POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Cód.: PO-SEIN-014

Versión 008

ELABORADO	REVISADO	REVISADO	APROBADO	APROBADO	APROBADO
Felipe Miranda Subgerente de Ciberseguridad y Ciberseguridad	Lorena Ramirez Jefa de Cumplimiento y Normativa Julio Villalobos Abogado Soledad Diaz Subgerente de Cumplimiento y Normativa Gabriela Covarrubias Fiscal	Cristian Ibaceta Contralor	Francisco Sepúlveda Gerente General	Cristian Abbott Presidente del Comité de Riesgo del Directorio	Marco Antonio Álvarez Presidente de Directorio
Fecha: 14-06-2024	**Fecha: 17-06-2024**	**Fecha: 14-06-2024**	**Fecha: 25-06-2024**	**Fecha: 25-06-2024**	**Fecha: 25-06-2024**

Contenido

I. Introducción

La Araucana C.C.A.F. reconoce la importancia, así como el valor de sus activos de información y como estos pueden verse expuestos a múltiples amenazas, razón por lo cual son considerados un elemento crítico para el correcto cumplimiento de los objetivos de la compañía, tanto en la continuidad de las operaciones como en los procesos de negocio.

Complementariamente, la Superintendencia de Seguridad Social instruyó por medio de la circular N°2821 y N°3594, contenidas actualmente en el Compendio de Normas que regulan a las C.C.A.F, numeral 6.1.12 y siguientes, que toda C.C.A.F. debe contar con un sistema de gestión de seguridad de la información.

Por estas razones, se establece la siguiente Política General de Seguridad de la Información (PGSI), enfocada principalmente en la protección de los activos de información derivados de las unidades de negocio de La Araucana C.C.A.F.

II. Objetivo

Establecer lineamientos precisos sobre la implementación del Sistema de Gestión de Seguridad de la Información, en adelante “SGSI” (ver definición en anexo IX SGSI – Dominios de Control) así como determinar el conjunto de medidas preventivas que permitan asegurar niveles razonables de: Confidencialidad, Integridad y Disponibilidad de la Información de La Araucana C.C.A..F., mitigar los riesgos sobre los activos de valor, mantener la continuidad operacional y fomentar el desarrollo de una cultura de seguridad de la información, determinando las respectivas responsabilidades de sus áreas y personal interno y externo.

III. Alcance

Esta política es de carácter obligatorio y se aplica a todas las áreas de La Araucana CCAF, incluyendo a proveedores externos y entidades con las cuales existan acuerdos de colaboración.

También es aplicable a todo activo de información que La Araucana C.C.A.F. posea, y cubre toda la información, entre otros, la impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos.

Cualquier excepción a esta política serán permitidas solamente cuando sean aprobadas previamente por escrito por el Subgerente de Seguridad de la Información & Ciberseguridad.

IV. Definiciones

Activo de información: Todo elemento tangible o no, que contenga datos relevantes para La Araucana CCAF, conservados en formato físico o electrónico, sean equipos, aplicativos, documentos e incluso personas cuyo conocimiento sirve para los propósitos de La Araucana CCAF.

Confidencialidad: Principio de seguridad que requiere que los datos deben únicamente ser accedidos por el personal autorizado a tal efecto.

Disponibilidad: Capacidad de ser accesible y estar listo para su uso a demanda de una entidad o persona autorizada.

Integridad: Principio de seguridad que certifica que los datos y elementos de configuración sólo son modificados por personal y actividades autorizadas. La Integridad considera todas las posibles causas de modificación, incluyendo fallos software y hardware, eventos medioambientales e intervención humana.

Incidente de seguridad de la información: Evento no esperado que tienen una alta probabilidad de comprometer las operaciones de La Araucana CCAF y/o amenazar la seguridad de la información de esta.

Continuidad del negocio: Persistencia de las operaciones de La Araucana CCAF.

Información: Toda comunicación o representación de conocimiento, como por ejemplo datos, en cualquier forma, tales como formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea digital, en papel, audiovisual u otro.

Seguridad de la información: Conjunto de medidas preventivas y reactivas de las C.C.A.F. y sus respectivos sistemas tecnológicos, que tienen por objeto resguardar y proteger la información, asegurando la confidencialidad, integridad, autenticidad y disponibilidad de los datos, continuidad de servicios y protección de activos de información.

Riesgo: Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes, equipos y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen corporativa.

Sistema de gestión de seguridad de la información (SGSI): Proceso sistemático basado en un enfoque de riesgo organizacional, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

Información confidencial: Se considera información confidencial aquella relacionada con aspectos estratégicos de negocios de La Araucana CCAF, bases de datos, segmentaciones de clientes o cualquier información sobre los negocios u operaciones de la organización y sus clientes, aunque en ellos no haya intervenido el trabajador directamente.

