Concesionaria Nueva Vía al Mar

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA TERCEROS
CVM-DT-TEC-006
VERSIÓN: 04
FECHA: 12/02/2024

TABLA DE CONTENIDO

1. OBJETIVO

Establecer las directrices y los lineamientos relacionados con el manejo adecuado de la información por terceros, para garantizar su seguridad a través de los principios de confidencialidad, integridad y disponibilidad, enmarcado en estándares internacionales de seguridad, en normas de entes reguladores y en aspectos de calidad en lo que se refiere a eficacia, eficiencia y confiabilidad.

2. ALCANCE

El presente documento aplica para todos los terceros contratados por la compañía que acceden de manera interna o externa a cualquier activo de información. Adicionalmente, aplica a toda la información creada, procesada o utilizada por terceros en el soporte al negocio, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

3. DEFINICIONES

- **Activo de Información:** Es toda aquella información que, sin importar su presentación, medio o formato, en el que sea creada, utilizada o almacenada, tiene valor e importancia dentro de la organización y sirve de fuente y/o soporte a las actividades de negocio y la toma de decisiones.

- **Clasificación de la Información:**

  - **Confidencial**: Información de uso exclusivo de un grupo de colaboradores y que no puede ser conocida por otros funcionarios o terceros sin autorización del propietario de la información.
  - **Privada**: Información propia de la Compañía disponible solamente para los colaboradores.
  - **Publica**: Información que puede ser conocida por el público en general.
  - **Sensible**: Aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

- Circular 038/2009: **(Superintendencia financiera) Instrucciones relativas a la revisión y adecuación del Sistema de Control Interno (SCI).**
- **Comunidad:** Son los usuarios que utilizan la información del negocio.

- **Controles:** Salvaguardas basadas en dispositivos o mecanismos que se requieren para cumplir con los requisitos de una política.

- **Criterios de Calidad de la Información:**

  - **Confiabilidad**: La información debe ser la apropiada para la administración de la compañía y el cumplimiento de sus obligaciones.
  - **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.

- **Incidente de seguridad de la información**: Es la materialización de un evento que compromete las operaciones de la compañía y amenaza la seguridad de la información.

- **Información del Negocio:** Es toda aquella que, sin importar su presentación, medio o formato, en el que sea creada o utilizada, sirve de fuente y/o soporte a las actividades de negocio 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.

- **Intranet:** Es una red informática que utiliza la tecnología del protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. Suele ser interna, en vez de pública como internet, por lo que solo los miembros de la organización tienen acceso a ella.

- **Ley 1581 de 2012:** (protección de datos personales – Superintendencia de industria y comercio) Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas.

- 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:** Se refiere al conjunto de políticas, procedimientos, estándares, normas de seguridad, elementos de seguridad y topologías que garantizan la protección de la información del negocio.

- **Medio Informático:** Son un conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión digitalizados de la información.

- **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.

- **NTC-ISO/IEC 27001:** Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI).

- **Nube**: La computación en la nube (cloud computing), conocida también como servicios en la nube, informática en la nube, nube de cómputo, nube de conceptos o simplemente "la nube", es un modelo que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

- **Organización de Seguridad de la Información**: Estructura organizacional que soporta la Seguridad de la Información, donde se definen roles y responsabilidades de cada uno de sus integrantes en la compañía. Lo compone el comité de gobierno, riesgos y cumplimiento.

- **Perímetros o áreas seguras:** Un área o agrupación (física o virtual) 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.

- **Política de Seguridad de la Información:** Documento donde se establecen las directrices y los lineamientos relacionados con el manejo seguro de la información.

- Principios de Seguridad de la Información:

  - **Confidencialidad**: Hace referencia a la protección de información cuya divulgación no está autorizada.
  - **Integridad**: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.
  - **Disponibilidad**: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

- **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.

- **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 la organización.

- **Seguridad de la información**: Protección de la información contra el acceso no autorizado accidental o intencional, su modificación, destrucción o publicación, con el fin de asegurar la continuidad, minimizar el riesgo y maximizar el retorno de inversiones y oportunidad de negocio.

- **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.

- **Tercero**: son personas o empresas contratadas por la organización, para realizar funciones, procesos, actividades, tareas, entre otros, en los activos de información de propiedad de la compañía.

- **Titular de la Información:** Persona natural cuyos datos personales sean objeto de Tratamiento.

