1. OBJETO

Establecer las directrices y los lineamientos relacionados con el manejo seguro de la información, enmarcado en estándares internacionales de seguridad (v gr. ISO 27001) y en normas de entes reguladores, SIC - Ley 1581 de 2012 y sus decretos reglamentarios o posteriores que las deroguen o modifiquen).

La presente Política de Seguridad de la Información y ciberseguridad es una declaración de las políticas, responsabilidades y de la conducta aceptada para proteger la Información de Central de Cobranzas S.A.S.

1.1 OBJETIVO GENERAL

El principal objetivo de la Política de Seguridad de la Información y ciberseguridad en Central de Cobranzas S.A.S., es proteger la organización frente a situaciones que representen riesgo para la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información, donde se establezcan los servicios propios y de terceros de la compañía. Además de dictar los principios de gobernanza y las reglas comunes formalizadas en las políticas que garantizan la protección efectiva de la información y la coherencia del sistema de gestión de seguridad de la información, así mismo La Alta Dirección de Central de Cobranzas S.A.S, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación y mejora continua de un sistema de gestión de seguridad de la información.

1.2 OBJETIVOS ESPECIFICOS

Los objetivos específicos que persigue La Política de Seguridad de la Información y ciberseguridad son:

a. Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información.

b. Administrar los riesgos en seguridad de la información y ciberseguridad.

c. Establecer los canales de comunicación que le permitan conocer los resultados del Sistema de Gestión de Seguridad de la Información.

d. Proteger la imagen, los intereses y el buen nombre de Central de Cobranzas S.A.S.

e. Fortalecer la cultura de seguridad de la información en los colaboradores y terceros de la empresa.

f. Asegurar el cumplimiento de los requisitos legales y normativos en materia de seguridad de la información.

2. ALCANCE

Esta Política de Seguridad de la Información y Ciberseguridad aplica para todos los niveles de la organización: Usuarios (que incluye empleados y accionistas), Clientes, Terceros (que incluye proveedores y contratistas), Entes de Control y Entidades Relacionadas; que acceden, ya sea interna o externamente, a cualquier activo de información independiente de su ubicación.

Adicionalmente, la presente Política aplica a la información creada, producida, modificada, procesada o utilizada por la compañía.

3. DEFINICIONES

- **Colaboradores:** Son los usuarios de la información de la compañía.
- **Confiabilidad:** La información debe ser la apropiada para la administración de la Compañía y el cumplimiento de obligaciones.
- **Controles:** Salvaguardas basadas en dispositivos o mecanismos que se requieren para cumplir con los requisitos de una política.
- **Efectividad:** La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
- **Eficiencia:** El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.
- **Información o Información de la Compañía:** Es toda aquella que, sin importar su presentación, medio o formato, en el que sea creada o utilizada, sirve de soporte a las actividades de la compañía y la toma de decisiones.
- **Internet:** Es la conexión lógica de múltiples redes de comunicaciones, las cuales utilizan como estándar el protocolo TCP/IP para comunicarse y compartir datos entre dichas redes.
- **Miembro de la Comunidad:** Un individuo que tiene autoridad limitada y específica del responsable de información para ver, modificar, adicionar, divulgar o eliminar información.
- **Modelo de Seguridad de la Información y ciberseguridad:** Se refiere al conjunto de políticas, procedimientos, estándares, normas de seguridad, elementos de seguridad y topologías que garantizan la protección de la información de la Compañía que se encuentre alojada en la infraestructura tecnológica y el ciberespacio donde se establezcan los servicios de la entidad y/o los prestados a través de terceros.
- **Norma:** Conjunto de reglas requeridas para implantar las políticas. Las normas hacen mención específica de tecnologías, metodologías, procedimientos de aplicación y otros factores involucrados y son de obligatorio cumplimiento.
- **Organización de Seguridad de la Información y ciberseguridad:** Estructura organizacional que soporta la Seguridad de la Información y ciberseguridad, donde se definen roles y responsabilidades de cada uno de sus integrantes.
- **Perímetros o áreas seguras:** Un área o agrupación dentro de la cual un conjunto definido de políticas de seguridad y medidas se aplica, para lograr un nivel específico de seguridad. Las áreas o zonas son utilizadas para agrupar activos de información con requisitos de seguridad y niveles de riesgo similares, para asegurar que cada zona se separa adecuadamente de las otras.
- **Política:** Es un conjunto de ordenamientos y lineamientos enmarcados, en los diferentes instrumentos jurídicos y administrativos que rigen una función, en este caso la Seguridad de la Información y ciberseguridad.
- **Política de Seguridad de la Información y ciberseguridad:** Documento donde se establecen las directrices y los lineamientos relacionados con el manejo seguro de la información, que se encuentre alojada en la infraestructura tecnológica y el

ciberespacio donde se establezcan los servicios de la entidad y/o los prestados a través de terceros.

- **Procedimiento:** Pasos operacionales específicos que los individuos deben tomar para lograr las metas definidas en las políticas.
- **Recursos de información:** Dispositivos o elementos que almacenan datos, tales como: registros, archivos, Bases de Datos, equipos y el software propietario o licenciado por Central de Cobranzas S.A.S.
- **Responsable de la información:** Un individuo o unidad organizacional que tiene responsabilidad por clasificar y tomar decisiones de control con respecto al uso de su información.
- **Riesgo:** La probabilidad de que ocurra un evento en seguridad de la información, que cause pérdida a Central de Cobranzas S.A.S.
- **Seguridad de la información:** Protección de la información contra el acceso no autorizado accidental o intencional, su modificación, destrucción o publicación.
- **Seguridad física:** Protección de los equipos de procesamiento de la información de daños físicos, destrucción o hurto; asimismo, se protege al personal de situaciones potencialmente dañinas.
- **NTC-ISO/IEC 27001:** Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI). Requisitos
- **NIST 800-53:** Proporciona un catálogo de controles de seguridad para todos los Sistemas federales de información de los Estados Unidos. Referenciado por la CE 007 de 2018 como uno de los marcos de referencia a tener en cuenta para la gestión de riesgos de ciberseguridad.
- **Ciberseguridad:** Es el conjunto de políticas, conceptos de seguridad, recursos, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para prevenir el acceso, obstaculización, interceptación, daño, violación de datos, uso de software malicioso, hurto de medios y la transferencia no consentida de activos informáticos, con el fin de proteger a los consumidores financieros y los activos de la entidad en el ciberespacio.
- **Ciberespacio:** Corresponde a un ambiente complejo resultante de la interacción de personas, software y servicios en Internet, soportado en dispositivos tecnológicos y redes conectadas a la red mundial, propiedad de múltiples dueños con diferentes requisitos operativos y regulatorios.

