CIRCULAR No. 003-2024

"Por medio de la cual se actualiza y socializa la "Política De Seguridad De La Información" dando cumplimiento a los estándares de la norma ISO 27001 y el inicio a la implementación del sistema General De Seguridad De La Información (SGSI)"

24/07/2024

Al contestar, cite este número: 20241000010983

Bogotá D.C., 24 de Julio de 2024

PARA: TODA LA CORPORACIÓN

DE: DIRECCIÓN ADMINISTRATIVA

ASUNTO: Actualización y Socialización de la Política De Seguridad De La Información en cumplimiento a los estándares de la norma ISO 27001 y el inicio a la implementación del sistema General De Seguridad De La Información (SGSI) de la Caja de Compensación Familiar campesina- COMCAJA.

Teniendo en cuenta los riesgos que se generan a nivel de tecnologías de la información y por el manejo de actualización en las diferentes herramientas sobre el cual se realizan actividades misionales y administrativas y en búsqueda de implementar controles y buenas prácticas de manejo, me permito socializar la actualización de la política de seguridad de la información el cual empezara aplicar a partir de la fecha de la publicación.

La Política es de cumplimiento tanto para colaboradores como para terceros que se encuentren vinculados a la Caja de Compensación Familiar Campesina-COMCAJA la cual busca realizar la implementación de accione encaminadas a la minimización de los riesgos y dar el debido manejo a las herramientas suministradas.

Para asegurar el manejo de la Política y la Efectividad se realizarán las siguientes medidas:

Socialización

Por medio de los líderes y Jefes de las Áreas se realizará la entrega del documento denominado ***"Política de seguridad de la información"*** el cual será

el encargado de dar el debido cumplimiento a una de las responsabilidades que se encuentran dentro del documento de Roles y responsabilidades del SGSI.

Para los colaboradores nuevos por medio del área de Talento Humano realizará la entrega de la Política con el fin de conocer las buenas prácticas y el manejo de controles definido en la entidad.

Capacitación y Sensibilización

Dar cumplimiento al desarrollo de las evaluaciones con el fin de identificar la recepción, terminología, acciones y demás que se encuentran en la Política tanto para Colaboradores como para personal nuevo que ingresa a la entidad; De esta manera dar cumplimiento al plan de capacitaciones. Procesos que será verificado por el área de talento humano en el cumplimiento de las obligaciones del personal vinculado a la entidad.

Seguimiento y Control

Realizar la verificación con el total de personal vinculado a la entidad y con el desarrollo de nuevas guías implementadas enfocadas al Sistema de seguridad de la información aclarar términos a mayor detalle que permitan velar por el buen manejo de controles tanto a nivel técnico como administrativo en los controles definidos.

Plan de acción

Con el desarrollo de las guías se realizará la entrega a todos los colaboradores a nuevas acciones a realizar y/o ajustar dentro de cada área con el fin de dar cumplimiento al desarrollo del Sistema De Seguridad De La Información (SGSI).

La presente circular rige a partir de la fecha de su expedición,

Comuníquese y Cúmplase,

EDGAR FABIO GARCÍA CASTAÑEDA
Director Administrativo

Elaboro y aprobó: Christian Armando Valero- Jefe de Oficina TICS
Verifico: Francisco Javier Bello Pinzón- Jefe Oficina de Planeación.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN COMCAJA

CONTENIDO

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información son derechos desarrollados basados en las guías y controles de cumplimiento a la ISO 27000 por medio de las cuales COMCAJA acoge con el fin de dar cumplimiento normativo.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013, así como a los anexos son derechos reservados por parte de ISO/ICONTEC, se tomarán algunas definiciones incluidas en la Ley 1581 de 2012, aplicadas a la estructura actual de la cual estar sujeta a cambios para mejorar la implementación de la seguridad información a nivel institucional.

2. AUDIENCIA

El documento está elaborado para tener la política de implementación de al Modelo de Seguridad y Privacidad de la Información de COMCAJA, así como proveedores de servicios y terceros que hacen uso de vinculación con la entidad.

3. INTRODUCCIÓN

COMCAJA reconoce y considera la información como el activo de mayor importancia para la entidad y eje primordial para el cumplimiento de sus objetivos misionales. Por lo que se hace necesario el establecimiento de reglas y medidas que permitan proteger la confidencialidad, integridad, y disponibilidad de la información de la entidad.

El presente manual de políticas constituye parte fundamental del sistema de gestión de seguridad de la información las cuales deben ser adoptadas por los directivos, funcionarios, contratistas y terceros que laboren o tengan relación con la entidad y se convierten en la base para la implantación de controles, procedimientos y estándares, que contribuyen a la prevención, protección y manejo de los riesgos de seguridad de la información para la entidad enfocadas en el cumplimiento de la normatividad legal Colombiana vigente y buenas prácticas de seguridad de la información basadas en el modelo de seguridad y privacidad de la información norma ISO 27001:2013.

4. PROPÓSITO

El siguiente documento permite dar a conocer la política general de seguridad y privacidad de información de COMCAJA, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015. Y a su vez será el insumo de consulta a las acciones que se realizaran tanto por colaboradores como proveedores que hagan parte e Comcaja en el uso de las buenas prácticas de manejo a nivel de tecnología y enfocada en el cumplimiento de controles de seguridad interno y externos.

5. GLOSARIO

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén

configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Seguridad de la información: Conjunto de procedimientos y herramientas de seguridad que protegen ampliamente la información confidencial de la empresa frente al uso indebido, acceso no autorizado, interrupción o destrucción.

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección de COMCAJA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para COMCAJA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por dar cumplimiento a los siguientes objetivos:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de COMCAJA
- Garantizar la continuidad del negocio frente a incidentes.
- COMCAJA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Finalmente se realizara la actualización e ingreso de otras políticas para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que son el apoyo sobre el cual se desarrolla; dentro de estas se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. El documento estará a detalle dentro de la "Guía de políticas específicas de seguridad y privacidad de la información" y mencionar aquellas que la Entidad haya establecido como necesarias y primordiales. De esta forma se presenta el siguiente ejemplo:
A continuación se establecen 11 principios de seguridad que soportan el SGSI de COMCAJA:

1. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
2. COMCAJA protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
3. COMCAJA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
4. COMCAJA protegerá su información de las amenazas originadas por parte del personal.
5. COMCAJA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. COMCAJA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. COMCAJA implementará control de acceso a la información, sistemas y recursos de red.
8. COMCAJA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9. COMCAJA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
10. COMCAJA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
11. COMCAJA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Formato #2 de Política de Seguridad y Privacidad de la Información

El siguiente documento es un formato de política de Seguridad y Privacidad de la Información *La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de COMCAJA con respecto a la protección de los activos de información (**los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software**), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.*

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de COMCAJA y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y en cumplimiento a las estrategias y objetivos del negocio de COMCAJA deberán dar cumplimiento un 100% de la política.