V. Referencia

- Compendio de Normas que regulan a las C.C.A.F,
- PO-GROP-001 Política Gestión de Riesgo Operacional
- PR-GROP-005 Procedimiento de Gestión de Riesgo Operacional
- PR-RIOP-184 Reporte incidente operacional
- PR-GISI-158 Procedimiento de gestión de incidentes de seguridad de la información
- PR-PEDP-157 Procedimiento de protección y eliminación segura de datos personales
- PR-CACO-174 Procedimiento de carpetas compartidas_V3
- Listado de normas aplicables, identificadas en anexo I.

VI. Política

1. Compromiso La Araucana C.C.A.F.

La Caja tiene como objetivo entregar calidad y oportunidad en las prestaciones de sus afiliados, basándose para ello en los principios de respeto, transparencia, dignidad e igualdad de trato. En tal sentido, el trabajo se enfoca en desarrollar conjuntamente con sus trabajadores, proveedores y afiliados relaciones armónicas para prestar un servicio adecuado, respetando el marco legal y sus propósitos; motivando alianzas con los actores socio-políticos y económicos en pro del desarrollo de las Cajas de Compensación de Asignación Familiar, beneficiando a toda la población afiliada, manteniendo una relación permanente con las empresas afiliadas, los trabajadores beneficiarios y los pensionados afiliados, buscando el crecimiento constante de la población beneficiaria, el equilibrio en la compensación y la ampliación de la cobertura subsidiada, siempre procurando la cooperación y la sana competencia, con entidades que puedan desarrollar objetos sociales similares.

La normativa que regula actualmente las Cajas de Compensación les permite proveer diversos servicios y prestaciones a sus afiliados, entre los cuales destacan la administración de prestaciones de seguridad social, las prestaciones legales, las de bienestar social, prestaciones adicionales y complementarias. Por lo tanto, todo activo de información relacionado a estos servicios y prestaciones, como también a los procesos que permitan otorgarlos, como Caja tenemos la responsabilidad y obligación de preservarlos frente a riesgos que atenten contra su confidencialidad, disponibilidad e integridad, como son la apropiación y distribución indebida, venta, alteración y/o destrucción. Esto se refuerza aún más si tienen relación con aspectos estratégicos, información de afiliados y/o trabajadores de la compañía, por lo que se debe velar por la continuidad del negocio ante cualquier contingencia que intente o vulnere alguno de los aspectos se seguridad de la información indicados en esta política.

En materia de privacidad y protección de la información personal, conforme con la legislación y normativa vigente, La Araucana CCAF deberá implementar mecanismos fiables que aseguren la protección de los datos personales proporcionados por los afiliados durante todo el ciclo de vida de su gestión.

2. Roles y responsabilidades

Para asegurar la correcta implementación, mantención, mejora y difusión del SGSI se definen los siguientes roles y responsabilidades.

2.1 Directorio

Es responsable de aprobar la presente Política General de Seguridad de la Información, así como proveer los recursos necesarios para su cumplimiento de acuerdo con el objetivo y compromiso definido.

2.2 Comité de Riesgo

En materia de seguridad de la información, son funciones del Comité de Riesgo las siguientes:

- Autorizar para la posterior aprobación del Directorio, de la presente Política General de Seguridad de la Información.
- Aprobar el alcance del SGSI.

- Revisar prioridades y asignar recursos para los proyectos relacionados con seguridad de la información.
- Supervisar la implementación del programa de trabajo asociado al SGSI.
- Conocer los riesgos a los cuales se encuentran expuestos los activos de información.
- Revisar el registro de incidentes de seguridad de la información y ciberseguridad, junto con las medidas de resolución y mitigación.
- Resolver conflictos que tengan relación con la seguridad de la información, discutir sus riesgos y proponer soluciones.
- Aprobar las medidas adoptadas por el mal uso de los activos de información.
- Promover la gestión de la seguridad de la información al interior de la compañía.

2.3 Subgerente de Seguridad de la Información y Ciberseguridad

Son funciones del Subgerente de Seguridad de la Información y Ciberseguridad, las siguientes:

- Tener bajo su responsabilidad el desarrollo de las políticas de seguridad de la información al interior de La Araucana CCAF, así como el control de su cumplimiento y difusión.
- Liderar la implementación de controles de seguridad de la información al interior de la compañía.
- Supervisar la arquitectura de la seguridad de la información de la Caja.
- Mantener informado al Comité de Riesgo sobre la implementación del SGSI.
- Establecer mecanismos de enlace con encargados de seguridad de la información de otros organismos y/o especialistas externos.
- Coordinar respuestas frente a incidentes que afecten los activos de información bajo el alcance del SGSI.
- Mantener un registro de incidentes de seguridad de la información.
- Revisar las recomendaciones de seguridad emanadas de auditorías internas y externas, para determinar los riesgos de seguridad de la información, y evaluar en conjunto con los dueños de la información, la implementación de los controles que permitan mitigar los impactos adversos a un nivel aceptable.
- Asesorar en forma permanente y cercana a las distintas áreas de La Araucana CCAF en temas referentes a seguridad de la información.