Nota: Para el presente documento, se entenderá ciberespacio como el entorno donde se establezcan los servicios de la compañía y los prestados a través de terceros.

- **Ciber-amenaza o amenaza cibernética:** Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar un ciberataque contra la población, el territorio y la organización política del Estado.
- **Cibernética:** Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnicas de funcionamiento de las conexiones de los seres vivos y de las máquinas.
- **Ciberataque o ataque cibernético:** Acción organizada o premeditada de uno o más agentes para causar daño o problemas a un sistema a través del ciberespacio.

- **Ciber-riesgo o riesgo cibernético:** Posibles resultados negativos asociados a los ataques cibernéticos.
- **Evento de ciberseguridad:** 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.
- **SIEM (Security Information and Event Management):** Sistema de información que proporciona análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones, dispositivos de seguridad y los elementos de red. Suelen ser sistemas de centralización de logs.
- **SOC (Security Operation Center):** Entidad o dependencia, donde los sistemas de información empresarial (sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, escritorios y otros dispositivos) son monitoreados, evaluados y defendidos.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio.
- **Información en reposo:** Datos guardados en dispositivos de almacenamiento persistente (por ejemplo, bases de datos, almacenes de datos, hojas de cálculo, archivos, cintas, copias de seguridad externas, dispositivos móviles, discos duros, entre otros).
- **Información en tránsito:** Información que fluye a través de la red pública o que no es de confianza, como Internet y los datos que viajan en una red privada, como una red de área local (LAN) corporativa o empresarial.
- **Terceros críticos:** Terceros con quien se vincula la entidad y que pueden tener incidencia directa en la seguridad de su información.

4. CONDICIONES GENERALES

El propósito de este documento es dar a conocer a los colaboradores de Central de Cobranzas S.A.S., la Política de Seguridad de la Información y Ciberseguridad establecida para la protección de la información.

En el presente documento se incluyen los aspectos que deben tenerse en cuenta por parte de todos los colaboradores para que la información sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones de la Compañía (Confidencialidad); que esté protegida contra modificaciones no autorizadas, realizadas con o sin intención (Integridad), que esté disponible cuando sea requerida (Disponibilidad), que sea utilizada para los propósitos que fue obtenida (Privacidad).

Por lo tanto, los colaboradores deben actuar teniendo en cuenta los lineamientos consignados en este documento y los que se desarrollen en los procedimientos, guías y manuales que soportan la implementación de la Política de Seguridad de la Información y Ciberseguridad; en el entendido que la alta gerencia tiene el firme propósito de apoyar todas las actividades necesarias para alcanzar las metas y principios de seguridad de la información, de acuerdo con las responsabilidades asignadas dentro de la organización en relación con este tema.

4.1 PRINCIPIOS

Central de Cobranzas S.A.S., ha establecido como fundamentales los siguientes principios que soportan la Política de Seguridad de la Información y Ciberseguridad:

a. La Información es uno de los activos más importantes de Central de Cobranzas S.A.S. y por lo tanto debe ser utilizada acorde con los requerimientos de la Compañía y conservando criterios de calidad (Efectividad, Eficiencia y Confiabilidad).

b. La confidencialidad de la Información de la Compañía, así como aquella perteneciente a terceros, debe ser mantenida, independientemente del medio o formato donde se encuentre.

c. La Información de la Compañía debe ser preservada en su integridad, independientemente de su residencia temporal o permanente, o la forma en que sea transmitida.

d. La Información de la Compañía debe estar disponible cuando sea requerida y por quienes tengan autorización de utilizarla; asimismo, presentarse de forma oportuna cuando por requisitos legales y reglamentarios así se requiera.

e. La privacidad de la información de Central de Cobranzas S.A.S. debe ser preservada.

4.2 ORGANIZACIÓN DEL DOCUMENTO

El documento está organizado fundamentalmente en dos partes: En la primera, se describe el objetivo general de la Política de Seguridad de la Información y Ciberseguridad, sus características, los responsables y la forma en que debe ser desarrollada, aplicada y mantenida. En la segunda, se definen las Políticas individuales, para el manejo de la información y las acciones que deben ser tomadas para lograr los objetivos de la presente.

4.3 ORGANIZACIÓN Y RESPONSABILIDADES

La administración de esta Política será responsabilidad de quienes al interior de Central de Cobranzas S.A.S. desempeñen los roles que componen la Organización de Seguridad de la Información y Ciberseguridad.

4.3.1 Oficial de seguridad

El oficial de Seguridad de Central de Cobranzas S.A.S. está a cargo de la implementación del Sistema de Gestión de Seguridad de la Información y su mantenimiento en condiciones operativas dentro de su respectivo alcance. Como parte de su deber, sus misiones son:

- Hacer cumplir la implementación de las Políticas de SGSI
- Manejar las vigencias de las Políticas de SGSI de su alcance
- Garantizar que se sigan las buenas prácticas de seguridad
- Definir campañas específicas de formación y sensibilización
- Generar informes de seguridad, analizar indicadores de seguridad y presentarlos a la Dirección y al Comité de Seguridad de la Información y Ciberseguridad
- Coordinar acciones de seguridad de la Información
- Contribuir con todas las áreas de la Organización, al entendimiento y aplicación de las políticas operativas y procedimientos técnicos

- Atender, asesorar y monitorear auditorías locales de seguridad de la información
- Participar en las reuniones del comité de cambios de los sistemas de información que afecten su alcance
- Asegurar el mantenimiento en condiciones operativas del proceso de gestión de incidentes de seguridad;
- Asegurar el mantenimiento en condiciones operativas del Plan de Continuidad de Negocio en los temas de Seguridad de la Información.
- Recibir las auditorías externas en términos de seguridad de la información y ciberseguridad de clientes y entes externos.