A continuación se establecen las 12 políticas de seguridad que soportan el SGSI de COMCAJA:

1. COMCAJA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
3. COMCAJA protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
4. COMCAJA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. COMCAJA protegerá su información de las amenazas originadas por parte del personal.
6. COMCAJA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. COMCAJA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. COMCAJA implementará control de acceso a la información, sistemas y recursos de red.
9. COMCAJA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. COMCAJA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
11. COMCAJA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
12. COMCAJA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

7. FASES DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para realizar una correcta implementación de políticas de seguridad de la información, es necesario cumplir con una serie de fases, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice e interiorice para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la entidad.

IMPORTANCIA DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Para COMCAJA es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad.

FASES DE IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN

1. Desarrollo de las políticas: En esta fase se incluye a todas las áreas para la creación de las políticas, estructuración, documentación, revisión y aprobación; por lo cual para llevar a buen término esta fase se requiere que se realicen actividades de verificación e investigación de los siguientes aspectos:

- **Justificación de la creación de política**: COMCAJA basados en la importancia del manejo de activos para la toma de decisiones y enfocados en el cumplimiento de informes a entes de control asume la obligación de realizar la creación de la política de seguridad de información y determinar los controles que se consideren necesarios para su implementación.
- **Alcance:** Áreas misionales y administrativas de COMCAJA. Proveedores, afiliados y demás que puedan tener un tipo de vinculación en el manejo de activos de la entidad
- **Roles y Responsabilidades:** Se encuentra documento específico determinando las acciones y responsabilidades para el cumplimiento de la política.
- **Revisión de la política:** Actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de los miembros del comité de SGSI y así evaluar la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de la misma. Lo anterior teniendo en cuenta que pueden presentarse más acciones que permitan madurar la implementación de controles de seguridad y el levantamiento documental de procedimientos.
- **Aprobación de la Política:** Proceso que estará a cargo de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de la misma. Persona que permitirá que se tenga todo el respaldo enfocado en la implementación de dicha política y el desarrollo de controles dentro de COMCAJA.

2. Cumplimiento: Política que al estar revisada, verificada, implementado y aprobada en el manejo de los controles de seguridad de la Información.

3. Comunicación: Política que será socializada a todo el personal por medio del proceso de talento humano y así tener el debido alcance esperado para que los controles puedan surgir el efecto de cumplimiento. Esta incluirá funcionarios, contratistas y/o terceros de la Entidad. Todos los funcionarios contratistas y/o terceros de la entidad debe conocer la existencia de las políticas, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requieran.

4. Monitoreo: Importante por medio del comité realizar la revisión de acciones o controles que permitan generar que la política sea dinámica y que cada proceso que se realiza a nivel de áreas puedan contar con las debidas acciones siempre encaminadas a la protección de los activos de la entidad.

5. Mantenimiento: Teniendo en cuenta las actualizaciones, cambios de manejo, desarrollos y demás acciones realizadas dentro de COMCAJA la política se deberá realizar las actualizaciones y los ajustes necesarios y a su vez ser retroalimentaciones a las todos los actores que hacen parte de la misma.

6. Retiro: Fase mediante la cual se hace eliminación de una política de seguridad en cuanto esta ha cumplido su finalidad o la política ya no es necesaria en la Entidad. Esta es la última fase para completar el ciclo de vida de las políticas de seguridad y requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema. Acción que generaría un retroceso en la entidad ya que los activos y las buenas prácticas a nivel de tecnología estarían expuestos para poder ser manejadas por otros terceros en beneficio propio y no de COMCAJA.

8. POLITICAS ESPECÍFICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN- COMCAJA

Teniendo en cuenta la creación de la política bajo la circular 12 del 2013 se realizará la actualización de la misma aplicándola al alcance actual la cual se describe a continuación:

"COMCAJA es una Entidad que cumple funciones de seguridad social dedicada al recaudo de los aportes de las empresas afiliadas y la prestación de servicios sociales de capacitación, recreación, vivienda entre otros, así como el pago de la cuota monetaria y su objeto social se centra en mejorar el bienestar de los afiliados y sus familias."

En la actualidad COMCAJA opera con cinco sedes distribuidas de la siguiente manera: **Sede Principal:** Nivel Central ubicada en Bogotá. **Departamentales:** Inírida (Guainía), San José del Guaviare (Guaviare), Vaupés (Mitú) y Puerto Carreño (Vichada);

A nivel general se cuenta con la siguiente infraestructura tecnológica sobre la cual están soportadas las diferentes operaciones de la Caja:

- Servidores
- Terminales o estaciones de trabajo de los usuarios internos de la Caja
- Equipos de comunicaciones: Switches, Routers
- Equipo de seguridad: Firewall
- Red de comunicaciones: Lan y Wan
- Sistemas Operativos
- Aplicativos
- Software de ofimática
- Internet
- Intranet
- UPS´s
- Aire Acondicionado
- Cableado de datos y regulado
- Data center

A continuación se agruparan las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad.

8.1 ORGANIZACIÓN DE LA SEGURIDAD INFORMATICA

Teniendo en cuenta que ya se tiene definida una circular en el manejo del comité de seguridad informática se deja el texto de la siguiente manera, realizando algunos ajustes:

"De acuerdo con la normativa vigente incluida dentro de la circular 023 de la Superintendencia del Subsidio Familiar, el comité de Seguridad Informática estará funcionalmente inmerso dentro del Comité de Control Interno.

La responsabilidad directa de dicha función estará a cargo del Jefe de TIC o del agente de seguridad de la información teniendo en cuenta el alcance de los roles y responsabilidades descritos dentro del mismo documento definido a nivel interno.
En cuanto a la periodicidad se realizara cuando se considere necesario, y se coordinará con el Comité las respectivas agendas de trabajo, para tratar diferentes aspectos y medidas tendientes a mejorar o implementar dentro de la seguridad informática de la organización.

El comité debe reunirse en forma periódica y la persona delegada, será la encargada de presentar el informe donde se muestre el resultado de los seguimientos y monitoreo realizados, con base en los registros, bitácoras y otros tipo de soportes, con el fin de dar a conocer los puntos más susceptibles en la seguridad que actualmente se tiene implementada, para efectos de tomar las medidas y/o correctivos respectivos o en su defecto con el fin de realizar la

implementación nuevos controles hasta que encontrar la madurez de obtener resultados en la protección de activos de la entidad."

8.2 GESTION DE ACTIVOS

Para dar inicio al manejo de activos es importante tener el concepto enfocado a activos de seguridad de la información y de esta manera aplicar la guía de referencia entregada por el MinTIC para el levantamiento de activos de Comcaja. Con lo anterior se toma una breve explicación de internet la cual dice: *"Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección. Los activos se encuentran asociados, de forma directa o indirectamente, con las demás entidades."*

Teniendo en cuenta con la anterior definición se deben tener en cuenta 7 capítulos y determinar el debido manejo de los activos de COMCAJA los cuales se explican a continuación:

Identificación de Activos: por cada área se encuentra una seria de activos que se manejan para el reporte, consulta y captura de datos que en su gran mayoría de veces son datos sensibles que permiten la toma de decisiones y que para estos se deben definir periodos de verificación en cuanto a cambios normativos, manejo de información, proceso de manejo desde la captura hasta el procesamiento, custodia, reserva, protección de datos entre otras causas que podrán identificar el activo a un nivel de procedimiento y así conocer el manejo del activo. Para esta política es importante definir que el proceso de identificación de activos debe estar relacionado con la TRD (tablas de retención documental) y a su vez direccionados por medio del mapa de procesos el cual permitirá darle una organización interna a la entidad en cuanto a los puntos antes descritos. Proceso que está a cargo de cada líder de área pues es el encargado de direccionar el debido manejo y de esta manera hacer entrega de manuales, procedimientos, formatos entre otros que lleven a identificar los activos de COMCAJA.