2.4 Personal interno

Es todo trabajador con quien La Araucana CCAF mantiene un contrato de trabajo vigente, el cual es responsable de conocer, cumplir y hacer cumplir la Política General de Seguridad de la Información con posterioridad a su toma de conocimiento.

2.5 Personal Externo

Es todo trabajador asociado a un servicio externalizado que realice trabajos para La Araucana CCAF con acceso a las dependencias como a la información de la compañía, tanto en forma física como lógica. El personal externo deberá tomar conocimiento de esta política por la gerencia que contrató sus servicios y la misma se hará responsable para que este cumpla con las obligaciones establecidas en esta política y su procedimiento.

2.6 Gerentes: Responsables de la Información

Son responsables de la información que se genera producto de los procesos bajo su responsabilidad, como de su clasificación, actualización y otorgamiento de permisos de accesos.

2.7 Gerente de Capital Humano

Es responsable de proveer oportunamente información de primera fuente respecto de las altas, bajas y/o modificaciones de cargo sobre los trabajadores de La Araucana CCAF, que permita controlar de manera efectiva el adecuado acceso a la información.

2.8 Fiscalía

Es responsable de asesorar, verificar y comunicar toda modificación relativa a la normativa legal vigente, relacionada con la seguridad de la información, que pueda generar deberes y obligaciones para La Araucana CCAF.

2.9 Contraloría

Es responsable de la revisión sobre la efectividad de los controles implementados, y de proporcionar oportunamente las observaciones y recomendaciones de seguridad de la información al Subgerente de Seguridad de la Información y Ciberseguridad, partes relacionadas, para que sean abordadas con la celeridad correspondiente.

3. Políticas específicas

De esta Política General de Seguridad de la Información, se desprenden las siguientes políticas específicas, que complementan e instruyen a todas las áreas, personal interno y externo de La Araucana CCAF sobre las diferentes responsabilidades y obligaciones que deberán asumir en materias relativas a la seguridad de la información.

Las políticas referidas a continuación adoptan las declaraciones y compromisos descritos en el presente documento.

3.1. Política de control de acceso

- **Objetivo**

Prevenir accesos no autorizados, que por consecuencia puedan terminar en daños, alteración y/o robo de los activos de información de La Araucana CCAF.

a.1 Sobre el control de acceso físico

División Administración

- Velar que los accesos a La Araucana CCAF se encuentren restringidos y sean controlados. Adicionalmente debe asegurar que el ingreso a toda área bajo la cual se administra información confidencial sea efectuado solamente por personas debidamente autorizadas.
- Otorgar credencial de visita a personas externas a La Araucana CCAF, las que deberán ser portadas en un lugar visible. Esta credencial será proporcionada por personal de la recepción de La Araucana CCAF.
- Revocar inmediatamente los permisos de acceso a las dependencias de La Araucana CCAF de aquellos colaboradores que han finalizado su relación laboral con ella, previa comunicación de la Gerencia de Capital Humano.

Gerencia de Capital Humano

- Revisar con la gerencia respectiva los permisos asignados según el perfil del colaborador. En los casos de cambio del perfil, deberá verificar que éstos sigan siendo válidos de acuerdo a su nueva función. De lo contrario, debe comunicar a División Administración para que ejecute los cambios y adecuaciones correspondientes.
- Comunicar a la División Administración el término de relación laboral de un colaborador para la revocación inmediata de los permisos de acceso en uso.

Personal interno.

- Portar y utilizar, para acceder a las instalaciones de La Araucana CCAF, su tarjeta de identificación. Esta es de uso personal e intransferible.
- No exhibir la tarjeta de identificación de La Araucana CCAF, en lugares públicos para el desarrollo de actividades que no tengan relación con ella.

a.2 Sobre el control de acceso a los sistemas y aplicativos

- Los accesos deben ser validados por la Subgerencia de Seguridad de la Información y Ciberseguridad, con la finalidad de identificar potenciales riesgos asociados a conflictos de intereses o falta de segregación funcional.
- El perfil de acceso debe limitarse solo al ámbito que sus funciones requieren, cuyas actividades se encuentran definidas en las descripciones de cargo respectivas.
- Todo nuevo acceso que no tenga relación con la descripción de cargo del colaborador debe ser solicitada por su jefatura directa. Esta asignación en ningún caso deberá ser permanente.
- El otorgamiento de accesos debe considerar una adecuada segregación de funciones, de modo tal, que un mismo trabajador no pueda disponer por su sola voluntad, del control total de un proceso de negocios.

Las excepciones a la regla deben ser aprobadas por el Subgerente de seguridad de la información y Ciberseguridad y presentadas en el siguiente Comité de Riesgo.