4.3.2 Comité de Seguridad de la Información y Ciberseguridad

Responsable por asegurar la planeación, implementación y mantenimiento de La Política de Seguridad de la información y Ciberseguridad; al igual que de la ejecución de las acciones requeridas para mantener los niveles de seguridad establecidos.

4.3.3 Colaboradores (Usuarios de la Información)

Son los demás funcionarios que utilizan la información y son responsables de proteger los activos de información de Central de Cobranzas S.A.S. por medio del cumplimiento de la Política de Seguridad de la Información y Ciberseguridad. Así mismo, deben estar alerta para identificar y reportar cualquier incumplimiento o falta de las normas o procedimientos establecidos.

Central de Cobranzas S.A.S. definirá los roles y responsabilidades requeridos para completar la definición de la Organización de Seguridad de la Información y Ciberseguridad, propendiendo siempre por la segregación de tareas como método para reducir los riesgos en el mal uso de la información.

4.4 CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LA POLÍTICA

El cumplimiento de la Política de Seguridad de la Información y Ciberseguridad con sus respectivas normas es obligatorio para los Colaboradores. Cada Colaborador debe entender su rol, conocer y asumir su responsabilidad respecto a los riesgos en Seguridad de la Información y Ciberseguridad y la protección de los activos de información de Central de Cobranzas S.A.S.

Cualquier incumplimiento de esta Política que comprometa la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información, puede resultar en una acción disciplinaria que puede llegar hasta la terminación del contrato de trabajo y a un posible establecimiento de un proceso judicial bajo las leyes nacionales o internacionales que apliquen.

La Política de Seguridad de la Información y Ciberseguridad está basada en las mejores prácticas en Seguridad de la Información y Ciberseguridad y está acorde con la legislación nacional e internacional y por ende tomará los pasos necesarios, incluyendo las medidas disciplinarias y/o legales aplicables, para proteger sus activos y el uso de ellos.

4.5 ADMINISTRACIÓN DE LA POLÍTICA Y PROCEDIMIENTOS DE CAMBIO

La Política de Seguridad de la Información y Ciberseguridad se debe preservar en el tiempo. Por lo anterior, es necesario efectuar una revisión anual o ante cambios estructurales que afecten a Central de Cobranzas S.A.S., para asegurar que ésta cumple con el cambio de las necesidades de la Compañía.

El Oficial de Seguridad de la Información y Ciberseguridad es responsable de esta tarea y debe llevarla a cabo con la participación del Comité de Seguridad de la Información y Ciberseguridad.

Cualquier Colaborador puede sugerir modificar La Política de Seguridad de la Información y Ciberseguridad. Dichas inquietudes y sugerencias deben ser comunicadas al Oficial de Seguridad de la Información y deben ser evaluadas por el comité de seguridad de la información y ciberseguridad.

4.6 EXCEPCIONES A LA POLÍTICA

No hay excepciones a la presente Política.

4.7 IMPLEMENTACIÓN Y PROGRAMACIÓN DE LA POLÍTICA

La Política de Seguridad de la Información y Ciberseguridad involucra el desarrollo e implementación del programa de Seguridad de la Información y Ciberseguridad, integrado a la operación de Central de Cobranzas S.A.S.

Un programa efectivo de Seguridad de la Información es un proceso continuo, no un evento. Para lograr los objetivos establecidos en este documento, la presente Política anticipa y autoriza el desarrollo de políticas, procedimientos, guías y manuales detallados y otras medidas administrativas, los cuales serán publicados para conocimiento de los funcionarios; así como el desarrollo y/o la adquisición de herramientas de software que ayuden a detectar o prevenir ataques contra los sistemas donde reside la información de Central de Cobranzas S.A.S.

5. CONTENIDO

5.1 POLÍTICAS INDIVIDUALES

5.1.1 Seguridad de la Información en la Gestión de Proyectos

La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto. Para ello se debe tener en cuenta los siguientes lineamientos:

- Cumplir en todos los proyectos con las políticas de seguridad de la información establecidas en la compañía.
- Identificar si existen requisitos específicos de seguridad de la información que deban ser tenidos en cuenta, desde la planeación del proyecto y durante todas sus fases.
- Identificar los riesgos de seguridad de la información en el proyecto y establecer los acuerdos definidos frente a la protección de la información, identificando los controles necesarios.
- Identificar las responsabilidades en seguridad, para los proyectos de la compañía y dar cumplimiento a lo establecido como mecanismos de seguridad.

5.1.2 SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La información de Central de Cobranzas S.A.S., sin importar su presentación, medio o formato, en el que sea creada o utilizada para en las actividades de negocio, se califica como información de la Compañía o activo de información. La Seguridad de la Información de la Compañía es el conjunto de medidas de protección que toma Central de Cobranzas S.A.S., contra la divulgación, modificación, hurto o destrucción accidental o maliciosa de su información. Dichas medidas de protección se basan en el valor relativo de la información y el riesgo en que se pueda ver comprometida.

Los responsables de la Información son los responsables de asegurar que la información de la Compañía cuenta con la protección apropiada para así preservar la Confidencialidad, Integridad, Disponibilidad y privacidad de la información.

Central de Cobranzas S.A.S. debe disponer de los medios necesarios para asegurarse de que cada Colaborador preserve y proteja los activos de información de una manera consistente y confiable. Cualquier persona que intente inhabilitar, vencer, o sobrepasar cualquier control de seguridad será sujeto de las acciones disciplinarias correspondientes. Central de Cobranzas S.A.S. debe contar con una estructura organizacional de Seguridad la Información

5.1.2.1 PROPIEDAD INTELECTUAL

La Propiedad Intelectual se define como cualquier patente, derecho de autor, invención o información que es propiedad de Central de Cobranzas S.A.S.

Todo el material que es desarrollado mientras se trabaja para Central de Cobranzas S.A.S. se considera que es de propiedad intelectual y de uso exclusivo de la organización, por lo tanto, debe ser protegido contra un develado, descubrimiento o uso que menoscabe la competitividad de Central de Cobranzas S.A.S.

5.1.2.2 RESPONSABLE DE LA INFORMACIÓN

Central de Cobranzas S.A.S. utiliza información para realizar sus actividades. Esta se crea y se entrega a cada Colaborador para que pueda desarrollar y cumplir sus respectivas metas dentro del marco de la Compañía.