Clasificación de Activos: COMCAJA por medio de la identificación de activos que se manejan por proceso determinara la clasificación de los activos de información de acuerdo a la criticidad, sensibilidad y reserva de la misma. En la elaboración de esta política debe tenerse en cuenta las leyes y normatividades actuales que afecten a la Entidad, algunos ejemplos: Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo a la naturaleza de la entidad.

Etiquetado de la Información: COMCAJA dentro del desarrollo de la guía de identificación y clasificación de activos determinara el mecanismo, responsable y obligatoriedad para el etiquetado o rotulación de Activos.

Devolución de los Activos: Anexo al manejo de los formatos de paz y salvo debe hacer una verificación por parte del líder del proceso y en apoyo al proceso de tecnología si así lo requiere en cuanto a la custodia y verificación de la información entregada al área el cual es de obligatoriedad para que los funcionarios, contratistas y/o terceros una vez finalizado el empleo, acuerdo o contrato que se tenga con COMCAJA.

Gestión de medios removibles: Teniendo en cuenta que COMCAJA no cuenta en la actualidad con procedimientos definidos para evitar la extracción de información se hace referencia al manejo de manera directa por parte del líder del área quien realizara la revisión del tipo de activo esta extrayendo y el manejo que le dará a esta. Por otra parte identificar que una vez se tenga generado los controles de manejo de puertos para evitar la extracción de los activos se dejara el cierre total en los equipos y será autorizado únicamente por el líder del área. Por ningún motivo la información o activos deben ser usados para fines particulares.

Disposición de los activos: Teniendo en cuenta que COMCAJA no cuenta en la actualidad con procedimientos definidos para evitar la verificación segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los activos. Se determina realizar backups de los activos evitando así el acceso o borrado no autorizado de

la información; con lo anterior y en busca de definir los la implementación de controles se debe generar los compromisos de responsabilidad los cuales estará a cargo del líder del área quien será el encargado de emitir las correspondientes autorizaciones y debe aplicar tanto para medios removibles como activos de procesamiento y/o almacenamiento de información.

Dispositivos móviles: el líder del área será el encargado de definir qué persona podrá tener el manejo de acceso a la red de COMCAJA el cual aplicar tanto como para funcionarios, contratistas o terceros que pueden tener acceso a las redes inalámbricas, quiénes pueden realizar instalación de chats corporativos y/o correos electrónicos de la entidad mediante el uso de este tipo de dispositivos, adicionalmente debe describir las responsabilidades que deben tener los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles así como como los controles de seguridad que la entidad utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.

8.3 CONTROL DE ACCESO

Este grupo de políticas hacen referencia a todas aquellas directrices mediante las cuales COMCAJA determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos; las políticas relacionadas con el control de acceso deben contemplar como mínimo:

Control de acceso con usuario y contraseña: los usuarios que hacen uso de los equipos de cómputo de COMCAJA cuentan con una cuenta el cual es entregada al momento de recibir el equipo. Es importante resaltar que envista de que no se tiene un servidor de dominio el manejo de usuarios y contraseñas se entrega como única vez de inicio y que una vez el empleado termine su vínculo laboral se deberá hacer entrega de la contraseña asignada para así poder extraer la información para ser validada por el líder del área.

Suministro del control de acceso: El manejo de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios se centra en las herramientas definidas por medio de las aplicaciones y sistemas de información que actualmente tiene COMCAJA y que son definida por el área TIC como único responsable del usuario administrador para la creación, modificación o inactivación de usuario. Por ningún motivo usuario no debe instalar o utilizar programas que no hayan sido previamente adquiridos y/o autorizados por el área de informática. No debe aceptar la ejecución de programas cuya descargar se active de forma no solicitada

Gestión de Contraseñas: Comcaja dentro del manejo de asignación de contraseñas indicar a los funcionarios, contratistas y/o terceros los parámetros mínimos para que una contraseña sea considera como fuerte o segura, y que por otra parte se recomienda sea diferente al del manejo de las aplicaciones y sistemas de información con el fin de tener la autenticación y acceso a la información de forma segura. Mientras se realiza la implementación de controles se informa la importancia de realizar cambios periódicos de manera personal ya que esto permitirá tener un control tanto de la información suministrada como la información recolectada dentro del equipo de cómputo como en los diferentes sistemas de información que pueda manejar el colaborador.

Perímetros de Seguridad: teniendo en cuenta referencia de la política definida en el 2013 se toma como referencia las acciones a realizar enfocadas en los controles y se ajustan a la vigencia actual en el cual se busca dar cumplimiento a herramientas que permitan mejorar este tipo de controles: en el data center la puerta de ingreso debe disponer de cerraduras y chapas con llave la cual actualmente continua con el mismo control pero es importante generar un tipo de acciones más encaminadas a la protección por medio de tarjetas o de huella y así poder dejar registro en la base de datos. Lo anterior teniendo en cuenta que el listado que se encuentra de ingreso no es diligenciado y no es nada seguro para la captura de ingresos a personal no autorizado; la señalización aunque es importante tenerla como área restringida es más seguro que el data center se encuentre en área de fácil inspección por parte del área TIC; el manejo del aire acondicionado aunque no se encuentra definido como un tema de acceso si

es de vital importancia contar con este elemento en buen estado y dejar dentro de cada vigencia el manejo presupuestal para su respectivo mantenimiento; por ultimo dentro de la política definido anteriormente se señala una serie de verificación que van en cumplimiento tanto al buen manejo del data center también aplica de una u otra manera a minimizar riesgos de daños físicos como lo son: Piso de cerámica y / o alfombra antiestática, Sensores de incendios para alertar la presencia de fuego en las instalaciones, UPS activas para que respalden en caso de bajas de luz, Extintores para utilizar ante la presencia de fuego en la sala de cómputo en caso de presentarse, Red eléctrica regulada y probada, Ventilación y luz adecuadas en la sala de servidores. Los anteriores antes descritos deben ser evaluados y por último y no menos importante la certificación del cableado de datos en cumplimiento a la transición de IPV6 la cual no se encuentra definida en el anterior documento de la política.

Áreas de Carga: Teniendo en cuenta que el data center se encuentra en la sede principal se debe evaluar la importancia de estar cerca al área TIC y aunque no se presenta ruta cruzada de despacho o descarga por parte de los proveedores, no exime que estos puedan acercarse al data center y poder hacer ingreso lo cual estaría de manera vulnerable a los activos de COMCAJA.