3.2. Política de carpetas compartidas

- **Objetivo**

Establecer criterios de uso seguro de las carpetas compartidas en servidores destinados para estos efectos, de tal manera de proteger la información de La Araucana C.C.A.F., velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en dichas carpetas.

b.1 Restricciones generales en el uso de carpeta compartidas:

- Se prohíbe el uso carpetas compartidas para el almacenamiento de archivos personales, música, videos, imágenes y cualquier otro tipo de archivo no relacionado con el cumplimiento de la función del colaborador.
- Cada área tendrá un único administrador que será autorizado con permisos de lectura y escritura quien administrará las carpetas y será responsable del contenido de las carpetas y de a qué usuarios otorgará permisos sobre esta, a la vez de mantener actualizada la vigencia de los permisos y los usuarios autorizados.

b.2 Responsabilidades y restricciones en el uso de carpeta compartidas

Comité de Riesgo

- Responsable de supervisar la implementación de procedimientos que se desprendan de la presente política de ciberseguridad para la utilización de carpetas compartidas.
- Propondrá estrategias y soluciones específicas para la implementación de los controles necesarios para velar por el fiel cumplimiento de la política.
- Monitorear el cumplimiento de esta política y de los procedimientos asociados.

Subgerente de Seguridad de la Información y Ciberseguridad

- Supervisar el cumplimiento de la presente política referidas a las carpetas compartidas.
- Realizar revisiones anuales del inventario de las carpetas y sus permisos, solicitando a los responsables de estas validar la vigencia de usuarios y permisos, de tal manera de pedir a TI la aplicación de los cambios que correspondan.
- Realizar comunicados a todos los funcionarios de la Caja indicando Supervisar el cumplimiento de la presente política referidas a las carpetas compartidas.

Personal interno:

- Las carpetas compartidas sobre la infraestructura ofrecida serán administradas por las áreas solicitantes, quienes velarán por el buen uso de la información y de las carpetas.
- Solicitar el acceso a carpetas compartidas para el desarrollo de su trabajo y/o función vía ticket de SOLMAN, incorporando la autorización de su respectivo Gerente junto con toda la información requerida para estos efectos, como son:
    - Listados de usuarios internos con su respectivo permiso: lectura, escritura y modificación.

- Listados de usuarios externos, indicando RUT de usuario, nombre completo, empresa, junto con su respectivo permiso: lectura, escritura y modificación.

- Solicitar la eliminación de acceso y/o de la carpeta compartida, para un funcionario en particular o todos lo que cuenten acceso, incorporando la autorización de su Gerente.
- Si se requiere de alguna carpeta compartida para almacenar información que sea clasificada como "RESERVADA" o "ESTRATÉGICA", deberá indicarse en la respectiva solicitud, de tal manera de que sean analizadas por TI para su creación, acceso y respaldo en forma especial (si corresponde).
- Responsable de utilizar las carpetas compartidas solicitadas, solo para lo que fue solicitado.
- Queda prohibido compartir carpetas en los equipos asignados a cada funcionario y a través de dispositivos externos no autorizados.

Gerencia de Ecosistemas Digitales:

- Establecer e implementar las reglas de acceso que permiten llevar un control de quién tiene acceso y a qué discos y directorios.
- Permitir a los funcionarios el acceso solo a las carpetas que se le han definido necesarias para el desempeño de su trabajo y/o función específica.
- El respaldo de las carpetas compartidas estará sujetas a las políticas implementadas para toda la infraestructura tecnológica.
- Implementar planes de recuperación de desastres de los discos y directorios donde se encuentran definidas las carpetas compartidas.

3.3. Política sobre pantalla y escritorio limpio

- **Objetivo**

Prevenir divulgación no autorizada, daño, interferencias o pérdida de información debido a su uso y/o manipulación en escritorios, equipos y muebles (estantes, impresoras, proyectores, etc.)

a.1 Ubicación de estaciones de trabajo y equipo

- Las estaciones de trabajo de los trabajadores deben situarse en ubicaciones que dificulten la exposición de información a personal externo, protegiendo así, tanto el equipamiento tecnológico como la información.
- Los equipos ubicados cerca de zonas de atención o tránsito de público deben situarse de forma tal, que las pantallas no puedan ser visualizadas por personas externas.
- Las impresoras destinadas a la impresión de documentos que contengan información confidencial deben situarse en áreas que cuenten con la seguridad necesaria.

b.2 Escritorios limpios

- Al ausentarse de su estación de trabajo, esta no deberá contener dispositivos de almacenamiento de información y/o documentación a la vista. Estos activos deben resguardarse en sitios seguros dispuestos para tales efectos por la compañía.
- No ingerir líquido en las estaciones de trabajo.
- Todo mueble que pertenezca a una estación de trabajo, que contenga información confidencial, debe ser administrado bajo llave.
- Los muebles de uso compartido que contengan información confidencial deben ser administrados bajo llave y solo ser abiertos cuando se requiera dicha información.
- Toda información de carácter confidencial contenida en pizarrones dentro de la compañía debe ser borrada una vez que ésta haya sido utilizada.
- Las pantallas gigantes para presentaciones no deben ser visibles desde lugares de acceso público.
- No dejar visible las credenciales y/o contraseñas.

b.3 Pantallas limpias

- La pantalla de autenticación a la red de La Araucana CCAF debe requerir identificación mediante una cuenta y clave.
- Cuando el trabajador se ausente de su estación de trabajo, debe bloquear su equipo con el propósito de proteger el acceso a las aplicaciones y servicios de la compañía.