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

- **Usuarios**: son las personas que utilizan los recursos tecnológicos, pueden ser usuarios internos como los empleados de la compañía o usuarios externos como proveedor o terceros.

4. DESCRIPCIÓN DE LA POLÍTICA

4.1 Seguridad de la información en las relaciones con los terceros.

- El área de tecnología en conjunto con el responsable del tercero que: acceda, procese, almacene, comunique o suministre información propia de la entidad, deberá establecer los requisitos de seguridad de la información para mitigar los riesgos asociados con los activos de la entidad y estos deben ser acordados y documentados. Entre los requisitos se encuentra el establecimiento de cláusulas de seguridad de la información y ciberseguridad en caso de que la relación con el tercero amerite la aplicación de dichas cláusulas.

- Las responsabilidades y deberes de seguridad de la información que permanecen después de finalizada la relación con el tercero se dejará establecido dentro de las cláusulas de seguridad de la información y ciberseguridad en caso de ser aplicables. Anualmente la coordinación de gobierno, riesgo y cumplimiento validará que se estén incluyendo las cláusulas de seguridad de la información y ciberseguridad en los documentos que formalicen la relación con los terceros, en los casos en que éstas sean aplicables.

- En los casos que se requiera y a criterio del área de tecnología y el área de GRC, se solicitará a los proveedores de servicios tecnológicos críticos, que puedan afectar la confidencialidad, integridad o disponibilidad de la información, diligenciar el formato CVM-RE-TEC-008 ANEXO SEGURIDAD DE LA INFORMACION TERCEROS, con el propósito de evaluar aspectos de seguridad de la información.

- Los acuerdos con terceros deben incluir requisitos para tratar los riesgos de

seguridad de la información, asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación. Estos acuerdos deberán ser revisados por el área de tecnología y el área de GRC, en los casos en que se presenten requerimientos de seguridad con los proveedores, para tomar los correctivos a los que haya lugar.

- Los diferentes aspectos contemplados en esta Política son de obligatorio cumplimiento por parte del tercero. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la compañía tomará las acciones disciplinarias y legales correspondientes.

- Las excepciones deben ser aprobadas por el comité de gobierno, riesgos y cumplimiento o en su defecto por el área de Tecnología.

4.1.1. Gestión de la prestación de servicios de terceros.

- La compañía, a través del área de compras, enviará las evaluaciones periódicas al área de tecnología, con el fin de auditar la prestación de los servicios tecnológicos por parte de los terceros, conforme a la política de compras (CVM-DT-REC-001).

- La compañía, a través del área encargada del tercero, deberá gestionar los cambios en el suministro de servicios prestados por este, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la reevaluación de los riesgos.

- Ningún tercero deberá poseer para usos distintos a sus responsabilidades, material o información propia de la compañía.

- En caso de que, por motivos directamente relacionados con las funciones del trabajo a realizar, para lo cual fue contratado el tercero o proveedor, entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.

- En los casos que aplique, la compañía deberá ejecutar procedimientos de borrado seguro de información en sus propios equipos o en equipos de terceros que sean utilizados para procesar información de la compañía.

- Todos los terceros o proveedores que presten servicios en sitio, es decir en las oficinas de la compañía, deberán acogerse a las políticas de seguridad de la información establecidas al interior de la organización, y que se encuentran en este documento.

- Cuando exista la necesidad de otorgar acceso a la información de la compañía a terceras partes, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

- En ningún caso se otorgará acceso de terceros a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto no se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso. Sera responsabilidad del propietario de la información asegurarse que los controles hayan sido establecidos.

- Se debe preparar y legalizar un acuerdo de confidencialidad entre la entidad y el tercero de acuerdo con el objeto y alcance del contrato, el cual debe quedar firmado por ambas partes. En todos los casos deben firmarse acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad de la información.

- Será responsabilidad del tercero asegurarse que los funcionarios que vayan a prestar servicios en las instalaciones de la compañía conocen y entienden sus responsabilidades con respecto a esta política. La compañía podrá realizar auditoria sobre los equipos de cómputo de los terceros que se encuentren en las instalaciones y sobre las cuales se realice tratamiento de información propia de la compañía.

- En el caso de que un tercero requiera realizar tratamiento de información al interior de la compañía a través de su propia máquina, el tercero deberá certificar por escrito que todo el software utilizado para sus actividades es licenciado.

