadas a la red sin la autorización del Jefe del Departamento de Sistemas o el responsable del procedimiento de gestión de operaciones.
- Todo software que se incorpore a producción debe tener su propio plan de contingencia: Siempre que se pase al ambiente de producción un nuevo software o uno significativamente modificado, se requieren procedimientos contingentes especiales para evitar considerables pérdidas en la corporación. Los lideres de los

procesos deberán preparar un plan de contingencia de conversión que refleje las diferentes formas o maneras de asegurar la continuidad del servicio a los usuarios que potencialmente se puedan ver afectados.

7.5.6. Gestión de la vulnerabilidad técnica

a) Gestión de vulnerabilidades técnicas.

- Prohibición para explorar vulnerabilidades de los sistemas de seguridad: Los usuarios no deben explorar vulnerabilidades o deficiencias en la seguridad de los sistemas de información para dañar sistemas o información, para obtener recursos mayores a los que han sido autorizados, para tomar recursos de otros usuarios, o para tener acceso a otros sistemas a los cuales no se les ha otorgado una autorización apropiada. Todas estas vulnerabilidades y deficiencias deben ser reportadas inmediatamente al Departamento de Sistemas. La protección de la información y de los datos se regulará mediante la aplicación de ley colombiana 1273 de 2009.
- Información que se sospecha como crimen informático o abuso del Computador: Para proporcionar evidencia en investigaciones y tomar acciones administrativas y de carácter legal, se debe obtener la información necesaria de, los archivos de seguridad “Logs”, los estados del sistema actual y las copias de los archivos (back-up) y de todos los demás potencialmente involucrados, cuando se sospecha que ha ocurrido un crimen informático o abuso en el computador. La información debe custodiarse por el jefe del Departamento de Sistemas y/o por el Director de la Caja.
- Se prohíbe el engaño a los controles de acceso al sistema a través de las puertas traseras: los programadores y todo el personal técnicamente especializado no deberá permitir la existencia, en el código de los programas, de las puertas traseras de trampa que engañan los mecanismos de control de acceso autorizados tanto en sistemas operativos como en los paquetes de control de acceso.

b) Restricciones en la instalación de software.

- No se deben almacenar ni usar juegos y/o aplicaciones de entretenimiento en los computadores de la entidad: No deben almacenarse, ni usarse juegos y/o aplicaciones de entretenimiento en ninguno de los computadores de la entidad.
- Prohibición para bajar y cargar Software de Internet, en los sistemas corporativos por parte de terceras personas: Los funcionarios de la Caja no deben permitir que terceras personas puedan bajar y cargar “down-loading” software de Internet, en los sistemas de la Corporación. Esta prohibición es necesaria porque dicho software puede contener virus, gusanos, caballos Troyanos y otro software malicioso que puede dañar la información y los programas en producción.
- Características o facilidades riesgosas del software en el momento de la instalación: Las características que son

innecesarias de un aplicativo en el ambiente de producción de la Caja, se deberán desactivar en el momento de la instalación del software.

7.5.7. Consideraciones de las auditorías de los sistemas de información

a) Controles de auditoría de sistemas de información

- Utilización de los log´s de los sistemas de información: Los archivos de Logs que contienen eventos relevantes de seguridad deben proporcionar suficiente información para apoyar el monitoreo, control y auditorías sobre la efectividad y cumplimiento con las medidas de seguridad implementadas en la Caja.

7.6. SEGURIDAD EN LAS COMUNICACIONES

Las redes de comunicaciones es un eslabón indispensable para compartir la información corporativa, lo que lleva a establecer controles claro para la protección y monitoreo en los sistemas de comunicación. Con lo anterior se garantiza la disponibilidad e integridad de la información que fluye a través de ella.