3.4. Política de protección de datos

Establecer directrices orientadas a proteger los datos personales de afiliados y personal interno de La Araucana C.C.A.F., estableciendo medidas y/o controles que impidan la filtración de datos sensibles, la manipulación no autorizada y la indisponibilidad de la información en todo el ciclo de vida de los datos personales.

Sobre la obtención: Se debe asegurar que se cuenta con el consentimiento y/o alguna base de legitimación para el tratamiento de datos personales.

Sobre el almacenamiento: Se debe establecer mecanismos de almacenamiento de datos personales tanto físicos como lógicos seguros, evitando el acceso indebido y la manipulación no autorizada.

Sobre la utilización: Se debe mantener la privacidad de los datos personales y utilizar únicamente para los fines correspondientes para los cuales fueron obtenidos.

Sobre la transferencia: Se debe velar por mantener la privacidad los datos personales al momento que se requiera realizar una transferencia hacia un tercero, ya sea externo o interno a la organización.

Sobre la eliminación: Se debe asegurar que la destrucción o eliminación de la información personal está siendo ejecutada mediante procesos seguros, evitando que estos puedan ser recuperados y utilizados para fines maliciosos.

VII. Aplicación de la Política de Seguridad de la Información

Con objeto de poder aplicar las líneas de actuación expuestas en esta política, se elaborará, implantará y mantendrá un SGSI para el monitoreo continuo y cumplimiento de los propósitos de seguridad de la información, que permitirá entre otros aspectos, conocer estado de La Araucana CCAF en materia de seguridad de la información, planificar y desarrollar los trabajos necesarios para la implementación efectiva de controles y de las mejoras necesarias de acuerdo con una escala de priorización, según los acuerdos y priorizaciones aprobados en el Comité de Riesgo.

La presente política será aplicada una vez que sea aprobada por el Directorio y publicada en el sitio Conectados.

VIII. Formación y Sensibilización

El Subgerente de Seguridad de la Información será responsable en conjunto con la Gerencia de Capital Humano, de elaborar el plan de formación y capacitación en materias específicas sobre la Seguridad de la Información y Ciberseguridad para todo el personal de La Araucana CCAF. Asimismo, se realizarán campañas de sensibilización sobre Seguridad de la Información y Ciberseguridad dirigidas a todo el personal de La Araucana a través del medio que se considere más efectivo, apoyado por la Gerencia de Capital Humano y comunicaciones internas.

IX. Vigencia

La presente política entrará en vigor una vez que sea aprobada por el Directorio y publicada en el sitio Conectados, de manera paulatina acorde con el desarrollo del plan de trabajo de formación y sensibilización que apruebe el Comité de Riesgo.

X. Sanciones por Incumplimiento de la Política

El incumplimiento de las obligaciones establecidas en este protocolo será sancionado de acuerdo a las disposiciones establecidas en el Título correspondiente del Reglamento Interno de Orden, Higiene y Seguridad de La Araucana C.C.A.F., en concordancia a lo señalado en el numeral 10 del artículo 154 del Código del Trabajo.

Asimismo, las infracciones por incumplimiento de la política podrán constituir una violación a los lineamientos éticos, valores y principios que deben orientar el desempeño de los trabajadores de La Araucana CCAF consagrados en su Código de Buenas Prácticas y de Conducta, siendo de su responsabilidad aplicarlos en cada una de las actuaciones que el ejercicio de sus funciones demande.

XI. Frecuencia de Revisión y Actualización de la Política

La Araucana CCAF establece que la presente política será revisada, evaluada y actualizada por el Subgerente de Seguridad de la Información y Ciberseguridad en forma anual o cada vez que existan circunstancias que así lo ameriten tales como cambios en la industria, condiciones legales, regulatorios o del cambiante entorno tecnológico actual.

La actualización a la que sea sometida la presente política deberá ser revisada y aprobada por el Comité de Riesgo, y posteriormente por el Directorio de La Araucana CCAF.