- Los proveedores de tecnología clasificados como críticos deberán, en su vinculación, hacer entrega del listado de personal titular y los reemplazos autorizados para la prestación de servicios de soporte ante la organización, incluyendo los perfiles de los cargos, en el cual se evidencien las competencias del personal junto con sus certificaciones académicas y de experiencia.

- La organización, a través del área encargada del tercero, y con el apoyo del área de GRC, deberá realizar el análisis de la documentación de los perfiles de los cargos

y sus certificaciones, así como la correspondiente verificación en las listas restrictivas definidas por la organización, del personal autorizado por el proveedor de tecnología para la prestación de servicios de soporte. Conforme al análisis anterior quedará a discreción de la organización la aceptación del personal asignado por el proveedor.

- En caso de presentar cambios en el listado del personal titular y el reemplazo asignado para la prestación de servicios de soporte ante la organización, el proveedor crítico de tecnología deberá informar previamente dicho cambio y adjuntar los soportes descritos anteriormente, con el propósito de realizar análisis a las competencias del personal asignado y emitir su correspondiente autorización, de lo contrario la organización no autorizará la prestación del servicio de soporte.

4.1.2. Control de acceso físico y lógico a las instalaciones por parte de los terceros.

- Los accesos a la oficina de la compañía por parte de visitantes temporales deberán ser registrados en la recepción del edificio y de la Concesionaria. Cuando se requiera el ingreso para un tercero permanente, es decir que necesite ingresar a las instalaciones de la compañía diariamente por más de 1 mes, este deberá ser registrado en el sistema de acceso digital.

- Los terceros que requieran recolectar datos de los colaboradores de la compañía por alguna actividad realizada en las instalaciones de Covimar deberán remitir dicha solicitud al área de gestión humana y contar con la aprobación del responsable del tercero. Los terceros que accedan por VPN “cliente – usuario” a la infraestructura tecnológica de la compañía, deberán solicitar autorización al área de tecnología para realizar esta conexión.

- El Centro de Cableado y los Racks de Comunicaciones tienen acceso restringido. El acceso al Centro de Cableado se controla a través de tarjeta de proximidad, los racks de comunicaciones permanecen bajo llave y están dentro de ubicaciones cerradas y alejados del acceso al personal externo. El líder del proceso es el responsable de coordinar con el Área de Tecnología las autorizaciones y condiciones de ingreso de terceros o proveedores al Centro de Cableado o a los Racks de Comunicaciones.

- La comunicación de las autorizaciones de ingreso al Centro de Cableado o a los Racks de Comunicaciones, se informará vía correo electrónico al área de Sistemas y a la dirección administrativa y financiera de la Concesionaria. Durante la visita al Centro de Cableado los empleados internos y proveedores en general que

requieran realizar alguna actividad, deberán permanecer acompañados por personal autorizado del área de sistemas de la Concesionaria y deben portar el carné institucional o de visitante en un lugar visible

- Es responsabilidad del empleado del área de sistemas que acompaña la visita de un tercero al Centro de Cableado y/o Racks de Comunicaciones, controlar que éste no realice actividades diferentes a las autorizadas, como, por ejemplo, la instalación de recursos informáticos a red de la Concesionaria, toma de fotografías, toma de videos, etc. Es responsabilidad del personal de tecnología realizar acompañamiento y control durante las actividades de aseo al interior del Centro de Cableado. El personal con autorización de ingreso permanente al Centro de Cableado es:

  - ✓ Coordinador de Sistemas, Tecnología e Infraestructura
  - ✓ Técnico de Sistemas
  - ✓ Coordinador Administrativo

- El motivo que origina la solicitud de ingreso al Centro de Cableado y a los Racks de Comunicaciones debe ser consecuente con las actividades de soporte, mantenimientos y gestión de los recursos que se encuentren en dicho lugar.

- Se recomienda no permitir la visita de varios empleados o proveedores de empresas en forma simultánea al Centro de Cableado o a los Racks de Comunicaciones, salvo aquellos casos especiales en los cuales se programan mantenimientos en horarios no hábiles, siempre y cuando se tenga la autorización del Área de Tecnología.

- En los casos de contingencia en los que se requiera manipulación de los Racks de Comunicaciones y el área de Tecnológica no pueda enviar personal calificado, los Racks de Comunicaciones podrán ser manipulados por personal externo, siempre y cuando se tenga autorización y direccionamiento de la Coordinación de Tecnología.