La información que Central de Cobranzas S.A.S. utilice para el desarrollo de sus objetivos de negocio debe tener asignado un responsable, quien la utiliza en su área y es el responsable por su correcto uso.

Así, él toma las decisiones que son requeridas para la protección de su información y determina quiénes son los usuarios y sus privilegios de uso. Central de Cobranzas S.A.S. actuarán como responsables de la Información, los Gerentes, Coordinadores, Supervisores, y demás titulares de las dependencias que reporten directamente a la Gerencia General o a quienes éstos deleguen.

5.1.2.3 CUMPLIMIENTO DE REGULACIONES

La Política de Seguridad de la Información y Ciberseguridad está acorde y apoya el cumplimiento de las leyes y regulaciones locales e internacionales relativas a la privacidad, la Seguridad de la Información y Ciberseguridad. Por lo tanto, tales requerimientos deben

ser incluidos en el desarrollo del Modelo de Seguridad de la Información y ciberseguridad y se deben establecer acciones específicas para mantener alineada permanentemente a Central de Cobranzas S.A.S. con tales disposiciones. Ejemplos de dichas disposiciones son el licenciamiento de software, las circulares de la Superintendencia Financiera, Superintendencia de Sociedades, entre otras.

Así mismo y con el fin de mantener un buen nivel de seguridad, esta Política se debe apoyar en las mejores prácticas de Seguridad de la Información y de la Ciberseguridad.

5.1.2.4 ADMINISTRACIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La información de la Compañía se debe proteger con base en su valor y en el riesgo en que se pueda ver comprometida. Por lo tanto, a través del Comité de Seguridad de la Información y Ciberseguridad, se debe realizar periódicamente un análisis del estado de la Compañía frente a la Seguridad de la Información y Ciberseguridad, para determinar o actualizar el valor relativo de la información, el nivel de riesgo a que está expuesta y el respectivo responsable.

Establecidos el nivel de riesgo y el valor de la información, cada responsable debe realizar una evaluación formal de riesgos, para que estos sean identificados, evaluados y se apliquen las acciones necesarias para subsanarlos o mitigarlos acorde con los niveles de riesgo permitidos por Central de Cobranzas S.A.S.

Cada usuario de la información debe estar enterado de los procedimientos de reporte de riesgos que puedan tener impacto en la Seguridad de la Información de Central de Cobranzas S.A.S., y se requiere que reporten inmediatamente cualquier sospecha u observación de un incidente a la Seguridad de la Información y la Ciberseguridad.

5.1.2.5 CAPACITACIÓN Y CREACIÓN DE CULTURA EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Central de Cobranzas S.A.S. debe contar con un programa permanente que permita asegurar que los usuarios y terceros están informados acerca de sus responsabilidades en Seguridad de la Información y Ciberseguridad y de las continuas amenazas que ponen en riesgo la información que maneja.

Los funcionarios y terceros deben estar enterados de los procedimientos de Seguridad de la Información y Ciberseguridad que deben aplicar adicionalmente a los que se requieren para realizar su función de trabajo.

5.1.3 ACCESO REMOTO

Esta política define las condiciones, directrices, acuerdos y restricciones que deben implementarse en las diferentes modalidades de teletrabajo de la compañía y el uso seguro de las herramientas tecnológicas suministradas para este fin, las cuales se encuentran alineadas con la legislación colombiana vigente.

Es responsabilidad de la Coordinación GTI, el Oficial de Seguridad de la información y en Coordinación con el área de Talento Humano, implementar medidas de seguridad para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares que se realiza trabajo remoto.

Para ello, se deben cumplir los siguientes lineamientos, teniendo en cuenta que el trabajo remoto requiere unas condiciones básicas tecnológicas que dan soporte a los trabajadores remotos en el desarrollo de sus funciones y que desprenden unas responsabilidades asociadas al manejo de la información en cuanto a su confidencialidad, integridad, disponibilidad y privacidad.

El uso de la información de Central de Cobranzas S.A.S. por Terceros ya sea que se encuentre en los aplicativos locales o en el ciberespacio y se acceda de manera ya sea local o remotamente, debe ser formalizado por medio de acuerdos y/o cláusulas que hagan obligatorio el cumplimiento de la presente Política.

En los contratos se debe incluir la obligación de proteger la información de Central de Cobranzas S.A.S, los requisitos de seguridad para mitigar los riesgos sobre la información y ciberseguridad y las consecuencias a que estarían sujetos en caso de incumplirla.

5.1.4 GESTIÓN DE ACCESOS

Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de Central de Cobranzas S.A.S. ya sea local o en el ciberespacio. Por lo tanto, la identidad de cada usuario de los recursos informáticos deberá ser establecida y autenticada de una manera única y no podrá ser compartida.

Los usuarios de Central de Cobranzas S.A.S. una vez creados y asignadas sus autorizaciones en el Sistema de Información, podrán acceder a la información mediante su usuario y clave de autenticación.

Dependiendo del valor de la información y del nivel de riesgo, Central de Cobranzas S.A.S. definirá medios de autenticación apropiados, que no podrán ser compartidos (como la clave de acceso) y dichos medios de autenticación contienen información confidencial que no debe ser revelada o almacenada en lugares que puedan ser accedidos por personas no autorizadas.

Se deben establecer mecanismos de control de acceso físico y lógico para asegurar que los activos de información se mantengan protegidos localmente y en el ciberespacio de una manera consistente con su valor para el negocio y con los riesgos de pérdida de Confidencialidad, Integridad, Disponibilidad de la información.

Los derechos de acceso no deben comprometer la segregación de tareas y responsabilidades. El acceso realizado localmente y/o en el ciberespacio a la información de Central de Cobranzas S.A.S. deberá ser otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad. El acceso a los recursos de Central de Cobranzas S.A.S. debe ser restringido en todos los casos, y se debe dar específicamente bajo las premisas de necesidad de conocer y menor privilegio posible.