8.4 NO REPUDIO

La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción. La política expresa los siguientes aspectos a tener en cuenta para su cumplimiento:

Trazabilidad: Al contar con los sistemas de información de SISU y Sysman estos permiten contar con información de las acciones realizadas para consulta, si bien es cierto que los aplicativos se encuentran divido para procesos misionales y ERP (administrativos) al realizar la unificación se realizara la verificación de movientes trazables por medio del usuario entregado para el ingreso de estas aplicaciones, por otra parte se encuentra que una vez se tenga el servidor de dominio se podrá realizar la trazabilidad de acciones en la red y la implementación de controles para el manejo de políticas encaminadas a la protección de activos de COMCAJA. Por lo anterior es importante resaltar que el usuario y contraseña de manejo de aplicaciones no debe ser compartido y que es de uso único a los colaboradores que realizan acciones dentro de estos sistemas de información, correos, plataformas etc.

Retención: La información suministrada por parte de los colaboradores, terceros, proveedores y cualquier persona que tenga una relación en COMCAJA manejara los controles de acceso a la base de datos de manera única por parte del proceso TIC, en cuanto a información documental creada por medio de guías, manuales, procedimientos, formatos etc. son salvaguardados por los líderes de las áreas y de fácil consulta bajo las TRD de COMCAJA para contar con la retención o respaldo de acciones o de derechos de autor de la entidad.

Auditoría: con la estabilización y unificación de los sistemas de información se realizar a la revisión por medio de los reportes a entregar por entes de control el cual como única fuente se tendrá la información consignada en la base de datos y bajo esta realizar si se presenta desviación en cuanto las acciones realizadas vs las consignadas en el sistema de información de COMCAJA. Por lo anterior la importancia de consignar toda acción dentro de los sistemas de información para poder realizar las auditorias desde el los líderes de proceso hasta llegar a evaluar sin algún procedimiento a nivel de software presenta inconvenientes y de esta manera realizar el perfilamiento hasta encontrar una desviación de cero errores.

Intercambio electrónico de información: con el fin de manejar la información consignada dentro del sistema de información que maneja COMCAJA y en busca de fortalecer las comunicaciones directa a plataformas externas se recalca la importancia de hacer el registro completo como única línea de transferencia de información y a su vez de contemplar la importancia de seguir con el contrato de mantenimiento a nuevos desarrollos que se puedan presentar de manera normativa para así poder tener la relación en el menor tiempo posible verificando que se cumplan criterios en cuanto a envías y tiempos definidos.

8.5 PRIVACIDAD Y CONFIDENCIALIDAD

En cumplimiento al manejo de la protección de datos personales, se definen:

8.5.1 Ámbito de aplicación: El cumplimiento a leyes definidas a nivel interno y externo como ley 1581 de 2012, ley 2157 de 2021 y decreto 1377 de 2013 se deben realizar los ajustes procedimentales en cuanto a el debido manejo de los datos personales y/o datos sensibles que se tienen tanto de afiliados, como de proveedores y terceros que se encuentran dentro de nuestros sistemas de información el cual en busca de la actualización permanente se busca la implementación de controles que permitan proteger este tipo de información.

8.5.2 Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales: Aplica información solicitada por algún ente como contraloría, procuraduría, fiscalía, policía u alguno que haga la solicitud de manera directa con el fin de revisar o buscar casos especiales el cual solo podrá ser autorizado por el director de COMCAJA y el Líder TIC para la entrega de información personal.

8.5.3 Principios del tratamiento de datos personales:

Principio de la Legalidad: el cumplimiento a leyes definidas a nivel interno y externo como ley 1581 de 2012, ley 2157 de 2021 y decreto 1377 de 2013

Principio de finalidad: la cual debe ser expresada al afiliado, proveedor, colaborador, terceros etc. en el cual se informa que los datos entregados serán de uso netamente para temas de manejo administrativo con el fin de realizar las acciones por las cuales se decepcionan y no tendrán uso diferente al manejo de plataformas para cubrir las necesidades al usuario.

Principio de libertad: Toda información suministrada por el afiliado, proveedor, colaborador, terceros etc. será recepcionada o recibida por COMCAJA únicamente con la autorización del titular quien estará de acuerdo que este tipo de datos tendrán una reserva y buen manejo para acciones administrativas y el cual estará supervisado por el área encargada de recibirla en el manejo del buen tratamiento de la información.

Principio de veracidad o calidad: Por ningún motivo se realizar la recepción por parte de COMCAJA de información sin validación de soportes como cedula, Rut, cámara de comercio entre otras que apliquen, lo anterior ya que afectara el debido manejo de verificación ante otras plataformas o en el buen uso de registro a las bases de datos. Por ningún motivo se incluirá datos sin su respectivo soporte o validación del titular y así no afectar el debido proceso administrativo para lo cual fue entregada la información por parte del afiliado, proveedor, colaborador, terceros etc.

Principio de transparencia: la información suministrada y almacenada en la base de datos de COMCAJA no podrá ser modificada sin plena verificación y a su vez se dejara consignada la trazabilidad de la persona que realiza el cambio por medio del ID o Usuario entregado con el fin de tener el soporte ante alguna novedad que se llegase a presentar por parte del afiliado, proveedor, colaborador, terceros etc.

Principio de acceso y circulación restringida: Las plataformas que permitan hacer uso de verificación de la información tendrá parámetros de validación de datos personales o de parámetros previstos dentro de la normatividad vigente, con el fin de no tener suplantación o mal manejo de soportes para fines diferentes a los cuales fueren entregados a COMCAJA.

Principio de seguridad: Toda la información suministrada estará protegida a nivel técnico por parte de los controles implementados en los sistemas de información que se manejen; a nivel humano que será el primer filtro de

verificación de información recepcionada y administrativa con el fin de validar parámetros normativos enfocados en dar el buen uso de información y generar los controles o validaciones pertinentes. Los anteriores actores de validación por parte de COMCAJA serán los responsables directos en que la información cuente con la privacidad, disponibilidad, confidencialidad, integridad y no repudio a los datos de los afiliados, proveedores, colaboradores, terceros etc.

Principio de confidencialidad: Todos los colaboradores que participen en el manejo de tratamiento de datos están en la obligación de manejar este tipo de información a manera de reserva y el cual se encuentra descrita dentro de las obligaciones contractuales las cuales serán motivo de aplicar las acciones legales en caso de incumplimiento.

8.5.4 Derechos de los titulares: Los titúlares de la información están en su derecho de:

Conocer, actualizar y rectificar sus datos personales: Con el fin de manejar datos de cambio de residencia, celular y demás que puedan afectar a la recepción de trámites o en cumplimiento al manejo de las bases de datos para los beneficios que tienen derecho. De igual manera podrá realizar al verificación por parte de los canales de comunicación y a su vez el colaborador de COMCAJA tendrá la obligación de hacer la validación al recibir este tipo de peticiones o en casos de requerir un soporte con el afiliado para así realizar la actualización permanente y evitar riesgos de mala captura de información o mala digitación por parte un anterior colaborador dentro de los diferentes sistemas de información que se manejan en la entidad.

Solicitar la prueba de su autorización para el tratamiento de sus datos personales: COMCAJA en cumplimiento al debido manejo de tratamiento de datos personales conserva los soportes de autorización, los cuales pueden ser entregados al afiliado, proveedor, colaborador, terceros etc. Para así dar el debido proceso de transparencia y buen eso de la información entregada a la entidad.