XII. Tabla Control de Cambios

Versión	Fecha Modificación	Aspectos Modificados
002	15-09-2016	Actualización de la política de seguridad vigente desde el día 12.08.2013, publicada en La Araucana al día y aprobada por el Comité de Seguridad de la Información, (versión 001).
003	20-03-2017	Actualización del documento actualizado anteriormente por la Subgerencia de Gobierno TI y Operaciones del 15.09.2016, que estaba a la espera de aprobación del Directorio, para la generación de la Política de Seguridad de la Información presentada en este documento. Corresponde a una modificación integral de la política. (Definición de roles y responsabilidades, objetivos propios de la seguridad de la información, incorporación de protección de datos de información personal).
003	13-06-2017	Incorpora al Gerente General y Fiscal como miembros del Comité de Seguridad de la Información, de acuerdo con lo solicitado por el Comité de Riesgo, en sesión del día 13.06.2017 en el cual se presentó la Política de Seguridad de la Información para solicitar su aprobación al Directorio.
003	11-07-2017	- Aprobación de la Política de Seguridad en el Comité de Riesgo.
004	23-12-2019	- Actualización de la Política General de Seguridad de la Información por el Oficial de Seguridad de la Información incorporando y actualizando los siguientes apartados: - Constitución del Comité de Seguridad de la Información - Detalle de responsabilidades del Oficial de Seguridad de la Información. - Lineamientos relativos al control de acceso - Lineamientos sobre pantalla y escritorio limpio - Lineamientos sobre el uso de internet - Lineamientos sobre el uso de correo electrónico - Listado de normas aplicables - Lineamientos sobre gestión de los Activos de Información - Se eliminó lista de procedimientos asociados dado que no eran procedimientos válidos, si no, más bien referenciales esperados.

		- Aprobado en Sesión de Comité N° 130. - Aprobado en Sesión de Directorio N° 610.

005	21-12-2021
	27-12-2021
		- Se incorporan referencias a documentos asociados a la Seguridad de la Información.
		- Se incorporan las indicaciones de la Circular N°3.594, Gestión del Riesgo Operacional en Materias de Ciberseguridad:
		  - Compromiso La Araucana CCAF.
		  - Frecuencia de revisión y actualización de la Política.
		- Se incorpora la Política específica de carpetas compartidas.
		- Se actualizan las funciones del Subcomité de Seguridad de la Información.
		- Aprobado en Sesión de Comité N° 155.
		- Aprobado en Sesión de Directorio N° 634.

006	21-12-2022 27-12-2022	- Se modifican roles y nombres de cargo, dada la nueva estructura organizacional y nuevos participantes. - Se deja el subcomité de seguridad de la información y ciberseguridad Trimestralmente, así se presentan los cierres y monitoreo de cada trimestre. - Se agrega un apartado de protección de datos, haciendo referencia al procedimiento y los lineamientos de protección. - Se agrega en el apartado de proveedores lineamientos que permitan mantener identificados a los proveedores. - Se agrega además la evaluación de los proveedores identificando sus ciber-riesgos. - Se agrega un apartado robusteciendo el ítem de desarrollo seguro. - Se modificarán los lineamientos para los proveedores externos asociados a las capacitaciones, con el final de garantizar que el personal externo mantenga conocimiento de la “Política de seguridad de la información”. - Se agregan referencias de procedimientos e instructivos como indica la nueva circular. - Aprobado en Sesión de Comité N°167. - Aprobado en Sesión de Directorio N° 646.
007	19-12-2023 20-12-2023	- Se agrega referencia a Procedimiento de carpetas compartidas. - Se elimina la posibilidad de solicitar permiso de control total.

		- Se elimina detalle de límite de tiempo para carpetas compartidas. - Se elimina detalle de tamaño aproximado para la información a almacenar. - Se elimina identificación, respaldo y posterior eliminación de información que supere 1 año de antigüedad. - Aprobado en Sesión de Comité N°179. - Aprobado en Sesión de Directorio N° 658.
008	25-06-2024	- Se separan los aspectos de Ciberseguridad de esta política, para adjuntarlos en una nueva Política de Ciberseguridad por separado conforme a REF.: Oficio PAE N° O-108415-202, del 17-11-2023 de la SUSESO, vinculado con el tema de "Ciberseguridad". - Aprobado en Sesión de Directorio N° 664.

XIII. Anexos

Anexo I : Listado de normas aplicables.

Anexo II : Consideraciones sobre la gestión de activos de información.

Anexo III : Consideraciones sobre el respaldo de Información.

Anexo IV : Consideraciones sobre seguridad de las comunicaciones.

Anexo V : Consideraciones sobre relación con proveedores.

Anexo VI : Consideraciones sobre adquisición, desarrollo y mantenimiento de sistemas.

Anexo VII : Dominio de control.

Anexo I: Listado de normas aplicables

El presente listado de normas, aborda aspectos referentes al dominio “A.18 Cumplimiento” del estándar NCh-ISO 27001:2013, y constituye una referencia normativa mínima a considerar por los trabajadores de La Araucana CCAF en la adquisición, diseño, desarrollo, operación, uso y/o gestión de activos de información, así como de la contratación y gestión de productos y servicios relacionados con ellos, con el fin de evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual, y de cualquier requisito de seguridad.