- En ausencia de todos los empleados del área de Tecnología titulados para autorizar ingreso al Centro de Cableado, el Director Administrativo y Financiero podrá dar la autorización con posterior ratificación del personal titulado.

- Anualmente el área de GRC revisará el formato de registro de acceso de proveedor o empleado de la compañía (CVM-RE-TEC-011 Control De Acceso al Centro de Cableado / Rack de Comunicaciones), que está ubicado en el centro de cableado, para verificar que se realice el diligenciamiento correspondiente, y quede como evidencia de las actividades realizadas por el tercero o empleado de la compañía, en el centro de datos. Los lineamientos establecidos en el presente documento son

de obligatorio cumplimiento y cualquier omisión o alteración es considerada práctica indebida, lo que acarreará sanciones de tipo disciplinario, de acuerdo con lo consagrado en el Reglamento interno de trabajo, el contrato de trabajo y las políticas corporativas de la Concesionaria.

4.1.3. Uso apropiado de los recursos por parte de los terceros.

Los recursos tecnológicos que la compañía pone a disposición del tercero, independientemente del tipo de recurso (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplir las obligaciones y propósito de la operación para la que fueron diseñados e implantados. Los terceros que usen dichos recursos deben tener la obligación de confidencialidad de la información que se maneje, por lo que queda terminantemente prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del servicio, o bien la extralimitación en su uso.
- El uso de los equipos y/o aplicaciones que no estén especificados como parte del software o de los estándares de los recursos informáticos propios de la compañía o bajo supervisión. Introducir en los sistemas de información o la red corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.

- Introducir cualquier tipo de malware como programas, macros, código, dispositivos lógicos, dispositivos físicos o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos de la compañía. Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.

- Intentar acceder a áreas u ambientes restringidos de los sistemas de información sin la debida autorización. Intentar distorsionar o modificar los registros “log” de los sistemas de información. Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, o dañar o alterar los recursos informáticos.

- Conectar medios extraíbles y/o habilitar conexiones inalámbricas no autorizadas en los equipos de la compañía.

- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.

4.1.4. Protección frente a software malicioso por parte de los terceros.

En los casos en los que el tercero disponga de su propio equipo de cómputo para la prestación de sus servicios en la compañía, deberá seguir las siguientes indicaciones:

- Mantener los sistemas al día, con las últimas actualizaciones de seguridad disponibles.

- El software antivirus deberá estar siempre habilitado y debe contar con actualización automática de los archivos de definición de virus.

4.1.5. Intercambio de información por parte de los terceros.

- En los casos que aplique, se deberá establecer un contrato de trasferencia y/o trasmisión de datos personales entre el tercero y la compañía.

- Cuando se requiera el intercambio de información confidencial, clientes, proveedores y/o colaboradores con terceros, dicha información deberá enviarse de manera segura a través de los mecanismos que la compañía dispone para tal fin. En relación con el intercambio de información, se considerarán no autorizadas las siguientes actividades:

    - Transmisión o recepción de material protegido por derechos de autor infringiendo la ley de propiedad intelectual.

    - Transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.

    - Transferencia de archivos a terceras partes no autorizadas de información de la compañía.

    - Transmisión o recepción de archivos que infrinjan la Ley de Protección de Datos Personales Ley 1581 de 2012.

- Transmisión o recepción de juegos y/o aplicaciones no relacionadas con el negocio.
- Todas las actividades que puedan dañar la buena reputación de la compañía están prohibidas en Internet y en cualquier otro lugar. Esto se refiere también a actividades realizadas para el propio beneficio económico del tercero o de terceras partes.

4.1.6. Uso del correo electrónico por parte de los terceros.

- Si un tercero requiere que se le asigne una cuenta de correo electrónico de la compañía, para prestar sus servicios, esta cuenta estará sujeta a las siguientes normas: Se considera el correo electrónico como una herramienta más de trabajo provista al usuario con el fin de ser utilizada conforme al uso para el cual está destinada. Esta consideración facultará a la compañía a implementar sistemas de control destinados a velar por la protección y el buen uso de este recurso.

- El sistema de correo electrónico de la compañía no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares que pongan en riesgo el buen nombre de la entidad. Los terceros no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples usuarios).

- No está permitido configurar el correo electrónico de la compañía en dispositivos personales del tercero.

- No está permitido el envío de información propia o confidencial de la compañía y que corresponda a clientes, terceros, y/o colaboradores a cuentas de correo electrónico personales o sitios de almacenamiento masivo en internet. Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información.