Ser informado respecto del uso que se le da a sus datos personales: Cuando se presente algún cambio a nivel transaccional o normativo que estén asociados con la conservación de datos personales, COMCAJA está en la obligación de realizar la socialización por los diferentes medios para así manejar de manera transparente el cumplimiento de privacidad, disponibilidad, confidencialidad, integridad y no repudio a los datos de los afiliados, proveedores, colaboradores, terceros etc.

Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere: El titular podrá solicitar que los datos no se sigan manejando para acciones por las cuales fueron entregados y se podrán inactivar dentro del sistema de información y no podrá ser eliminado por ningún motivo si se encuentra dentro del Banco los servicios o productos que dieron origen a dicha autorización.

Presentar quejas ante la entidad administrativa encargada de la protección de los datos personales: El titular está en su derecho de imponer la queja, denuncia y/o inconformidad por los diferentes canales de comunicación en caso de verificar alguna anomalía con el mal manejo de los datos personales entregados a COMCAJA y obtener respuesta en los tiempos establecidos según sea el caso.

8.5.5 Autorización del titular: Dentro de la página institucional se deja consignada el manejo de a tratamiento de datos personales y en cada formulario se deja descrito el uso del cumplimiento y autorización de datos personales en los diferentes procesos que se manejan con COMCAJA.

8.5.6 Deberes de los responsables del Tratamiento: Los afiliados, proveedores, colaboradores, terceros etc. Están en la obligación o deber de informar y garantizar el ejercicio de los derechos de los titulares de los datos personales, tramitar las consultas, solicitudes y reclamos que halla a lugar de alguna inconformidad, los datos entregados se usaran únicamente que se encuentren autorizados, se implementaran los controles y o reglas para dar cumplimiento a

las condiciones de seguridad y privacidad de información del titular y cumplir con las instrucciones, normatividad, requerimientos impartidos por la autoridad competente.

Política de controles criptográficos: Dentro de los sistemas de información que se tienen implementados para el manejo misional y administrativo se realizara la verificación del manejo de información confidencial y se generan los controles de roles y privilegios para evitar fuga de información por medio de la extracción de querys que puedan obtener la información por un canal diferente al de verificación de los módulos implementados. Estos controles serán solicitados y verificados de manera directa entre el área TIC y los proveedores encargados de la operación de los diferentes sistemas de información que maneja COMCAJA.

Todos los colaboradores, funcionarios y/o contratistas se encuentran en la obligación de dar cumplimiento al acuerdo de confidencialidad por medio del compromiso de no divulgar la información interna y externa que conozca de COMCAJA, así como la relacionada con las funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización. Esta política rige a partir de la publicación como documento institucional y en cumplimiento a los controles de seguridad de la información de todos los procesos que hacen uso de datos en sus diferentes áreas.

8.6 INTEGRIDAD

Todos los funcionarios, contratistas y/o terceros que hagan parte de COMCAJA se comprometen a dar el buen uso de manejo íntegro e integral de la información tanto interna como externa, y la cual será responsabilidad de cada líder de área socializar la política ya sea de manera verbal, física o electrónica, para ser adoptada, procesada y entregada o transmitida. De igual manera toda persona podrá conocer la política por medio de los canales de comunicación de COMCAJA y bajo esta se dará el debido proceso para hacer los procedimientos que hallan a lugar en caso de no estar de acuerdo en algún manejo que se le dará la información.
Toda información entregada a COMCAJA ya sea a través de los medios de comunicación o de manera física no debe presentar modificaciones ni alteraciones teniendo en cuenta que es un factor que afectaría el debido registro dentro del sistema de información que maneja COMCAJA.
Para el manejo de vinculación contractual, el compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información. La política de integridad, deberá establecer asimismo la vigencia de la misma acorde al tipo de vinculación del personal al cual aplica el cumplimiento.

8.7 DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

COMCAJA deberá contar con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información. Dentro de la identificación de riesgo se debe priorizar en un alto nivel la indisponibilidad o afectación de un servicio el cual es importante resaltar que el tercero contrato es quien directamente debe dar la respuesta en los tiempos acordados y que este proceso no depende directamente de las áreas como TIC o infraestructura; La política de disponibilidad evalúa los siguientes aspectos:

Niveles de disponibilidad: Teniendo en cuenta que la prestación de servicios de operación se encuentra suministrada por terceros (entiéndase por agua, energía e internet) se debe disponer en la verificación contractual el cumplimiento de los niveles de disponibilidad de servicios e información acordados con COMCAJA los cuales deben estar verificados como riesgos dentro del levantamiento técnico y a su vez identificar la necesidad de contar con plan de respaldo para el caso de energía (entiéndase por planta eléctrica) e internet (canal de respaldo) para de esta

manera no afectar la operación del negocio la cual debe dejarse consignada dentro del presupuesto de cada vigencia y poder tener el recurso con el fin de minimizar el riesgo.

Planes de recuperación: Cada acción debe tener un procedimiento de manejo identificando tipos de desviación y clasificar por medio de tiempos y a nivel de costo cuanto puede afectar a su operación por una no prestación del servicio ofertada por el tercero y a su vez definir el plan de acción a realizar para no afectar la operación, proceso que debe ser construido por cada líder de área en proponer la solución con las diferentes herramientas que pueden aportar a la continuidad de la operación. Ejemplo: para área misionales que hacen uso del SISU el manejo de internet desde celulares o desde casa para poder cargar la información y no afectar el cargue, para el área administrativa en caso de no contar con el registro de bancos poder realizar la solución de manera directa en las sedes de bancarias y realizar el proceso de pagos o solicitud de extractos para no afectar la operación; ejemplo para el manejo de reportes a plataformas como extraer la información en medios magnéticos y cargar ya sea desde casa o por medio de internet de celulares para cumplir con los compromisos. Las anteriores son algunas opciones que se pueden dar para no afectar los diferentes factores que pueden afectar la operación y a su vez generar la cultura del saber cómo actuar ante este tipo de eventos.

Interrupciones: Teniendo en cuenta la identificación de factores que puedan afectar la continuidad del negocio desde cada área y realizando la verificación de los respaldos que se tienen en COMCAJA cada líder debe encontrar los planes de acción que puedan apoyar o ejecutar al momento de presentarse algún inconveniente en la no prestación del servicio tecnológico y de esta manera no afectar a los afiliados, terceros, empleados etc. que se encuentren relacionados de una u otra manera con los diferentes sistemas de información que maneja la entidad.

Acuerdos de Nivel de servicio: COMCAJA al estar dependiente de la prestación de un servicio específicamente con el internet y la energía se debe dar cumplimiento a las respuestas definidas a nivel contractual y por otra parte iniciar con el nivel de escalamiento el cual el proceso TIC y de Infraestructura para este caso deberán ser el puente directo para reportar la No prestación del servicio y de esta manera realizar la socialización para informar a las áreas el tiempo posible de restauración del servicio. Es importante resaltar que los niveles de servicio dependen de manera directa de la respuesta por parte del tercero que presta el servicio y a nivel institucional identificando la importancia de los riesgos que este genera realizar el plan de respaldo para ser minimizado y tener el debido seguimiento de la implementación de controles

Segregación de ambientes: Tomando en cuenta que COMCAJA maneja varios sistemas de información (SISU, Sysman (en proceso de renovación o cambio, Orfeo y otras plataformas de reporte)) El área TIC en su búsqueda de realizar la implementación de controles realiza la validación de migrar los servicios a la nube y con este poder tener disponibilidad en los diferentes procesos internos y a su vez permitir al proveedor contar con un soporte de manera directa a los canales definidos para los inconvenientes que se presenten o para su debida actualización y desarrollo que se requiera dentro de los diferentes sistemas que hace uso la entidad.

