Reglamento

“CI04-07 Seguridad de la Información para Proveedores y Terceros”

Confuturo 2021

INDICE

Hoja De Aceptación

Nombre del Documento : Seguridad de la Información para Proveedores y Terceros

Versión Nº	Fecha Versión	Fecha Vencimiento (Max. 24 meses)	Comentarios / Modificaciones
2.0	Diciembre 2021	Diciembre 2023	**Cargos que deben conocer el procedimiento:** Todos los cargos **Editor** Seguridad de la Información

Información del Reglamento

Nombre :	Reglamento Seguridad de la Información para Proveedores y Terceros	Código	CI04-07
Proceso:	CI Gestión de Control Interno	Subproceso:	CI04 Seguridad de la Información
Dueño del Proceso:	Gerente de Riesgo y Finanzas	Clasificación de la información:	Uso Interno
Responsable de Proceso	Oficial de Seguridad de la Información	Aprobado	por CSI

Condiciones de Aceptación
La aceptación tiene como objeto el cumplimiento de las siguientes afirmaciones: ✓ La descripción de este procedimiento es el fiel reflejo de las tareas y acciones que se desarrollan durante la ejecución del mismo. Contempla el análisis de los riesgos inherentes y residuales propios del proceso, establece los controles mitigadores de éstos cuando corresponde y contiene las mejoras sugeridas por la Subgerencia Eficiencia y Control de Riesgo Operacional que son aceptadas por el dueño del proceso. ✓ Toda modificación al procedimiento debe ser informada por el usuario líder, tanto a las áreas involucradas como a la Subgerencia Eficiencia y Control de Riesgo Operacional, para su actualización y publicación

I. INTRODUCCIÓN

El constante avance en el desarrollo y adopción de nuevas y mejores tecnologías aplicadas a las organizaciones y sus procesos, junto con hacer estos procesos más efectivos y eficientes trae consigo un cambio en los riesgos existentes junto con permitir la aparición de nuevos. Si a este escenario le agregamos la interacción con entes externos a las organizaciones, como es el caso de proveedores de servicios, tenemos un ecosistema más amplio que requiere atención y una gestión de riesgos efectiva. Dentro de las funciones de Seguridad de la Información es clave contar con definiciones y lineamientos que permitan regular las relaciones con proveedores y terceros que interactúan y/o tienen acceso a los activos de información de las organizaciones, con la intención de hacer estas interacciones seguras en un entorno protegido

II. PROPÓSITO

El presente documento pasa a incorporarse al marco normativo de Seguridad de la Información de Confuturo S.A. (en adelante, la Compañía), con la finalidad de establecer los lineamientos, principios y definiciones en torno a la relación con proveedores de servicios y socios estratégicos en este mismo contexto.

III. ALCANCE

El presente documento tiene por alcance la totalidad de los proveedores, socios y otros entes externos equivalentes que interactúen de forma autorizada con la información (o activos de información) de la Compañía. Adicionalmente, este documento pasa a complementar las definiciones vigentes en la Compañía en lo referente a la gestión de proveedores y la relación con terceros.

IV. DOCUMENTOS DE REFERENCIA

- Política de Compras
- Procedimiento de Gestión de Compras
- Política de Riesgo Operacional
- Política de Seguridad de la Información
- Política de TI y Comunicaciones

V. ROLES Y RESPONSABILIDADES

Oficial de Seguridad de la Información. Es el colaborador que preside el Comité de Seguridad de la Información y, además, es el responsable de velar por la difusión y el cumplimiento de lo establecido en la política, los reglamentos y procedimientos derivados de ésta a nivel de la Compañía; junto con proponer las modificaciones que sean necesarias para mantenerlos actualizados en relación con los estándares y normativas vigentes relativas a la seguridad de la información. Debe actuar como un asesor para las distintas áreas de negocio en el ámbito de seguridad y gestión de riesgos.