- Las cuentas de correo electrónico son propiedad de la compañía, las cuales se deben utilizar única y exclusivamente para las tareas propias de la función desarrollada y no debe utilizarse para ningún otro fin. No está autorizado el envío de cadenas de correo, correos masivos con archivos adjuntos de gran tamaño que puedan afectar y/o congestionar la red. Si se requiere alguna de

estas tareas se debe gestionar y revisar con el área de tecnología.

- Cuando un funcionario o tercero se retire de la compañía, y tengan una cuenta de correo electrónico a su nombre, se deberá realizar copia de seguridad a dicha cuenta y posteriormente desactivarla.

- El tamaño del buzón de correo electrónico estará determinado por el rol que desempeñe el usuario.

- El tercero es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo.
- Todos los mensajes enviados y/o recibidos pueden ser sujetos a análisis y conservación permanente por parte de la compañía.

- El usuario deberá abstenerse de abrir mensajes cuyo origen sea desconocido o sospechoso. No está permitido crear cuentas de correo electrónico a nombre de la compañía con un dominio distinto a los autorizados (@covimar.com.co.)

Todo proveedor que tenga una cuenta de correo electrónico proporcionada por la compañía debe identificar en la firma, la empresa a la cual pertenece el funcionario, o en caso de ser una persona natural, deberá informar su cargo o función general, con el cual se pueda identificar.

4.1.7. Conexión a la red por parte de los terceros.

- La compañía se reserva el derecho, sin aviso previo, de bloquear, suspender, alterar o monitorear los servicios soportados en su red informática y puestos a disposición de las entidades externas.

- No se deberá conectar a los recursos de la compañía ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas a la red corporativa. Nadie deberá conectarse a la red corporativa a través de otros medios que no sean los definidos.

- La navegación en Internet debe realizarse de forma razonable y con propósitos laborales. No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de la compañía o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la compañía.

- Cuando se requiera acceder a una página con fines laborales y se encuentre bloqueada por los mecanismos de seguridad, deberá solicitar la autorización al área de tecnología, quienes otorgaran autorización de acceso, una vez realizado un análisis de riesgos. La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet de la compañía.

4.1.8. Control de accesos por parte de los terceros.

Requisitos de negocio para el control de accesos

a. El área de tecnología deberá definir y mantener actualizada la matriz de perfiles de acceso de cada uno de los aplicativos internos, portales financieros y perfiles de navegación.

b. Se deberá establecer un proceso formal para la gestión de los accesos de los usuarios a los sistemas de información de producción.

c. Los proveedores de tecnología no deberán acceder a los ambientes de producción y contingencia para realizar actividades mantenimiento, pruebas y soporte, a no ser que esta actividad sea coordinada y autorizada por el área de tecnología de la compañía.

d. El área de tecnología deberá mantener un registro formal de todos los usuarios autorizados y respectivos roles de acceso a los sistemas de información.

e. Se deberá evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de la compañía deberá ser única y personalizada.

- Control de acceso a sistemas y aplicaciones

a. Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas y cumplir las directivas que la compañía imparta para tal efecto.

b. Las estaciones de trabajo deben ser bloqueadas mediante la facilidad del sistema operativo, mientras se encuentran desatendidas.

c. Toda solicitud de acceso u obtención de copias totales o parciales de bases de datos de los sistemas de información de la organización, por parte de cualquier área o ente externo y en cualquier medio, debe acogerse a los procedimientos

definidos para tal fin en la compañía.

d. Todo acceso a los sistemas operativos debe estar controlado por registros de inicio seguro. Se debe definir un procedimiento para la conexión de los usuarios al sistema informático el cual minimice la posibilidad de acceso no autorizado.

e. El área de tecnología deberá establecer las medidas necesarias para el acceso controlado a las fuentes de las aplicaciones de software.

f. El área de tecnología deberá realizar una revisión trimestral con el fin de eliminar o bloquear usuarios que ya no laboran con la entidad, y la eliminación o bloqueo de cuentas redundantes o innecesarias. Esto quedará registrado en los formatos de SAP (EPI-ANX-GSI-02 – Matriz de Acceso), en el formato de directorio activo (CVM-RE-TEC-020_Matriz_Perfiles_DA_V1), y en formato de WorkManager (CVM-RE-TEC-021_Matriz_Perfiles_WorkManager_V1).

g. Las modificaciones en las necesidades de acceso a los sistemas deben estar alineados con las matrices de derechos de acceso.