Es importante resaltar que antes de colocar algún desarrollo en producción se cuenta con la fase de respaldo para verificar que los cambios a implementar tendrán el resultado esperado una vez sea aprobado por el líder del área o persona que hace uso de la herramienta para el registro de información. Por ningún motivo se implementara de manera directa en los módulos de producción sin antes tener la verificación de funcionamiento y de esta manera evitar rollback en los diferentes sistemas de información.

Gestión de Cambios: Teniendo en cuenta la evolución de los sistemas de información en cuanto a tecnológica o por el manejo de cumplimiento normativo de las entidades que nos vigilan se considera obligatorio que todo cambio que se realice dentro de los diferentes sistemas de información sean evaluados inicialmente por el líder del área y de esta manera dar el aval de funcionamiento para la implementación.

En cuanto a infraestructura se refiere antes de realizar alguna modificación a nivel físico se informara por parte del líder TIC el plan de trabajo con el fin de no afectar el manejo administrativo de otras áreas. Cualquier cambio que se vaya a realizar será socializado y aprobado antes de ser ejecutado.

8.8 REGISTRO Y AUDITORÍA

Responsabilidad: Teniendo en cuenta a nivel institucional el manejo de auditoria en cuanto a la revisión de controles y/o documentos administrativos consignados por el Área TIC. Las Oficina de Control Interno y revisoría Fiscal dentro de su plan de auditoria están en la obligación de dejar planteado el desarrollo de las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías al equipo directivo y de esta manera dejar definido los planes de mejoramiento a que haya lugar.

Almacenamiento de registros: Teniendo como referencia los controles y procesos realizados desde el área TIC se deben evaluar el cumplimiento al manejo de procedimientos como: copias de seguridad de la base de datos, Backups de equipos entregados por parte de los colaboradores y demás que sean de revisión de cumplimiento en cuanto a las actividades que se dejan plasmadas basados en el MSPI (controles ISO 27000).

Normatividad: Las auditorías realizadas por el área de control interno y revisoría fiscal adicional a los controles ISO 27000 deben estar alineadas con demás normatividades definidas por las entidades que nos regulan y así tener el soporte de controles implementados tanto dentro de los sistemas de información que maneja COMCAJA como a nivel de infraestructura física.

Garantía cumplimiento: Las auditorías realizadas por el área de control interno y/o revisoría fiscal debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de COMCAJA; así como recomendar las deficiencias detectadas para de esta manera definir el plan de acción por parte del proceso TIC o áreas que se encuentren involucradas para dar el debido cumplimiento.

Periodicidad: La política debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta COMCAJA, lo cual se logra a través de auditorías periódicas alineada a los objetivos estratégicos y gestión de procesos de la Entidad. Proceso que debe ser evaluado, actualizados y socializados por las áreas encargadas y una vez terminar la vigencia contar con los soportes de la implementación de controles hasta llegar al máximo punto de minimización del riesgo.

8.9 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

Dentro del desarrollo de guías suministradas por el MinTIC y las cuales fueron adaptados y adoptadas por COMCAJA se encuentra la guía de Gestión de Incidentes las cual explica a detalle la ruta de manejo en la materialización de algún evento que afecte la operación del negocio en el cual se explica de manera específica temas como:

Visión General (explicando: ¿Qué se debe reportar? ¿A quién debe reportarse?, ¿Qué medios pueden emplearse para hacer el reporte?), los roles y responsabilidades (como se debe escalar y encargar de gestionar los eventos), **Actividades** (manera general en que consiste el proceso de gestión de incidentes desde el reporte hasta la resolución), **Documentación** (documentación del esquema de gestión y los procedimientos) **Descripción Del Equipo Que Manejará Los Incidentes** (Se indica cómo está compuesta la estructura general para la gestión de incidentes y vulnerabilidades de seguridad) y **Aspectos Legales (referenciando el cumplimiento de** aspectos legales que se deben tener en cuenta o los cuales debe darse cumplimiento).

8.10 CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN:

Para que la política de seguridad tenga el resultado esperado dentro de COMCAJA el talento humano es el eje central para que este tenga éxito. Teniendo en cuenta que los controles que se implementen no servirían de nada si el personal realiza malas prácticas ya sea por desconocimiento o por no estar alineados con las políticas de seguridad informática de la entidad.

La política se encuentra alineada con el plan institucional de capacitaciones (PIC) en el cual buscara fortalecer conocimiento de manejo de las herramientas tecnológicas suministradas y para el personal que ingresa nuevo a la entidad dar a conocer el debido manejo tanto a nivel físico como a nivel de los diferentes medios tecnológicos a los cuales va a tener uso en su entorno laboral.

Es importante que el proceso de talento humano bajo su política defina la obligatoriedad de este tipo de información y a su vez cuente con soporte de evaluación en el cumplimiento a los planes y políticas de COMCAJA.

Por ultimo todo este tipo de capacitaciones permitirán que se mejoren en la implementación de más controles ya que permitirá al colaborador conocer temas de gran relevancia como es: ética empresarial, normatividad y afectaciones al no cumplimiento, manejo y protección de activos la cual aplica no solo a nivel institucional si no a cualquier actividad personal relacionada con tecnología.

8.11 PRÁCTICAS O LINEAMIENTOS DE CUMPLIMIENTO A TENER EN CUENTA EN SEGURIDAD DE LA INFORMACIÓN COMCAJA

- Hacer uso responsable y eficiente de los elementos y/o servicios tecnológicos que le sean asignados.
- Acatar medidas disciplinarias internas de tipo administrativo, por el incumplimiento a las políticas y procedimientos de seguridad establecidos.
- Hacer buen uso de la red eléctrica regulada la cual solo debe tener la conexión de equipos de cómputo (entiéndase por portátiles y/o computadores de mesa);demás dispositivos como impresoras, celulares, multi-tomas no deben estar conectadas a estas tomas
- La información que se maneje relacionada con las funciones del cargo, se considera propiedad de la COMCAJA y por lo tanto se podrá llevar el registro de la actividad de cada recurso informático, así como sacar copia de cualquier información, archivo, mensaje o conversación.
- El usuario (empleado, contratista, colaborador) es responsable de la información de la compañía y por lo tanto debe velar por su confidencialidad, seguridad, integridad, conservación, veracidad, consistencia y oportunidad
- La información es el mayor activo de la COMCAJA y se le debe dar el tratamiento correspondiente, cualquier irregularidad que se observe sobre la información propia y de terceros debe ser informada de manera inmediata al área de informática o realizar la actualización dentro de los sistemas de información que se manejan si el Rol o perfil lo permite actualizar para así contar con información real y veraz.
- El usuario (empleado, contratista, colaborador) no puede comunicar o facilitar a terceros información diferente a la divulgada en forma pública por COMCAJA
- El usuario (empleado, contratista, colaborador) en ninguna circunstancia debe buscar o usar los medios para adquirir, leer, ver, imprimir o tener acceso a información que no sea de su competencia.
- El usuario es responsable de asegurar que la información a su cargo tenga copia de respaldo con la periodicidad adecuada y siguiendo el procedimiento establecidos haciendo referencia aquella que se maneja diferente a las registradas dentro del sistema de información (ósea documentos Word, Excel, escaneados y demás que sirvan de soporte a las actividades diarias).
- La información de carácter privado o confidencial, será gestionada utilizando los mecanismos de seguridad definidos por el área de informática. Si en el proceso interviene un tercero, se coordinará con el los mecanismos y/o medios de seguridad. En caso de identificar algún movimiento de consulta, eliminación o sustracción por parte de algún usuario será informado al área jurídica con el fin de dar cumplimiento a la normatividad legal vigente.