Comité de Seguridad de la Información (CSI). Establecer y aprobar las políticas y procedimientos para el cumplimiento de las funciones relacionadas con la Seguridad de la Información en la Compañía, su ámbito de acción, conformación, funcionamiento, funciones y resoluciones. También es responsable de aprobar los reglamentos relacionados a esta política, así como también tomar conocimiento, analizar y determinar acciones a realizar frente a las excepciones que le sean escaladas por el Oficial de Seguridad de la Información o que sean detectadas por otras vías en relación a lo establecido en el presente documento. Sus responsabilidades se definen en el Reglamento del Comité de Seguridad de la Información.

Comité de Gestión de Riesgos. Comité responsable de analizar todos los incidentes de riesgo operacional originados por fallas de personas, procesos, sistemas o eventos externos, proponiendo mitigaciones para fortalecer el ambiente de control de los procesos de la Compañía. En materias de Seguridad de la Información, responsable de tomar conocimiento de las gestiones realizadas y reportadas por el área de Seguridad junto con definir acciones a realizar dentro de este mismo ámbito. Al Comité de Gestión de Riesgos le corresponde, además, contribuir a la coordinación y coherencia de las decisiones y gestiones que adopten las diversas áreas o gerencias cuyo trabajo incide en la Seguridad de la Información, particularmente las encargadas de operaciones, riesgos y tecnologías de información.

Especialista de Seguridad de la Información. Responsable de llevar a cabo los procesos y actividades propios del ámbito de Seguridad de la Información, asesorar a las áreas de negocio y apoyar la gestión del Oficial de Seguridad de la Información.

Dueños de Activos de Información. Es el colaborador, usualmente de la alta administración de la Compañía, quien, en función de su rol en la organización, tiene la responsabilidad sobre determinados activos de información. Deben velar por su adecuada protección al determinar qué usuarios pueden tener permisos de acceso a esos activos de información y con qué nivel de privilegios. Es responsable de administrar, autorizar el uso, regular o gestionar el activo de información. El dueño del activo propone el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

Custodios de Activos de Información. Son los colaboradores o grupos de colaboradores a los cuales el dueño de la información entrega, total o parcialmente, la tenencia y protección de determinados activos de información que son de su responsabilidad. Habitualmente, aunque no exclusivamente, el área de Infraestructura Tecnológica es custodio de los activos de información de la Compañía que son capturados, generados, almacenados, procesados y transmitidos electrónica o digitalmente a través de la plataforma tecnológica que esta área entrega a la Compañía. Deberá mantener comunicación permanente con el dueño del activo para reportes de los resultados de la aplicación de los controles.

Gerentes de Área. Asegurar la incorporación, aplicación y fomentar el cumplimiento de esta normativa en los procesos bajo su responsabilidad.

Administrador de Contrato. Encargado de definir y establecer los requerimientos técnicos (especificaciones técnicas, condiciones de operación y puesta en marcha, plazos, rendimientos, etc.), y niveles de servicio para conformar las bases de licitación y solicitar las cotizaciones a los proveedores. Corresponde a la contraparte técnica en el proceso de contratación y gestión de proveedores que lidera la Subgerencia de Administración. Es también responsable, en los proveedores, de verificar el cumplimiento de las cláusulas contractuales, controlar y analizar los niveles de servicio de modo de detectar oportunamente

incumplimientos, coordinar plazos de entrega de bienes y/o prestación de servicios, velar por el cumplimiento de la legislación vigente, cumplimiento de obligaciones previsionales, ingreso de solicitudes de compra y autorizar los pagos en base a los acuerdos contractuales celebrados con los proveedores. A su vez, debe informar aquellas situaciones especiales que puedan afectar la relación entre las partes para establecer planes de mitigación cuando corresponda. Todo lo anterior enmarcado por las definiciones y normativa interna establecidas por la Compañía, a través de la Subgerencia de Administración.