7.6.1. Gestión de la seguridad en las redes

a) Controles de red:

- Toda la red de datos corporativa debe estar configurada y bajo la seguridad de un corta fuegos (firewall). En dicha configuración también se deben encontrarse los computadores de la empresa.
- El firewall donde este configurada la red corporativa, debe tener herramientas de monitoreo y análisis del tráfico y vulnerabilidad.
- El departamento de sistemas debe establecer controles necesarios en el firewall corporativo para preservar la confidencialidad, integridad y disponibilidad de la información
- Todo usuario que acceda a la red corporativa por medio una computadora debe contar un usuario y una contraseña de acceso.
- Ningún colaborador puede ingresar a la red dispositivos (AP, routers, entre otros) no autorizados por el departamento de sistemas.

b) Mecanismos de seguridad asociados a servicios en red:

- Todos los servicios de red (Internet) deben ser contratados a un externo legalmente constituido. Dicho proveedor debe garantizar la disponibilidad del servicio y contar con un acuerdo de nivel de servicio.
- El departamento de sistemas debe realizar seguimientos periódicos a los servicios de red contractados, de esta

forma tomar acciones preventivas y correctivas a posibles inconsistencias.

c) Separación de redes.

- Con la finalidad conservar la seguridad en la información, el departamento de sistemas debe realizar separación de redes de acuerdo con la complejidad organizativa de la entidad y sus sedes.
- Toda configuración de la separación de las redes de datos se deben realizar a través del firewall corporativo.

7.6.2. Intercambio de información con partes externas.

a) Políticas y procedimientos de intercambio de información.

- Toda la transferencia de información corporativa entre empleados y externos deben realizarse a través de los canales establecidos por el departamento de sistemas como lo son correo electrónico, drive, chat corporativo entre otras. No está permitido compartir información por medio de dispositivos de almacenamiento extraíble.
- Software, documentación y cualquier otro tipo de información interna de la entidad no debe ser vendida o transferida a ninguna parte que no pertenezca a la entidad, para ningún propósito diferente al del negocio expresamente autorizado por los jefes de área.
- Se debe definir el tipo de acceso y los roles estrictamente necesarios sobre la carpeta en la nube (Lectura, escritura, modificación y borrado).
- No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con autorización, en caso de requerirlo se deberá ser autorizado por el dueño de la información.

b) Acuerdos de intercambio.

- Toda información corporativa compartida entre un empleado de la organización con un tercero, debe estar autorizado por su jefe inmediato. Adicionalmente debe realizarlo por canales autorizados donde sea posible darle los permisos de manipulación de la información requeridos o necesarios.

c) Mensajería electrónica.

- El departamento de sistemas debe realizar las configuraciones de seguridad pertinentes al administrador de correo electrónico, de manera que se garantice la confidencialidad, integridad y disponibilidad de la información.
- Las cuentas de correo electrónico que manejen información sensible o protección de datos personales, deben contar con el factor de doble autenticación, para los cuales el oficial de protección de datos personales deberá indicar que personas se le debe habilitar esta configuración.

d) Acuerdos de confidencialidad y secreto.

- En todo contrato con proveedor de la organización de existir un acuerdo de confidencialidad firmado entre las partes y de esta manera garantizar la no divulgación o el adecuado uso de la información corporativa.

7.7. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Para la organización la adquisición, desarrollo y mantenimiento de los sistemas de información es un factor indispensable para la generación y seguridad de la información corporativa. Por lo anterior es importante asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

7.7.1. Requisitos de seguridad de los sistemas de información.

a) Análisis y especificación de los requisitos de seguridad.

- Antes de cada compra o desarrollo de software se debe realizar un análisis de necesidad y de requerimientos mínimos, en los cuales deben estar involucrados el departamento de sistemas y área solicitante.
- En marco de análisis y especificaciones se deben establecer requisitos mínimos funcionales y no funcionales que apunten a los principales pilares de la seguridad de la información (confidencialidad, integridad y disponibilidad), tales como: infraestructura física y lógica, interoperabilidad, perfiles de usuario, auditorías, autenticación, entre otras.
- Dentro de los requerimientos no funcionales para la adquisición de software se deben establecer la simplicidad, facilidad para administrar, usar y auditar.
- Los requerimientos o controles de seguridad de la información deben ser validados y aprobados por los líderes de los procesos y el delegado del departamento de sistemas.

b) Seguridad de las comunicaciones en servicios accesibles por redes públicas.

- Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la entidad, debe pasar a través de un punto adicional de control como firewall.
- Todos los canales de comunicación que permitan el acceso a la red de comunicaciones o servidores deben pasar a través de un punto de control adicional (Firewall) antes de que el pantallazo de login aparezca en la terminal del usuario.
- Todo colaborador o tercero que necesite acceder desde una red pública o doméstica a los sistemas de información de la organización, debe contar con unas credenciales para la VPN, credenciales que deben ser solicitadas por el jefe inmediato o supervisor del contrato en caso de ser un tercero.

c) Transacciones en línea.

- A la hora de adquirir un sistema de información se debe identificar un inventario de integraciones o un diagrama de conexiones con otros sistemas de información, si así lo requiere.
- Toda transacción que afecte información de valor, sensible o crítica debe ser procesada únicamente cuando se valide la autenticidad del origen (usuario o sistema) y se comprueba su autorización mediante un mecanismo de control de acceso o perfiles. Los procesos de autenticación pueden ser realizados a través de contraseñas, tarjetas inteligentes, lectores biométricos, firmas digitales en correo electrónico.
- Las transacciones que afecten información de valor, crítica o sensible deben ser originadas desde documentos y mensajes electrónicos en los que el individuo o sistema que origine la transacción esté explícitamente definido.
- Toda transacción entre un sistema de información dentro de la organización y uno externo, deben estar previamente configurada y habilitada en el firewall.

7.7.2. Seguridad en los procesos de desarrollo y soporte.

a) Política de desarrollo seguro de software.

- Antes de que una nueva aplicación se adquiera o se desarrolle, el departamento de sistemas deberá especificar los requerimientos de seguridad necesarios y su cumplimiento será validado durante la implementación y antes de pasarlo al ambiente productivo.
- Se deberán definir previamente las especificaciones o requerimientos formales para todo desarrollo de software. Estas especificaciones deberán ser parte integral de un acuerdo entre los dueños de la información involucrada y los programadores del software, ya sean internos o externos. El acuerdo deberá ser completado y aprobado por el área o dueño del proceso, antes de comenzar el desarrollo o personalización del código del aplicativo.
- Utilizar lenguajes de programación de últimas generaciones para reducir el volumen de código a desarrollar, la dificultad de mantenimiento del software, el tiempo exigido para desarrollar una aplicación, y el número de fallas.
- Se deberán utilizar convenciones estándar para nombrar los archivos del ambiente de producción, que permitan diferenciarlos claramente de los respectivos archivos utilizados en los ambientes de desarrollo, pruebas o con propósitos de entrenamiento.
- Se debe contar con un ambiente de desarrollo en el cual sea posible, realizar todo tipo de cambios sin afectar la producción o la disponibilidad del servicio.

b) Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

Antes de comenzar a instalarse, nuevas o diferentes versiones del sistema operativo y el relacionado con el software de los sistemas en producción, deberá ser validado primero por el proceso de control de cambios establecido en la

corporación.

c) Restricciones a los cambios en los paquetes de software.

- Para prevenir copias de software no autorizadas y el empleo de la propiedad intelectual, todo el software desarrollado por la entidad para ser usado para fines misionales, deberá ser distribuido únicamente el código objeto (ejecutable).
- Para prevenir el uso no autorizado, del software desarrollado por la entidad por parte de los terceros, deberá distribuirse sólo después de que los destinatarios hayan firmado un acuerdo que declare que ellos no desensamblarán, modificarán, ni usarán indebidamente los programas entregados.
- Todo el software que posea la entidad deberá incluir avisos de los derechos de autor y propiedad literaria.
- Siempre que la entidad haya adquirido un software integral, el proveedor deberá proporcionar por escrito la licencia del software.

d) Uso de principios de ingeniería en protección de sistemas.