- El usuario no debe almacenar información personal, confidencial o privada en carpetas públicas, ni en directorios compartidos de programas o dentro del equipo asignado por COMCAJA ya que estos podrán ser eliminados sin pleno aviso, teniendo en cuenta que esta es una herramienta institucional y puede generar un alto riesgo a la red adicional al espacio de almacenamiento que afecta de una u otra manera a los equipos tecnológicos de la entidad
- No debe instalarse o utilizar programas que no hayan sido previamente adquiridos y/o autorizados por el área TIC.
- No debe aceptar la ejecución de programas cuya descargar se active de forma no solicitada
- No debe instalarse o conectarse ningún equipo de comunicaciones ni dispositivo de almacenamiento (memorias USB, Palm, celulares, cámaras etc.), sin la previa autorización del área TIC y con el visto bueno del Jefe del área.
- El usuario debe revisar periódicamente que el antivirus se encuentre actualizado en su equipo. En caso contrario debe informar al área TIC.
- El usuario debe asegurarse que el equipo se bloquee después del tiempo de inactividad que se defina por el área TIC obligando a proveer la contraseña para desactivarlo nuevamente. En caso de no tener configurada la opción se debe realizar de manera manual (instrucción tecla de Windows + L), esto permitirá tener un control interno de protección de seguridad en la información que maneja del área.
- Como fondo de pantalla o escritorio del PC, únicamente podrá estar el oficialmente establecido como institucional
- El usuario no debe facilitar, ni compartir la contraseña a ninguna persona.
- Por razones de seguridad no debe utilizar las mismas contraseñas en los sistemas de información y la de ingreso al equipo de cómputo.
- No escribirla en papel ni en ningún documento del ordenador las contraseñas de manejo, lo anterior teniendo en cuenta que es la forma de identificar el manejo que realiza en los diferentes sistemas de información y puede ser utilizado por un tercero.
- Cambiar las contraseñas periódicamente. (Se recomienda cada 30 días.).
- Al finalizar la jornada laboral, el funcionario debe dejar completamente apagado su equipo de cómputo.
- Los equipos asignados deben mantenerse limpios, libres de polvo y suciedades (no se deben limpiar de manera directa con algún tipo de líquido como agua o alcohol)
- No colocar sobre los equipos o cerca de ellos bebidas, alimentos y otro tipo de elementos que puedan atentar contra los equipos y su funcionalidad.
- En el evento que algún equipo de mesa requiera ser trasladado a otro lugar dentro de las instalaciones, se debe realizar la solicitud directamente al área TIC, quienes serán las únicas personas que podrán ejercer la función de traslado desconexión y conexión de los mismos (haciendo la salvedad que no aplica para portátiles que puedan ser utilizados para presentaciones)
- La utilización de dispositivos y memorias en los puertos USB, serán concertado directamente con los líderes de área para determinar el manejo que tendrán este tipo de dispositivos.
- En la medida que se autorice la conexión de medios de almacenamiento a los puertos USB, estos deben primero ser escaneados con el antivirus, siguiendo las indicaciones dadas por el área TIC.
- En eventos que sea necesario enviar equipos a las diferentes sedes, se debe coordinar directamente con el área TIC, quienes se encargarán de realizar el proceso y adicionalmente gestionar el respectivo traslado de inventario dando aviso al área de Servicios Generales.
- Las únicas personas autorizadas para abrir los equipos de cómputo serán los funcionarios del área TIC o en su defecto los terceros delegados por dicha área.
- Toda persona que no pertenezca a COMCAJA se debe registrar en la portería siguiendo el procedimiento establecido por la administración del edificio y se debe notificar a la persona que busca para que autorice el ingreso y realizar el acompañamiento hasta finalizar la visita.
- En caso de traer equipos y/o elementos de cómputo, debe registrarlos en portería de acuerdo con el procedimiento establecido.

- Los equipos portátiles asignados a las dependencias no se pueden retirar de la COMCAJA. En situaciones especiales, debe tramitarse la solicitud ante el área TIC y dejar registro del equipo en la portería de las instalaciones de COMCAJA.
- El funcionario autorizado, es responsable del equipo y accesorios que retire de las oficinas de COMCAJA y de la información que contenga.
- Si el equipo que está a cargo presenta algún daño por parte del colaborador deberá informar al líder del área para realizar el manejo de reposición e informar al área TIC para verificar el arreglo o cambio del componente sea el adecuado y no afectar el activo de COMCAJA.
- Todo portátil externo que se conecte a la red de COMCAJA debe ser autorizado por el líder de área donde se va conectar e informar al área TIC para así identificar que este equipo cuente con el servicio por el cual se va a conectar y no genere afectaciones dentro de la red por estar en otro segmento de red y/o algún programa que pueda afectar a los configurados en la red local.
- El personal de informática debe ser informado para revisar que el portátil tenga como mínimo el software de seguridad instalado y actualizado (Antivirus, Anti Spam)
- La persona encargada de informática debe registrar en la planilla de control los datos básicos del portátil como son: Empresa , Nombre de la persona, Dirección MAC, Jefe que autoriza por parte de COMCAJA, Fecha y hora del inicio de conexión, Fecha y hora de desconexión, firma
- El área encargada de proporcionar el servicio de acceso institucional a Internet será el área de TIC, No se puede socializar la contraseña ya que esto puede afectar la operación de navegación a los equipos conectados al mismo recurso de internet.
- Los líderes de cada área determinarán qué usuarios funcionales tendrán derecho al servicio de Internet, e informar las restricciones que deban ser aplicadas.
- Es responsabilidad del líder y/o Colaborador informar según sea el caso, cuando se haya cometido una falta a los presentes lineamientos en cuanto al manejo de internet o malas prácticas ya que pueden afectar a todos los equipos de COMCAJA.
- Las sanciones por el uso inadecuado de los servicios de e-mail e Internet, se establecerán de acuerdo con las directrices que se estipuladas en el reglamento interno de trabajo y por las normas actuales en cuanto al mal manejo de herramientas tecnológicas
- No se puede hacer uso de los dispositivos móviles de uso personal (celulares, tabletas, etc.) para trasladar archivos no institucionales en ellos descargados, a los equipos de cómputo de la Caja
- Si encuentra dentro de la recepción de correos que hay un archivo adjunto sospechoso o link, abstenerse de abrirlo e informar de manera inmediata al área TIC para hacer la validación y no afectar el equipo en robo de información o daño a la red.
- El usuario no debe visitar sitios Web con contenidos pornográficos o similares ni sitios cuya información pueda resultar ofensiva, discriminatoria y que potencialmente represente peligro para nuestros sistemas.
- A nivel de Internet , no navegar por sitios desconocidos o de dudosa reputación
- No está permitido utilizar el correo electrónico de COMCAJA para fines diferentes a los de su trabajo.