5.1.5 CLASIFICACIÓN DE LA INFORMACIÓN

Al igual que otros activos, no toda la información tiene el mismo uso o valor, y por consiguiente requiere diferentes niveles de protección. Toda la información de Central de Cobranzas S.A.S. será clasificada por el responsable de la Información con base en un análisis de alto nivel del impacto al negocio en Seguridad de la Información y Ciberseguridad, que determine su valor relativo y nivel de riesgo a que está expuesta.

Según los riesgos que se detecten, el responsable de la información y el Oficial de Seguridad de la Información, determinarán los controles que sean necesarios para proveer un nivel de protección de la información apropiado y consistente en Central de Cobranzas S.A.S., sin importar el medio, formato o lugar donde se encuentre. Estos controles deben ser aplicados y mantenidos durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

Por lo tanto, no se debe asumir que otros protegen la información, ya que es deber de los funcionarios de Central de Cobranzas S.A.S., tomar las medidas necesarias para proteger la información. De acuerdo con la clasificación de la información y a los riesgos a los que está expuesta, se deben implementar controles de cifrado durante los procesos de transmisión y almacenamiento de la misma.

5.1.6 CONTINUIDAD DE NEGOCIO

La información debe estar disponible para su uso autorizado cuando Central de Cobranzas S.A.S. la requiera en la ejecución de sus tareas regulares. Por lo que se deben desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de Central de Cobranzas S.A.S., tanto localmente como en el ciberespacio, sin disminuir los niveles de seguridad establecidos.

Esto debe ser independiente tanto del medio tecnológico que utilice Central de Cobranzas S.A.S. como de la posibilidad de que la información se dañe, se destruya o no esté disponible por un lapso de tiempo.

Central de Cobranzas S.A.S. establecerá medidas de reacción inmediata que permitan detectar y mitigar los efectos de ataques en seguridad de la información y ciberseguridad como son los de negación de servicios y el ingreso de código no autorizado. Estas medidas estarán fundamentadas en procedimientos y elementos que permitan mantener informada a Central de Cobranzas S.A.S. de la existencia de estas amenazas, detectar los ataques de manera inmediata y ejecutar las acciones consiguientes.

5.1.7 SEGURIDAD FÍSICA

Las áreas físicas construidas para soportar toda la operación de la Compañía deberán estar provistas de los controles adecuados (por ejemplo: puertas, cerraduras, lectores de tarjetas, biométricos, entre otros) según el valor de la información que contienen.

Los recursos informáticos de Central de Cobranzas S.A.S. deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades de

negocio. La información clasificada como confidencial o restringida no se dejará desatendida o sin control, por lo que Central de Cobranzas S.A.S. desarrollará un programa que permita prevenir que la información crítica de la Compañía sea accedida sin autorización, dentro de lo cual está comprendido la implantación y cumplimiento de las directrices de Escritorio Limpio y Pantalla Limpia.

5.1.8 ADMINISTRACIÓN DE ALERTAS – REGISTRO DE EVENTOS (TRAZABILIDAD)

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas e informadas al Oficial de Seguridad de la Información de manera inmediata.

Se debe desarrollar un programa de manejo de eventos e incidentes que dé prioridad a dichas alertas y las resuelva conforme a la criticidad de la información. Dicho programa debe incluir la definición de una organización de reacción inmediata, con el objetivo de atender éstas y otras situaciones que Central de Cobranzas S.A.S. considere como críticas.

Los responsables de la Información deben definir los eventos considerados como críticos (por ejemplo: intentos de acceso fallidos al sistema de información, borrado o alteración de información, entre otros) y los respectivos registros de Seguridad de la Información y Ciberseguridad que deben ser generados.

Los registros de Seguridad de la Información y Ciberseguridad deben ser activados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera oportuna a los responsables, así como a los niveles requeridos. Los registros y los medios que los generan y administran deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las pruebas.

5.1.9 SEGURIDAD EN LAS REDES

Las conexiones a la red privada de Central de Cobranzas S.A.S. deben realizarse de una manera segura para preservar la confidencialidad, integridad, disponibilidad de la información trasmitida sobre la red. Igualmente, todos los accesos de salida al ciberespacio y a otras empresas deben realizarse sobre redes aprobadas por Central de Cobranzas S.A.S.

Los Colaboradores que se conecten a la red privada, deben cumplir con la presente Política antes de que se realice la conexión. Esto aplica igualmente a cualquier conexión actual o futura en la red de Central de Cobranzas S.A.S., que utilice redes públicas.

Se requiere la aprobación del responsable de la Información para poder acceder remotamente a la información de Central de Cobranzas S.A.S., y dichos accesos deben cumplir con la Política de Identificación y Autenticación.

5.1.10 GESTION DE DISPOSITIVOS MOVILES

Los recursos informáticos de Central de Cobranzas S.A.S. tanto locales como en el ciberespacio, son exclusivamente para propósitos de la Compañía y deben ser tratados

como activos dedicados a proveer las herramientas para realizar el trabajo requerido. Los Colaboradores que intenten acceder a información para la que no tienen un requerimiento autorizado de negocio, están violando la presente Política.

En el uso de la información de Central de Cobranzas S.A.S. no se debe presumir privacidad, por lo que cuando ésta sea utilizada se podrán crear registros de la actividad realizada, que pueden ser revisados por Central de Cobranzas S.A.S. y deben ser conocidas y aceptadas por todos los funcionarios.

Central de Cobranzas S.A.S. se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente. Personal seleccionado por Central de Cobranzas S.A.S. podrá utilizar tecnología de uso restringido como la de monitoreo de red, datos operacionales y eventos en seguridad de la información. Ningún hardware o software no autorizados serán cargados, instalados o activados en los recursos informáticos, sin previa autorización formal del Líder de Seguridad de la Información o la Gerencia General.

Para acceder a la información de Central de Cobranzas S.A.S. tanto local como en el ciberespacio a través de medios tales como los dispositivos móviles o trabajo móvil, se deben implementar los controles necesarios para reducir los riesgos introducidos por estas prácticas.