- Para cualquier desarrollo o adquisición de software es indispensable que este cuente con un mecanismo de autenticación de usuario guardando los parámetros mínimos de seguridad contemplados en el dominio de acceso.
- Para cualquier desarrollo o adquisición de software, el código fuente del mismo debe estar protegido fuera del ambiente productivo.
- Para todos los sistemas información administrativos, la seguridad debe hacerse por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en producción.

e) Seguridad en entornos de desarrollo.

- Todo ambiente de desarrollo de software realizado en la corporación debe estar separado del productivo.
- Se deberán utilizar convenciones estándar para nombrar los archivos del ambiente de producción, que permitan diferenciarlos claramente de los respectivos archivos utilizados en los ambientes de desarrollo, pruebas o con propósitos de entrenamiento.
- El nuevo software de aplicación en desarrollo o personalización deberá guardarse estrictamente separado del que se encuentra en producción y del respectivo de pruebas. Si las facilidades existentes lo permiten, la separación de los ambientes deberá hacerse en equipos de cómputo independientes. Si no se deberán separar los directorios y librerías, y hacer cumplir estrictamente los controles automáticos de acceso a los usuarios.

- Los colaboradores que estén vinculados específicamente con el desarrollo del software no deberán ser los responsables del resultado de las pruebas formales ni de la operación diaria de la solución tecnológica.
- En caso que para algún desarrollo se requiera información privada reservada o clasificada, el desarrollador debe solicitar formalmente la autorización al propietario del activo de información.
- En todo equipo que se use para el desarrollo de algún software de la corporación debe tener antivirus instalado y estar bajo las reglas del firewall.

f) Externalización del desarrollo de software.

- En caso de que la empresa contrate un desarrollo de software a un tercero este debe supervisar que los requerimientos se están plasmando según lo solicitado.
- En caso de que la empresa contrate un desarrollo de software a un tercero debe exigir la licencia del mismo o propiedad del código fuente, según se establezca en el contrato.
- En caso de que la empresa contrate un desarrollo de software a un tercero, debe definir la metodología de desarrollo a utilizar.

g) Pruebas de funcionalidad durante el desarrollo de los sistemas.

- Para cualquier desarrollo o adquisición de software el departamento de sistema debe realizar pruebas de los requerimientos no funcionales, de seguridad e interoperabilidad.
- Todas las pruebas realizadas deben desarrollarse en el ambiente de pruebas, esto con la finalidad de no afectar los datos del servicio en producción.
- Para cualquier cambio realizado en un sistema de información, se deben realizar verificación del control de cambio o notificación del cambio en el ambiente de pruebas.

h) Pruebas de aceptación.

- Los líderes de procesos, sus delegados o usuarios finales realizarán pruebas funcionales de todo lo requerido en el ambiente correspondiente, con la finalidad de autorizar si el desarrollo está de acuerdo con lo solicitado o rechazar si existe alguna inconsistencia o error en la parte funcional del desarrollo.
- El representante del departamento de sistemas realizará pruebas de requerimientos no funcionales, de seguridad y de interoperabilidad, con la finalidad de autorizar si el desarrollo está de acuerdo con lo solicitado o rechazar si existe alguna inconsistencia o error en la parte técnica del desarrollo

7.7.3. Datos de prueba.

a) Protección de los datos utilizados en prueba.

- Siempre que se pueda se debe utilizar datos no reales para realizar las pruebas, en caso contrario el ambiente de pruebas debe contar con las mismas medidas de seguridad que el ambiente productivo.

7.8. SEGURIDAD EN EL RECURSO HUMANO.

Con la finalidad de brindar protección a la información corporativa mediante su recurso humano, es necesario contar controles referentes a la vinculación y desvinculación de sus empleados, así la educación y socialización en materia de la seguridad de la información.

7.8.1. Previo al empleo.

a) Investigación de antecedentes.