N°	DOCUMENTO
1	NOMBRE: SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA TIPO DE NORMA: LEY NÚMERO: 19.799 ORGANISMO: MINISTERIO DE ECONOMÍA, FOMENTO Y RECONSTRUCCIÓN; SUBSECRETARÍA DE ECONOMÍA, FOMENTO Y RECONSTRUCCIÓN url: http://www.leychile.cl/navegar?idnorma=196640
2	NOMBRE: SOBRE PROTECCIÓN DE LA VIDA PRIVADA TIPO DE NORMA: LEY NÚMERO: 19.628 ORGANISMO: MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA URL: http://www.leychile.cl/Navegar?idNorma=141599
3	NOMBRE: ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS, DEROGA LA LEY N° 19.223 Y MODIFICA OTROS CUERPOS LEGALES CON EL OBJETO DE ADECUARLOS AL CONVENIO DE BUDAPEST TIPO DE NORMA: LEY NÚMERO: 21.459 ORGANISMO: MINISTERIO DE JUSTICIA URL: https://www.bcn.cl/leychile/navegar?idNorma=1177743&idParte=10343833
4	NOMBRE: PROPIEDAD INTELECTUAL TIPO DE NORMA: LEY NÚMERO: 17.336 ORGANISMO: MINISTERIO DE EDUCACIÓN PÚBLICA URL: https://www.leychile.cl/Navegar?idNorma=28933

5	NOMBRE: MODIFICA EL CODIGO PENAL, EL CODIGO DE PROCEDIMIENTO PENAL Y EL CODIGO PROCESAL PENAL EN MATERIA DE DELITOS DE PORNOGRAFIA INFANTIL TIPO DE NORMA: LEY NÚMERO: 19.927 ORGANISMO: MINISTERIO DE JUSTICIA URL: https://www.leychile.cl/Navegar?idNorma=220055
6	NOMBRE: TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. TIPO DE NORMA: NORMA CHILENA NÚMERO: NCH-ISO 27001.OF2013 ORGANISMO: INSTITUTO NACIONAL DE NORMALIZACIÓN URL: N/A
7	NOMBRE: CONDUCTAS Y PRACTICAS CORPORATIVAS QUE DEBEN SER IMPLEMENTADAS POR LAS CAJAS DE COMPENSCIÓN DE ASIGNACION FAMILIAR TIPO DE NORMA: Compendio de Normas que Regulan las C.C.A.F. TÍTULO: Libro V Aspectos operacionales y administrativos. ORGANISMO: SUPERINTENDENCIA DE SEGURIDAD SOCIAL
8	NOMBRE: REGLAMENTO INTERNO DE ORDEN, HIGIENE Y SEGURIDAD TIPO DE NORMA: DOCUMENTO INTERNO
9	NOMBRE: GESTIÓN DE RIESGO OPERACIONAL TIPO DE NORMA: Compendio de Normas que Regulan C.C.A.F. TÍTULO: Libro VI Gestión de Riesgos ORGANISMO: SUSESO
10	NOMBRE: INSTRUCCIÓNES SOBRE EL SISTEMA DE CONTROL INTERNO TIPO DE NORMA: Compendio de Normas que regulan las C.C.A.FTÍTULO: 5.2 TÍTULO II Control Interno. ORGANISMO: SUSESO

Anexo II: Consideraciones sobre la gestión de activos de información

Las siguiente consideraciones, abordan aspectos relativos al dominio “A.8 Administración de los activos” del estándar NCh-ISO 27001:2013, y tienen por objeto establecer en términos generales una adecuada administración de los activos de información de La Araucana CCAF.

Todo activo de información de la compañía deberá clasificarse según su nivel de importancia, criticidad y sensibilidad a la divulgación, modificación no autorizada y/o eliminación. Los niveles de clasificación deben ser evaluados no sólo respecto de la perspectiva de la compañía, sus procesos y su necesidad de compartir información, sino también respecto de aquellos aspectos que afectan directamente a nuestros afiliados (Ej.: Información de deudas, créditos, datos personales, pagos, diagnósticos de licencias médicas, etc.) considerando aspectos legales y normativos, según corresponda.

La divulgación de información puede tener diferentes niveles de impacto para la compañía dependiendo si ésta afecta la continuidad operacional de los procesos de negocio, como aquella divulgación que impacta en el logro de los objetivos de La Araucana CCAF en el corto, mediano y largo plazo. Por tanto, al clasificar los activos de información se debe considerar si la misma debe permanecer de manera confidencial, sólo para uso interno de la compañía, pública, pública con restricciones, o restringida.

Adicionalmente, deberá existir coherencia entre los privilegios de accesos otorgados a los usuarios y la clasificación de la información. Es decir, el nivel de protección que se requiere respecto de la Confidencialidad, Disponibilidad e Integridad de la información. Estos criterios de evaluación serán los mismos para todas las evaluaciones de activos de información, con el objeto de unificar criterios.