5.1.11 SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD EN OPERACIONES DE SISTEMAS

La seguridad de las operaciones hace parte del Sistema de gestión de seguridad de la información y ciberseguridad (SGSI) que describe cómo gestionar y proteger las operaciones en los sistemas de información de Central de Cobranzas S.A.S. Dentro de los temas que debe considerar están los requisitos y buenas prácticas con respecto al respaldo o copias de seguridad; debe definir los requisitos para una administración segura de los recursos operativos; da las reglas para la administración adecuada de servidores y operaciones de soporte de software; describe el alcance, las funciones y los pasos principales del tratamiento de malware y los procesos de parcheo (procesos de reparación) de vulnerabilidades; garantizar que los cambios se realicen correctamente y que mantengan los niveles de seguridad; y finalmente dar las reglas sobre el seguimiento de las operaciones y el control de los sistemas de información.

5.1.12 POLITICA DESARROLLO Y MANTENIMIENTO DE APLICACIONES

Se debe contar con una política de Desarrollo y Mantenimiento de Aplicaciones en la que se describe cómo realizar desarrollos de aplicaciones de forma segura, debe definir los requisitos y dar precisiones sobre la seguridad de la información y Ciberseguridad con respecto al desarrollo y la puesta en marcha de aplicaciones; ya sea con desarrollo interno o externo.

Se debe aplicar en cada paso de un proyecto de desarrollo, desde el diseño hasta la puesta en marcha, y durante todo el ciclo de vida de la aplicación; adicionalmente debe considerar temas relacionados como, estructura de los proyectos ambientales y las reglas de

seguridad asociadas, reglas para el desarrollo subcontratado a un Proveedor, y definir el marco de la formación de los desarrolladores.

5.1.13 GESTIÓN DE PROVEEDORES

La política gestión de proveedores es un documento del Sistema de gestión de seguridad de la información (SGSI) que describe las mejores prácticas para abordar las interacciones con los proveedores de TI de Central de Cobranzas S.A.S.

La política tiene como objetivo definir los requisitos de seguridad de la información y ciberseguridad de Central de Cobranzas S.A.S. con respecto a las relaciones con sus proveedores; y define los requisitos desde la propuesta hasta la terminación del Contrato con el Proveedor, además expone las reglas específicas con respecto a los Servicios en el sitio y fuera del sitio aplicables al Personal de Proveedores.

5.1.14 GESTION DE ACTIVOS

Se debe establecer la política que entregue las directrices para identificar y clasificar los activos de información, con el propósito de controlar y mantener actualizado el inventario realizando una buena gestión, incluye realizar el levantamiento, actualización, clasificación y valoración de los activos de información, para controlar y gestionar los activos, de acuerdo con los criterios de confidencialidad, integridad, disponibilidad y privacidad de la información.

La Gestión de Activos de Información debe interactuar con la gestión de riesgos de Seguridad de la Información y Ciberseguridad, para la identificación de activos críticos, adicionalmente con la gestión de Continuidad del Negocio identificando los activos que soportan los servicios críticos de la compañía.

5.1.15 GESTION DE INCIDENTES DE SEGURIDAD

La Política de Gestión de Incidentes de Seguridad y ciberseguridad, describe cómo definir, manejar, compartir y cerrar los incidentes de seguridad.

Su objetivo es definir los requisitos de seguridad de la información y ciberseguridad para catalogar un incidente como incidente de seguridad; define la organización de la gestión de incidentes de seguridad y debe proporcionar las reglas para la descripción de los pasos en la gestión de incidentes de seguridad, desde la detección y reporte hasta la resolución y diagnóstico.

5.1.16 POLITICA DE ESCRITORIO LIMPIO

Las guías y los lineamientos internos que definen las buenas prácticas para el manejo, uso del escritorio y pantalla limpia que deberán seguir que es aplicable a todos los usuarios de Central de Cobranzas S.A.S. se encuentran establecidos en el Procedimiento de escritorio y Pantalla limpios (PRO-GTI-026).

5.1.17 POLÍTICA DE GESTIÓN DE MEDIOS REMOVIBLES

Se deben establecer los lineamientos para implementar los controles necesarios sobre el uso de medios removibles, para mitigar riesgos, como pérdida, daño, fuga o modificación de información.

La política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, interactúen o hagan uso de algún sistema de información, e incluye los siguientes lineamientos:

Gestión de Medios Removibles

El uso de medios removibles con información conlleva a riesgos, como pérdida, daño, fuga o modificación, que compromete no solamente la información sino también la infraestructura tecnológica, por lo tanto, el colaborador que los use será quien asuma la responsabilidad por la seguridad de la información.

Disposición de los Medios Removibles

Los medios que se regresen para asignarse a otro colaborador, se les deberá realizar un borrado de información. Es requisito realizar el respaldo o copia de la información contenida en el medio, previa ejecución del borrado de información.

En caso de que los medios sean donados, dados de baja o sean devueltos al proveedor, en la medida de lo posible se deberán emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes, con el fin de controlar que la información la compañía contenida en estos medios no se pueda recuperar.

Transferencia de Medios Físicos

Cuando se requiera transferir un medio físico que contenga información de Central de Cobranzas S.A.S., se deben usar transportes o servicios de mensajería confiables.

El dueño o propietario de la información a transferir debe autorizar dicho traslado.

Para la transferencia de medios de almacenamiento físicos, es necesario que este medio se proteja contra acceso no autorizado como claves y si es necesario el cifrado de la información.

5.1.18 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

Asegurar la implementación y el uso apropiado de controles para cifrado de la información en donde el nivel de criticidad de ésta lo requiera.

Esta política define los lineamientos de seguridad para el uso de controles de cifrado de información con el fin de proteger su confidencialidad, integridad, disponibilidad y privacidad.

La política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, hagan uso de controles criptográficos e incluye los siguientes lineamientos:

En Central de Cobranzas S.A.S. se utilizarán sistemas y técnicas criptográficas para la protección de la información y datos almacenados que así lo requieran (solicitudes del propietario de la información o solicitudes regulatorias).

Se deben identificar los sistemas y aplicaciones en los que se considere necesario hacer uso de controles criptográficos para proteger la información. El uso de controles criptográficos quedará determinado por el análisis de riesgos del sistema, así como el nivel o fortaleza de los mecanismos de cifrado a utilizar (algoritmos, longitudes de clave mínimas, etc.).

Gestión de Llaves

El área de TI debe realizar la gestión de llaves criptográficas durante todo su ciclo de vida, incluida la generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción de las llaves. Los algoritmos criptográficos, la longitud de las llaves y las prácticas de uso se deberán seleccionar de acuerdo con las mejores prácticas.