- La oficina de administración de personal debe validar antecedentes disciplinarios y penales de los candidatos, esto teniendo en cuenta el perfil a desempeñar en la corporación.

b) Términos y condiciones de contratación.

- Con respecto a los términos y condiciones contractuales referentes a la seguridad de la información se debe remitir a las políticas de la oficina administrativa.

7.8.2. Durante la contratación.

a) Responsabilidades de gestión.

- Facilitar los recursos necesarios para el funcionamiento y mejora de la seguridad de la información
- La alta dirección debe facilitar los recursos pertinentes para que todo colaborador o contratista, conozca las políticas de seguridad y privacidad de la información.
- Asignar las responsabilidades en materia de seguridad de la información.

b) Concientización, educación y formación en seguridad de la información.

- Todos los colaboradores deben contar con entrenamiento y material de referencia de soporte que les permita

proteger adecuadamente los recursos de información de la entidad a nivel digital.

- Cada colaborador debe entender las políticas y procedimientos de la entidad con respecto a la seguridad de la información, debe estar de acuerdo para su ejecución y desarrollar su trabajo en base a estas.
- Es requerido realizar el proceso de entrenamiento y capacitación en el manejo de sistemas de información en producción por parte de los colaboradores antes de realizar alguna transacción en este.
- Cada trabajador debe atender a la inducción general en el tema de seguridad en la información. Para que exista una evidencia de que cada colaborador ha atendido a dicha inducción, estos deben dejar constancia de que ellos han asistido, entendido el material presentado y han tenido la oportunidad de hacer preguntas.

c) Proceso disciplinario.

- El departamento de sistemas debe reportar al jefe inmediato las brechas de seguridad de la información realizada por un colaborador que generen pérdidas de recursos a la organización. Lo anterior para que dicho jefe tome las acciones disciplinarias necesarias.

7.8.3. Finalización o cambio de puesto de trabajo.

- Cuando un colaborador tuvo un cambio de puesto de trabajo, la oficina administrativa y los lideres de los procesos, debe informar oportunamente indicando que permisos en los diferentes aplicativos se deben retirar y cuáles serán los nuevos asignar.
- Cuando se termina la relación laboral con algún colaborador, la oficina administrativa o lideres de los procesos debe informar su retiro al departamento de sistemas para que este retire los accesos a la información.
- Hasta la culminación del empleo, los empleados no pueden retener, traicionar, o retirar cualquier información de la entidad, diferente a copias personales de correspondencia relacionada directamente con los términos y condiciones de su empleo. Cualquier otra información de la entidad en custodia del trabajador que se retira, debe ser entregada al jefe inmediato del trabajador en el momento de su salida.
- En la terminación o expiración de su contrato, todos los contratistas, asesores y temporales deben entregar personalmente al jefe inmediato toda la información (documentos, bases de datos, etc) creada durante la ejecución del contrato.

7.9. RELACIÓN CON PROVEEDORES

Los proveedor son parte importante a la organización, estos por cualquier circunstancia debido a su vínculo con la empresa trabajan o manejan información sensible o que cuenta con protección de datos personales, por lo anterior es conveniente establecer de modo formal las condiciones para el uso de dicha información y supervisar el cumplimiento de las condiciones.

7.9.1. Seguridad de la información en las relaciones con proveedores.

CONTENIDO

a) Política de seguridad de la información para proveedores.

- Todo proveedor de servicios tecnológicos de la organización debe acogerse a la normatividad y procedimientos internos tales como el manual de contratacion, manual de políticas de seguridad de la información, manual de salud y seguridad en el trabajo, entre otros.
- Los proveedores que accedan a los servicios tecnológicos deben realizarlo por medio de unas credenciales, previamente otorgadas por el departamento de sistemas. Dichas credenciales deben ser solicitadas por el supervisor del contracto.
- El terminar la relación comercial con el proveedor de la empresa, el supervisor del contrato informara al departamento de sistemas para que sean retiradas o inactivadas las credenciales de acceso a los servicios tecnológicos.

b) Tratamiento del riesgo dentro de acuerdos de proveedores.

- Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura tecnológica para la información.
- Exigir que, en todos los contratos o acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información, se deben realizar acuerdos de confidencialidad y/o acuerdos de protección de datos sobre el manejo de la información.
- Asegurar y describir que los requisitos legales y de reglamentación, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor se cumplan.
- Exigir el derecho de auditar los procesos y controles de los proveedores, relacionados con el acuerdo.

c) Cadena de suministro en tecnologías de la información y comunicaciones.

- Aquellos proveedores de servicios tecnológicos que subcontraten lo acordado con la empresa, debe informar al supervisor del contrato el tercero subcontratado. Adicionalmente este último tercero debe acogerse a todo lo reglamentado y a las condiciones en materia de seguridad de la información de la organización.

7.9.2. Gestión de la prestación del servicio por proveedores.

a) Supervisión y revisión de los servicios prestados por terceros.

- Todo supervisor de contrato debe realizar un informe de supervisión sobre la ejecución del mismo.
- Los supervisores de contratos exigirán al proveedor un informe de ejecución de las actividades ejecutadas durante el proceso contractual. La periodicidad de este informe dependerá de la frecuencia de los pagos

pactados.

- Anualmente se debe realizar evaluación de los proveedores de servicios tecnológicos, con la finalidad de monitorear su desempeño durante el año en la ejecución de los servicios contratados.

b) Gestión de cambios en los servicios prestados por terceros.

- Por cualquier eventualidad que se presente en la ejecución de los contratos que afecten el alcance, valor y tiempo del contrato, el supervisor debe evaluar los escenarios presentados y tomar decisiones en común acuerdo con el proveedor de manera de abordar la situación de la mejor manera. Estos cambios deben ser informados al proveedor oportunamente.
- Los cambios generados en materia normativa o documentación especifican que afecte el servicio del proveedor debe ser informado oportunamente al tercero por parte de sus supervisor.

7.10. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los incidentes de seguridad de la información hace parte del día a día de una organización por eso conveniente que la organización establezca pautas para la atención oportuna de dichos incidentes, así como implementar acciones correctivas para disminuir la probabilidad de su ocurrencia.

7.10.1. Gestión de incidentes de seguridad de la información y mejoras.

a) Responsabilidades y procedimientos.

- El departamento de sistemas debe disponer de un canal oficial para que los usuarios puedan reportar incidentes o requerimientos de seguridad de la información.
- Los usuarios de la corporación deben reportar cualquier incidente o requerimiento, por medio de la mesa de ayuda autorizada por el departamento de sistemas. Este reporte debe estar correctamente diligenciado, de manera que describa claramente la problemática y adjunte las evidencias necesarias.
- Es responsabilidad del departamento de sistemas asignar, responder y dar oportuna solución al incidente o requerimiento de acuerdo con el acuerdo de nivel de servicios interno.
- Cuando algún incidente o requerimiento reportado no brinda información necesaria para ser tramitado el técnico o profesional responsable del caso puede elaborar un seguimiento al caso por la mesa de ayuda solicitando la información, sin el usuario no responde al seguimiento el caso se cerrará.

7.10.2. Notificación de los eventos de seguridad de la información.

CONTENIDO

Todo usuario de la corporación debe reportar oportunamente ante la mesa de ayuda establecida por el departamento de sistemas cualquier amenaza, vulnerabilidad, evento o incidente de la seguridad de la información.

a) Notificación de puntos débiles de la seguridad.

- Cualquier debilidad en seguridad de la información que sea detectada por algún colaborador de la empresa, este debe reportarla al departamento de sistemas en la mesa de ayuda establecida.
- Ningún colaborador de la compañía debe probar las vulnerabilidades o fortalezas de los sistemas de información, exceptuando el personal capacitado del departamento de sistemas. Lo anterior es interpretado como un mal uso de los sistemas de información.

b) Evaluación y decisión sobre los eventos de seguridad de la información.