Del mismo modo, se deberá mantener control sobre los activos de información, así como los medios que los soportan, junto con los responsables de su utilización y protección, documentados en un inventario de activos de información indicando claramente a los dueños y responsables de los mismos.

Anexo III: Consideraciones sobre el respaldo de Información

Los siguientes lineamientos tienen relación con el dominio “A.12 Seguridad de las operaciones” del estándar NCh-ISO 27001:2013. Particularmente con el control A.12.03.01 Respaldo de información.

Toda información que sea crítica para La Araucana CCAF y que sea determinante para la continuidad de las operaciones y relación con nuestros afiliados, deberá ser debidamente respaldada, permitiendo su restauración frentes a incidentes de seguridad en el menor tiempo posible.

Todo el personal interno deberá mantener su información en las carpetas designadas para tales efectos.

Los respaldos de sistemas de información deben contar con un adecuado control de protección física y ambiental, y deben contar con un plan regular de prueba de restauración y verificación de los tiempos, exactitud y completitud de la información. Las pruebas y la capacidad de restaurar los datos de respaldo deben ser realizadas sobre copias independientes, no sobrescribiendo el soporte original en el caso que el proceso de restauración sufra algún tipo de falla y produzca daños irreparables o pérdida de datos. Adicionalmente, si los respaldos contienen información confidencial, estos deben ser protegidos de acceso no autorizado.

Los planes de restauración de copias de datos, deben estar en sintonía con el plan de recuperación y continuidad operacional. (BCP – Plan de Continuidad de Negocio y DRP – Plan de Recuperación de desastre)

Anexo IV: Consideraciones sobre seguridad de las comunicaciones

Las siguientes consideraciones tienen relación con el dominio “A.13 seguridad en las comunicaciones” del estándar NCh-ISO 27001:2013.

Tanto el personal interno como el personal externo que tenga acceso a información estratégica y/o confidencial de La Araucana CCAF, tiene la responsabilidad de administrar dicha información a través de canales seguros de comunicación.

Se deberán mantener los resguardos necesarios que permitan asegurar la protección de la confidencialidad, disponibilidad e integridad de la información, en las redes locales y públicas, contra el acceso no autorizado.

Anexo V: Consideraciones sobre relación con proveedores

Las siguientes consideraciones tienen relación con el dominio “A.15 relaciones con el proveedor” del estándar NCh-ISO 27001:2013.

Se deberá acordar y documentar los requisitos de seguridad de la información, con cada proveedor que requiera acceder tanto física como lógicamente a la información de la compañía, ya sea para procesar, almacenar, comunicar o proporcionar componentes de infraestructura tecnológica. Del mismo modo, se identificarán y documentarán los riesgos asociados, así como los controles que serán aplicados. Adicionalmente, se deberán documentar un acuerdo de confidencialidad, antes de dar inicio al servicio junto con la acreditación de participación en el curso de Seguridad de la Información de CCAF La Araucana.

Las acciones que realicen los proveedores dentro de la compañía deberán ser monitoreadas y registradas por el responsable de la contratación o en quién se delegue, las cuales deben ser consistentes con las prestaciones contratadas, y todo cambio requerirá una reevaluación de los riesgos identificados a partir del mismo.

Se evaluará a todos los proveedores nuevos que trabajen con la Caja para poder determinar el nivel de madurez que tienen con el ciber-riesgo, a raíz de la evaluación se realizara el monitoreo de los ciber-riesgos encontrados.

Anexo VI: Consideraciones sobre adquisición, desarrollo y mantenimiento de sistemas

Los siguientes lineamientos tienen relación con el dominio “A.14 desarrollo, adquisición de mantenimiento de sistemas” del estándar NCh-ISO 27001:2013.

Los aspectos de seguridad de la información deberán ser parte integral de los procesos de adquisición, cambios significativos en la tecnología existente, durante la planificación, diseño, evaluación de riesgos del proyecto, desarrollo, prueba, control de calidad, puesta en producción, control de cambios y mantención de los sistemas de información que se produzcan en La Araucana CCAF, con el fin de asegurar la protección de la información respecto de la confidencialidad, disponibilidad e integridad de la misma.

Anexo VII: SGSI - Dominios de control

La implementación del SGSI de La Araucana CCAF se enmarca en función de los requisitos establecidos a través el estándar NCh-ISO 27001:2013 bajo los siguientes dominios de control:

a. Políticas de Seguridad de la Información
b. Organización de la Seguridad de la Información
c. Seguridad ligada a los Recursos Humanos
d. Administración de Activos
e. Control de Acceso
f. Criptografía
g. Seguridad Física y del Ambiente
h. Seguridad de las Operaciones
i. Seguridad de las Comunicaciones
j. Adquisición, desarrollo y mantenimiento del Sistema
k. Relaciones con el Proveedor
l. Gestión de Incidentes de Seguridad de la Información
m. Aspectos de la Seguridad de la Información en la gestión de la continuidad del negocio
n. Cumplimiento