5.1.19 POLÍTICA INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

Establecer los lineamientos para implementar controles que protejan la Organización de la instalación de software, ilegal o no autorizado que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información.

La política aplica para todos los empleados, contratistas, proveedores, terceras partes o que, por su rol, tengan acceso a la información de la cooperativa, en medio digital o físico, y se debe considerar los siguientes lineamientos:

La actualización del software operacional, aplicaciones y librerías de programas solo la debe llevar a cabo el personal que designe el área de TI.

Las aplicaciones y el software del sistema operativo solo se deben implementar después de pruebas exitosas y siguiendo el procedimiento de control de cambios.

Se debe de conservar las versiones anteriores del software de aplicación como una medida de contingencia.

Restricciones Sobre la Instalación de Software

Sólo está permitido el uso de software licenciado por la Empresa y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado por el área de TI.

El área de TI es la única área autorizada para la administración del software, el cual no deberá ser copiado, suministrado a terceros o utilizado para fines personales por parte de los colaboradores.

El área de TI designará y autorizará al personal para instalar, configurar y dar soporte a los equipos de cómputo de la Organización

El área de TI podrá en cualquier momento realizar una inspección del software instalado en los equipos de cómputo de los colaboradores.

5.1.20 POLÍTICA DE GESTIÓN DE VULNERABILIDADES TÉCNICAS

El objetivo es establecer los lineamientos para la implementación de los controles que aseguren la ejecución de las pruebas de vulnerabilidad, tanto para las aplicaciones como

para la infraestructura de TI y se establezca el plan con las acciones de remediación requeridas.

Aplica para todos los administradores de los sistemas de información, servidores, bases de datos etc. Y considera los siguientes lineamientos:

El área de TI debe establecer un procedimiento para que periódicamente se realicen las pruebas de vulnerabilidad a los sistemas, con el fin de verificar y analizar los riesgos de seguridad, encontrando vulnerabilidades y realizando gestión sobre cada una para definir el plan de acción especifico necesario para la remediación.

Todo análisis de vulnerabilidad o prueba de penetración debe contar con la autorización del Coordinador GTI y estas deberán ser previamente informadas a las partes interesadas con el fin de evaluar el riesgo de la ejecución de ellas, su alcance y el cumplimiento de la normatividad vigente.

5.1.21 POLITICA GESTIÓN DE CAPACIDAD

El área de TI debe asegurar la implementación y el uso apropiado de controles que garanticen la aplicación de la gestión de capacidad sobre los elementos que componen los sistemas de información en Central de Cobranzas, para evitar la interrupción de los servicios y la afectación de la información respecto de la confidencialidad, integridad y disponibilidad.

El área de TI debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido de las soluciones tecnológicas.

Deben identificarse los requisitos de capacidad sobre los nuevos desarrollos y/o soluciones con el fin de evaluar y aplicar los ajustes necesarios en la plataforma tecnológica y garantizar la disponibilidad y eficiencia de los sistemas.

El área de TI debe hacer monitoreo que permita detectar problemas oportunamente frente a la capacidad de la plataforma tecnológica y tomar medidas necesarias para la continuidad de la prestación de los servicios.

5.1.22 POLITICA SEPARACIÓN DE AMBIENTES DE DESARROLLO

Se debe asegurar la implementación de los controles que garanticen la separación de los ambientes de desarrollo, pruebas y producción, para evitar la interrupción de los servicios y la afectación de la información respecto de la confidencialidad, integridad y disponibilidad.

La Coordinación GTI debe tener separados de manera física y lógica los ambientes de desarrollo, pruebas y producción.

Todo paso a producción debe de realizarse por medio del procedimiento de cambios.

Se deberá utilizar datos que no sean sensibles para la Empresa en los ambientes de prueba, exceptuando aquellos casos en los que el usuario funcional solicita la restauración de datos de producción para verificar la correcta funcionalidad.

Se deberá permitir que los ambientes de prueba, desarrollo y producción sean similares para prevenir situaciones en las cuales el software desarrollado o adquirido presente comportamientos distintos y errores.

Se deberá garantizar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y nunca en los ambientes de pruebas o producción.

5.1.23 POLITICA GESTIÓN DE CODIGO MALICIOSO

Establecer los lineamientos para implementar en todos los activos de información de la organización, controles para la detección y remediación de códigos maliciosos.

Verificar la presencia de códigos maliciosos en archivos de medios de almacenamiento masivo extraíbles o en archivos recibidos a través de la red.

Realizar tareas de escaneo en busca de códigos maliciosos en todas las unidades de almacenamiento de la estación de trabajo.

Ningún colaborador podrá ejercer actividades de administración sobre su equipo.

Los únicos autorizados para desarrollar esta función son los colaboradores autorizados por la Coordinación GTI.

Se prohíbe estrictamente el uso de software no autorizado, todo software instalado debe contar con licencia.

La Coordinación GTI realizará sensibilización a los colaboradores sobre la protección contra software malicioso y buenas prácticas de seguridad informática, está prohibido la descarga de software no licenciado en cualquier dispositivo de la Empresa, adicionalmente se prohíbe la instalación de software propiedad de la Empresa en equipos que no pertenezcan a la organización.

Los colaboradores que sospechen o detecten alguna infección por software malicioso debe notificar al área de TI, para que, a través de ella, se tome las medidas de control correspondientes.

La Coordinación GTI debe incluir en la infraestructura tecnológica que permita identificar y proteger a la organización de ataques externos y que afecten las plataformas tecnológicas de Central de Cobranzas.

La Coordinación GTI debe monitorear los intentos de ataque tanto internos como externos para tomar acciones que mitiguen este riesgo.

La Coordinación GTI debe asegurar la instalación y configuración de un antivirus que identifique y proteja los equipos tecnológicos. Así mismo, debe actualizar periódicamente sus firmas para garantizar que la protección sea dinámica y encaminada a los nuevos vectores de ataque.

Cuando se identifique un programa maligno en los equipos de la Empresa, se debe seguir conducto regular y reportar y tratar como un incidente de seguridad de la información.