- Los eventos de la seguridad de la información reportados deben ser evaluados y priorizados para su atención, lo anterior con base en el acuerdo de nivel del servicio.
- El departamento de sistemas debe establecer una base de conocimiento donde se deben guardar los eventos de seguridad más relevantes, así como su solución. Lo anterior para que sirva a la toma de decisiones.

c) Respuesta a los incidentes de seguridad.

- El jefe del departamento de sistemas debe asignar oportunamente el caso al técnico o profesional responsable de su análisis o solución.
- Todo técnico o profesional que se le asigne algún caso debe dar respuesta y solución oportuna. Si la solución de este caso depende de un proveedor, entonces se debe reportar ante la mesa de ayuda externa y documentar cualquier novedad a la mesa de ayuda de la corporación.
- Todo evento o caso reportado debe ser documentado y cerrado oportunamente una vez ya se haya dado solución.

d) Aprendizaje de los incidentes de seguridad de la información.

Todo aquel evento o incidente recurrente y de alto impacto para la seguridad de la información debe ser guardado en la base de conocimiento de la mesa de ayuda. Con lo anterior se puede ayudar a identificar soluciones rápidas a futuros casos similares, además de implementar controles para evitar su recurrencia.

e) Recopilación de evidencias.

Todas las evidencias de los eventos de la seguridad de la información deben ser salvaguardados y preservados en un lugar seguro.

7.11. SEGURIDAD DIGITAL

7.11.1. Condiciones de la seguridad digital.

- Establecer un modelo de seguridad y privacidad de la información de acuerdo a las buenas prácticas establecidas por el Ministerio de las Tecnologías de la Información y Comunicaciones.
- Reportar todos los incidentes cibernéticos ocurridos en la entidad ante CSIRT-PONAL y partes interesadas, estos incidentes tendrán un reporte en la mesa de servicio establecido por el departamento de sistemas.
- Socializar los reportes o incidentes publicados por CSIRT-PONAL.
- Establecer e implementar controles asociados con los incidentes.

7.11.2. Controles de la seguridad digital en desarrollos web y aplicaciones.

- Las aplicaciones desarrolladas o adquiridas por la corporación que sean publicadas, tendrán controles de autenticación para su acceso y de roles y privilegios para el acceso a información y transacciones.
- Los sitios web estarán alojados en un proveedor de hosting.
- Realizar monitoreo a los sitios web, de manera que sea posible detectar archivos, patrones sospechosos y posibles ataques.
- Garantizar conexiones seguras a través del uso de certificados SSL (HTTPS para la confianza de usuarios) para los sitios web y/o aplicaciones corporativas publicadas.
- Implementar sistemas antivirus en los servidores de aplicaciones, para garantizar medidas contra infecciones de malware a los archivos del mismo.
- Establecer condiciones contractuales con terceros (Proveedores páginas web corporativas), que permita evidenciar controles orientados a la seguridad digital en el desarrollo de sitios web y sus aplicaciones, durante todo el ciclo de vida.

7.12. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

La continuidad del negocio posterior a cualquier evento catastrófico o tecnológico evita o disminuye la pérdida de valor de una empresa, es por eso que una organización debe establecer controles que sirvan como herramientas de respuestas a la continuidad o recuperación de los servicios de la entidad ante amenazas que puedan afectar dichos servicios.

7.12.1. Continuidad de la seguridad de la información.

CONTENIDO

a) Planificación de la continuidad de la seguridad de la información.

- La Corporación debe contar con un plan de continuidad del negocio, adecuado para cada uno de los servicios prestados.
- El plan de continuidad del negocio corporativo debe estar alineado con los requisitos de seguridad de la información en situación de crisis o en caso de desastres.
- El plan de continuidad del negocio corporativo debe contemplar cualquier evento externo que pueda afectar la prestación de los servicios.
- Dentro del plan de continuidad del negocio debe existir una estrategia de recuperación de información ante desastres.

b) Implantación de la continuidad de la seguridad de la información.