8.12 FORMATO DE AUTORIZACION Y CUMPLIMIENTO A POLITICAS DE SEGURIDAD INFORMATICA COMCAJA

Basados en las políticas definidas todo colaborador que tenga acceso al recurso tecnológico de COMCAJA debe entregar el siguiente documento firmado aceptando las condiciones, políticas, reglas y manejo a los controles implementados en el buen uso de equipos, sistemas de información, internet, infraestructura física entre otras que fueron descritas en este documento y así ser anexo en el soporte de la hoja de vida en el proceso de talento humano.

AUTORIZACION Y CUMPLIMIENTO A POLITICAS DE SEGURIDAD INFORMATICA COMCAJA

En mi calidad de trabajador de la CAJA DE COMPENSACIÓN FAMILIAR CAMPESINA "COMCAJA" y con el fin de administrar de manera profesional, prudente, diligente y segura, la información de propiedad de COMCAJA, reconozco que:

1. Entiendo que toda la información que manejo relacionada con mis funciones, es de propiedad de la compañía y que por lo tanto se podrá llevar el registro de la actividad de cada recurso informático así como sacar copia de cualquier información, archivo, mensaje o conversación.
2. En la empresa y fuera de ella soy responsable de la información de la compañía y por lo tanto debo velar por su seguridad, integridad, conservación, veracidad, consistencia y oportunidad.
3. Estoy consciente del valor de la información y en tal sentido debo darle el tratamiento correspondiente, cualquier irregularidad que observe sobre la información propia y de terceros debo informarla de manera inmediata a la Sección de Informática y Telecomunicaciones.
4. No debo comunicar o facilitar a terceros ninguna información diferente a la divulgada en forma pública por la compañía.
5. De ninguna manera debo buscar, o usar ningún medio para adquirir, leer, ver, imprimir o tener ningún tipo de acceso, a información que no sea de mi competencia.
6. Soy responsable de asegurar que la información a mi cargo tenga copia de respaldo con la periodicidad adecuada.
7. Si la información es privada o confidencial, debe ir encriptada o protegida por contraseña y en todo caso la transmitiré y recibiré por los canales seguros establecidos por la Sección de Informática y Telecomunicaciones
8. No debo almacenar información secreta, confidencial o privada en carpetas públicas, ni de Outlook, ni en carpetas compartidas ni en ninguna otra de naturaleza pública.
9. Si de alguna manera estoy relacionado con la transmisión y recepción de información, aplicaré los estándares definidos por la Sección de Informática y Telecomunicaciones que apliquen para este tipo de procesos y me aseguraré que los terceros que envían o reciben, también lo hagan.
10. No debo instalar o utilizar programas que no hayan sido previamente adquiridos, de los cuales no se cuente con licencia de uso o que no haya sido autorizados por la Sección de Informática y Telecomunicaciones.
11. No debo guardar archivos mp3, fotos, textos cualquier otro documento que no sea de dominio público y cuya licencia de uso no haya sido previamente adquirida.
12. No debo instalar y/o conectar ningún equipo de comunicaciones ni dispositivo de almacenamiento (memoria USB, Tablets, Disco Externo USB, etc.), sin la previa autorización de la Sección de Informática y Telecomunicaciones.
13. No debo utilizar el correo electrónico institucional asignado para fines diferentes a los de la compañía.
14. No debo utilizar el correo electrónico enviando correo no solicitado ni correo masivo que pueda ser considerado como "Spam" y sancionado como tal.
15. Debo utilizar mi buen juicio al abrir mensajes de correo y attachments (adjuntos) con el fin de evitar el contagio de virus, gusanos y otros programas informáticos dañinos.
16. No debo visitar sitios Web con contenidos pornográficos o sitios en internet cuya información pueda resultar ofensiva, discriminatoria y que potencialmente sistemas. represente peligro para nuestros
17. La información que requiera guardar en discos o dispositivos magnéticos externos, necesariamente debe contar con la respectiva autorización del Jefe inmediato o de la Sección de Informática y Telecomunicaciones de acuerdo con el procedimiento establecido.
18. Debo asegurarme que mi equipo tenga configurado el protector de pantalla para activarse automáticamente, de acuerdo con el tiempo establecido de inactividad obligando a proveer la contraseña para desactivarlo nuevamente.

19. No debo facilitar, ni compartir mi contraseña a ninguna persona bajo ningún motivo
20. La estructura de mi contraseña no debe ser de fácil deducción y por seguridad no la debo escribir en ninguna parte.
21. No debo compartir ninguna carpeta de mi equipo a menos que haya sido expresamente autorizado para ello por la Sección de Informática y Telecomunicaciones. De ninguna manera debo compartir las carpetas del sistema.
22. Debo procurarle a mi equipo el cuidado que requiere evitando el mal uso y el abuso.
23. Para efectos de solicitar soporte, debo seguir los lineamientos establecidos por la Sección de Informatica y telecomunicaciones.
24. Debo calificar el servicio de soporte, incluyendo las observaciones que considere pertinentes una vez sea realizado el servicio.

Equipos audiovisuales y computadores Portátiles

25. Soy responsable de los elementos, equipos y accesorios que bajo determinadas circunstancias retire de las oficinas de COMCAJA y de la información que contenga. Previamente debe existir la autorización del Jefe inmediato o de la Sección de Informática
26. Cualquier información secreta, confidencial o privada debo almacenarla en carpetas seguras. Si no sé cómo hacerlo, debo solicitar a la Sección de Informática y Telecomunicaciones una capacitación al respecto.
27. Es de mi conocimiento, que al utilizar un equipo portátil para trabajar en lugares públicos como una sala de espera o un avión, estoy exponiendo la información en la pantalla a terceros que pueden estar observándola.
28. Soy consciente que, al conectar el computador portátil a Internet a través de un proveedor de acceso a Internet externo, no cuento con las protecciones que me ofrece el firewall de la compañía por lo que debo tener aún más cuidado con los sitios por los que navego y la
29. información que acceso. En particular, no debo abusar de la falta de restricciones ni descargar programas ni instaladores que no pueda descargar desde la compañía.

Debo tener una cuenta personal de correo electrónico con un proveedor de acceso a Internet ode servicio gratuito de correo para utilizar en caso de contingencia. Mi dirección de correo electrónico personal es:

_____

Autorizo a COMCAJA para gestionar la adecuada protección de mis datos personales que en adelante residan en sus archivos, así como al respectivo tratamiento de información que deban cumplir de acuerdo con la ley y políticas regulatorias que apliquen a la entidad.

En constancia de que entiendo y acepto lo anterior firmo la presente:

Firma: _____
Nombre: _____
Nro. Identificación: _____
Área: _____
Cargo: _____
Fecha: _____