La Coordinación GTI debe ejecutar, al menos una vez al año, una prueba que identifique vulnerabilidades en las plataformas tecnológicas (Análisis de Vulnerabilidades, Ethical Hacking, entre otros), con el fin de mejorar los niveles de seguridad y proteger los activos de ataques externos e internos, con la interventoría de un proveedor externo.

Se prohíbe la descarga de cualquier archivo que provenga de correos sospechosos o de destinatarios desconocidos, su descarga sólo podrá ejecutarse con la validación y autorización del oficial de seguridad de la información.

Cualquier equipo que se conecte a la red y que no sea propiedad de la Empresa debe contar con los requisitos mínimos de seguridad establecidos en la Política de uso de dispositivos móviles previamente expuesta.

5.1.24 POLITICA COPIAS DE SEGURIDAD

Se deben establecer los lineamientos para generar las copias de respaldo de los activos de información con el fin de preservar su disponibilidad.

El área de TI debe asegurar que se realicen las copias de respaldo de la información de la organización almacenada en los sistemas de Información, servidores y bases de datos.

Es responsabilidad del coordinador GTI o a quien el jefe asigne realizar las copias de seguridad de información, realizando seguimientos regulares a su ejecución. El coordinador GTI o a quien el jefe asigne debe validar el resultado de la ejecución de las copias de seguridad y registrar las novedades en la bitácora establecida para ello.

Cuando se requiera un soporte o mantenimiento correctivo por parte del fabricante, que pueda afectar los procesos o los sistemas de procesamiento de la información, quien ejecute el rol de Administrador de backups debe solicitar la aprobación del jefe de área.

Es responsabilidad del Coordinador GTI o a quien el jefe asigne realizar por lo menos pruebas de restauración una vez al año.

El área de TI debe asegurar la custodia de las copias de seguridad en un sitio externo a las instalaciones de la Empresa e incluir el detalle de las actividades en el procedimiento especifico desarrollado para este fin.

5.1.25 POLITICA DE SINCRONIZACIÓN DE RELOJES

Establecer los lineamientos para contar con controles que protejan la interceptación, copiado, modificación de la información a través de la manipulación de los relojes de los dispositivos tecnológicos

La Coordinación GTI deberá definir un único procedimiento técnico que permita la sincronización de relojes de los servidores con una única fuente de referencia de tiempo, por ejemplo (http://horalegal.inm.gov.co/), con el fin de garantizar la exactitud de los registros de auditoría y evitar posibles fraudes relacionados con la manipulación de los relojes.

5.1.26 POLITICA TRANSFERENCIA DE INFORMACIÓN

Se deben establecer los lineamientos para contar con controles que protejan la información transferida con respecto a la interceptación, copiado, modificación, y enrutado, así como mantener la seguridad de la información transferida al interior de la Empresa y/o con cualquier organización externa.

Acuerdos de confidencialidad o de no divulgación

Confidencialidad: Todos los empleados y terceras partes con quienes se firme un acuerdo de confidencialidad están obligados a dar cumplimiento a la Política de Confidencialidad establecida por la Empresa.

El intercambio de información al interior de la Empresa debe hacerse por medio de los canales de comunicación formalmente establecidos para ello. Está prohibido el envío de información Empresa a canales personales como correo electrónico, drive, WhatsApp web, entre otros.

Acuerdos sobre transferencia de información

Cuando se trate de un intercambio o transferencia de información confidencial con un tercero, el propietario del activo de información debe realizar acuerdos para el intercambio seguro de la información mediante acuerdos y/o actas en donde ambas partes deben estipular los medios por los cuales se realizará la transferencia de la información.

El propietario del activo de información debe establecer un acuerdo de confidencialidad con la parte externa solicitante o interesada, esto con el fin de, prevenir que se vulnere la confidencialidad de la información y que pueda ser usada para fines fuera del acuerdo con las partes firmantes. Los acuerdos de confidencialidad sólo aplican cuando la información a intercambiar sea clasificada como Confidencial.

5.1.27 POLITICA DE ENMASCARAMIENTO DE DATOS

Se debe asegurar la implementación de los controles que permitan proteger la información sensible gestionada en los sistemas internos, implementando el enmascaramiento de datos como una medida de seguridad clave. Este proceso se aplicará según las necesidades específicas de cada sistema, garantizando el cumplimiento de los requisitos legales y contractuales aplicables.

5.1.28 POLITICA DE GESTIÓN DE BASE DE DATOS

Con el propósito de garantizar la protección de la información almacenada en las bases de datos, el acceso a estas debe estar restringido únicamente a personal autorizado según sus funciones y responsabilidades, se asignarán permisos de acceso basados en el principio de mínimo privilegio, otorgando solo los privilegios necesarios para realizar las tareas asignadas.

La información almacenada en las bases de datos será considerada confidencial y solo se divulgará a personas autorizadas y con un propósito legítimo.

Se deben implementar medidas para garantizar la disponibilidad de las bases de datos.

6. DOCUMENTOS ASOCIADOS

Norma Técnica Colombiana NTC ISO/IEC 27001:2013", la Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales.", Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" y demás normativas vigentes aplicables a los activos de información.

7. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN	AUTOR	REVISIÓN	APROBACIÓN
04/04/2022	01	Versión Inicial	BCM Consultores	Oficial de Seguridad de la Información	Gerente General
25/07/2022	02	Corrección / adición depolíticas	BCM Consultores	Oficial de Seguridad de la Información	Gerente General
30/11/2022	03	Se actualiza tipo de sociedad de la organización, cambia de Central de Cobranzas Ltda. a Central de Cobranzas SAS.	BCM Consultores	Oficial de Seguridad de laInformación	Gerente General
24/04/2023	04	Corrección / adición de políticas	Oficial de Seguridad de la Información	Coordinador GTI	GerenteGeneral
12/09/2023	05	Se realiza etiquetado del documento de acuerdo con la política de clasificación de la información	Oficial de Seguridad de la Información	Coordinador GTI	GerenteGeneral

12/11/2024	06	Actualización del etiquetado del documento, adición de Políticas.	Oficial de Seguridad de la Información y Datos Personales	Coordinador GTI	GerenteGeneral

REVISADO POR
PABLO EMILIO NARVAEZ
Coordinador de GTI
12/11/2024

APROBADO POR
MONICA PATRICIA VELEZ ANGULO
Gerente General
12/11/2024