- Ante la eventualidad de una emergencia o desastre se debe activar el plan de continuidad del negocio, de manera que se preserve como prioridad la seguridad de la información corporativa.
- La entidad debe definir los responsables en la ejecución del plan de continuidad del negocio, así como las funciones de cada integrante.
- Luego de asegurar la información, el plan debe estar orientado a la recuperación de los sistemas de información, esto de acuerdo a la criticidad de los servicios.

c) Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

- El plan de continuidad de negocio debe ser revisado periódicamente, esto para inclusión de nuevos controles o nuevos sistemas de información, de acuerdo a la actualidad de la corporación.
- Los controles pueden variar de acuerdo a la realidad de la empresa, por ende es necesario evaluarlos periódicamente para validar su funcionamiento ante una eventualidad.

7.13. CUMPLIMIENTO

El cumplimiento de toda legislación, regulación, buenas prácticas o normatividad sobre la seguridad de la información es necesario para la protección de la misma. Tomando en cuenta lo anterior es conveniente establecer criterios para el

conocimiento y divulgación de las normas y de esta forma puedan ser aplicadas correctamente.

7.13.1. Cumplimiento de los requisitos legales y contractuales.

a. Identificación de la legislación aplicable y de los registros contractuales.

- La entidad debe identificar toda aquella normatividad que dicte el estado e incluso normas internacionales sobre la seguridad de la información y trabajar bajo la misma.
- La entidad debe realizar revisión periódica de las normatividades vigentes de manera que sea posible identificar aquellas que no están derogadas o incluir las nuevas.

b. Derechos de propiedad intelectual (DPI).

- Los colaboradores de la entidad solo deben hacer uso de las herramientas dispuestas por el departamento de sistemas, las cuales ya deben contar con los derechos de uso según la normatividad vigente.
- El departamento de sistemas debe promover el uso de herramientas tecnológicas con derechos de propiedad intelectual y licencias de uso ya adquiridas por la corporación.
- El departamento de sistemas debe tener salvaguardado e inventariado las licencias de uso y los derechos de propiedad intelectual del software que adquiera.

c. Protección de los registros de la organización.

Los registros o datos de los sistemas de información debe estar salvaguardado según las normas internacionales de seguridad de la información como lo es la ISO 27001, adicionalmente clasificada e inventariada según su confiabilidad, disponibilidad e integridad.

d. Protección de datos y privacidad de la información personal.

El área de servicio al cliente de la corporación debe contener políticas o pautas claras para la protección de datos y privacidad de la información personal.

CONTENIDO

e. Regulación de los controles criptográficos.

- Todo control criptográfico que adquiera la corporación debe estar avalado por algún organismo de seguridad de la información nacional o internacional.
- La entidad debe evaluar qué información requiere dicha protección, según su sensibilidad.

7.13.2. Revisiones de la seguridad de la información.

a) Revisión independiente de la seguridad de la información.

- El departamento de sistemas debe permitir y facilitar la documentación necesaria para ser revisados y evaluados por la sección de control interno corporativo, auditorías internas y externas. Esto es importante para tener puntos de vista ajenos al personal del departamento.
- El departamento de sistemas debe tomar en cuenta las recomendaciones resultantes de las auditorías realizadas.

b) Cumplimiento de las políticas y normas de seguridad.

- Todo colaborador debe laborar bajo las políticas en este documento establecidas, así como bajo las leyes del ente nacional.
- Cualquier incumplimiento de estas políticas, deben ser reportado al departamento de sistemas para que este tome reporte ante su jefe inmediato la falta y se tomen acciones correctivas.

c) Comprobación del cumplimiento.

- Todo sistema de información corporativa debe ser evaluado periódicamente, con la finalidad de velar que esté cumpliendo con las políticas descritas en este documento.
- De acuerdo a la evaluación realizada el Departamento de sistemas debe tomar acciones correctivas, sin en caso tal encontró algún incumplimiento.