- Gestión de acceso de usuarios

a. Cada usuario debe ser identificado de manera única, y su actividad en los sistemas de procesamiento de información debe ser controlado, monitoreado y revisado, en ese orden de ideas, se debe entregar a los usuarios autorizados un acceso único a la información mínima necesaria para la realización de sus labores.

b. No está permitido el uso de un mismo código de acceso por varios usuarios, los usuarios son responsables de todas las actividades realizadas con su código de acceso. Los usuarios no deben divulgar ni permitir que otros utilicen sus credenciales de usuario, al igual que tiene prohibido utilizar las credenciales de acceso de otros usuarios.

c. La compañía deberá definir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

d. La asignación y uso de derechos de acceso con privilegios especiales deberá ser restringido y controlado.

e. Al finalizar la contratación de un colaborador y/o un tercero, todas las credenciales de acceso a los sistemas de información de la organización

deberán ser retiradas y/o deshabilitadas. Sera responsabilidad del área de talento humano informar al área de tecnología la novedad.

f. Los accesos y respectivos privilegios solo se implementan en los sistemas después de obtener todas las aprobaciones necesarias.

4.1.9. Incidentes de seguridad de la información relacionados con los terceros.

En el caso de detectarse alguna incidencia o vulnerabilidad relacionada con los sistemas de información se seguirán las siguientes pautas:

- El tercero podrá trasladar al área de tecnología sugerencias y/o debilidades, que pueda tener relación con la seguridad de los datos y las directrices contempladas en la presente Política.

- El tercero deberá notificar, al responsable del área de tecnología, la incidencia que se detecte y que afecte o pueda llegar a afectar la seguridad de la información de la compañía.

- En caso de que el área de tecnología detecte incidentes o vulnerabilidades relacionadas con los sistemas de información de los terceros contratados, deberá informar al tercero esta situación, con el fin de este tome las acciones correctivas pertinentes a las que haya lugar.

5. DOCUMENTOS, REGISTROS Y ANEXOS RELACIONADOS.

Código	Descripción
CVM-RE-TEC-008	ANEXO SEGURIDAD INFORMACION TERCEROS
EPI-ANX-GSI-02	-Matriz de Acceso de SAP
CVM-RE-TEC-020	_Matriz_Perfiles_DA_V1- Directorio Activo
CVM-RE-TEC-021	_Matriz_Perfiles_WorkManager_V1

6. CAMBIOS O MODIFICACIONES EN ESTA VERSIÓN

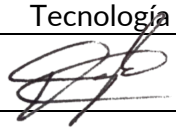
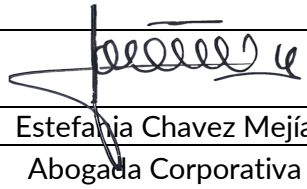
Capítulo	Fecha	Página	Lista de Cambios o Modificaciones Resumidas
NA	19-04-2018	NA	Versión inicial.

Capítulo	Fecha	Página	Lista de Cambios o Modificaciones Resumidas
4.1.1.	19-08-2020		Se incluyeron disposiciones para el ingreso de personal de soporte de los terceros contratados a nuestra plataforma tecnológica.
NA	28-10-2022		Se incluyen disposiciones de la ISO 27001: 2013, en los puntos 4.1, 4.1.2 y 4.1.9
Todo	12/02/2024	Todo	Modificación en el logo por cambio de imagen corporativa

7. CONTROL DE CAMBIOS.

No.	Fecha
1	19/04/2018
2	19/08/2020
3	28/10/2022
4	12/02/2024

8. REVISIÓN Y APROBACIÓN

	Elaboró	Revisó	Aprobó
Nombre:	Daniel Martinez Arcos	Jose Ignacio Clavijo	Adriana Fawcett Vargas
Cargo:	Coordinador de Sistemas, Infraestructura y Tecnología	Director Administrativo y Financiero	Gerente General
Firma:			
Nombre:		Estefanía Chavez Mejía	
Cargo:		Abogada Corporativa	
Firma:		ESTEFANÍA CHÁVEZ MEJÍA	
Nombre:		Paola Andrea Blanco	
Cargo:		Coordinador de Gobierno, riesgo y cumplimiento	
Firma:			

Documento aprobado en la sesión de Junta Directiva No. 103 del 11/10/2022