Fiscalía. Responsable de revisar los antecedentes legales de la contraparte (proveedor o tercero), tales como personerías, vigencias y constitución de sociedades; validar desde el punto de vista legal borradores de contrato y sus anexos, NDAs, cartas de término y finiquitos de contratos de proveedores. También es responsable de asesorar y apoyar en materias contractuales a las áreas de la Compañía que lo requieran.

Colaboradores. Proteger proactivamente, en todo momento, los Activos de Información de la Compañía, conociendo, comprendiendo y cumpliendo las directrices y normativas internas de ésta. Es también una obligación de los colaboradores reportar oportunamente cualquier riesgo no identificado (amenaza o vulnerabilidad) y los eventos sospechosos e incidentes que comprometan o puedan comprometer a los Activos de Información de la Compañía, de acuerdo a los canales establecidos por ésta para ello.

Es también una obligación de los colaboradores reportar oportunamente cualquier riesgo no identificado (amenaza o vulnerabilidad) y los eventos sospechosos e incidentes que comprometan o puedan comprometer la Seguridad de la Información de la Compañía, de acuerdo al Procedimiento de Gestión de Incidentes de Riesgo Operacional.

En el caso de terceros que trabajen con la Compañía y tengan acceso a activos de información de ésta, es responsabilidad de los colaboradores de la Compañía poner en conocimiento de los terceros nuestras prácticas y normas de seguridad de la información y asegurarse de que éstas sean cumplidas por ellos, y que existan los resguardos contractuales correspondientes, de acuerdo al presente documento y las definiciones establecidas por la Subgerencia de Administración. Esta responsabilidad recae en el Administrador de Contrato o bien en la contraparte interna que coordina la entrega de productos o servicios con el proveedor.

VI. Relación con Clientes Proveedores y Terceros DIRECTRICES Y LINEAMIENTOS GENERALES

6.1. Previo a Establecer la Relación

El proceso para establecer una relación con un nuevo proveedor o tercero que prestará servicio a la Compañía debe pasar por una serie de instancias de revisión, aprobación y formalización, que se describen en el documento Política de Compras de la Compañía. Cabe mencionar que este proceso se encuentra bajo responsabilidad de la Gerencia de Recursos Humanos y Administración, específicamente de la Subgerencia de Administración.
Todo lo establecido en el presente documento es una extensión de las definiciones establecidas por la Subgerencia de Administración para este efecto y, en caso de existir

precisiones o diferencias, primarán las definiciones establecidas en la Política de Compras y documentos que de ella deriven.

En aquellos casos en que, por las características del servicio, demostraciones o instancias de validación de las capacidades del producto o servicio a adquirir, se requiera compartir información de la Compañía o más específicamente de sus clientes y pensionados de cualquier modo y en cualquier formato previo al establecimiento de una relación comercial con un potencial proveedor, la Compañía debe firmar un acuerdo de confidencialidad o NDA (por sus siglas en inglés) con el proveedor o tercero respectivo. Lo anterior, con el fin de proteger la información que se comparta producto de la actividad a realizar.

Los acuerdos de confidencialidad serán gestionados por la Subgerencia de Administración y deberán ser revisados y autorizados por el área de Fiscalía.

Se excluyen de lo anterior los siguientes casos:

- Cuando la información que se comparta sea de carácter público y de libre acceso tanto para el proveedor, como para la Compañía y cualquier tercero.
- Cuando se utilicen datos de prueba, es decir, datos que no tengan similitud alguna con la información real de la Compañía o sus clientes y pensionados, ya sea a través de procesos de enmascarado o aleatorización o modificación de estos. Cabe señalar que estos datos no deben permitir bajo ningún concepto identificar información real de clientes, pensionados o de procesos de la Compañía.

En caso que el proveedor o potencial proveedor corresponda a un servicio y/o producto crítico, su tratamiento debe ser de acuerdo a lo establecido en la Política de Compras y Procedimiento de Gestión de Compras para los proveedores críticos. A su vez, esta información debe estar en conocimiento del área de Riesgo Operacional, para ser abordado de acuerdo a las definiciones de Continuidad del Negocio que establece la Compañía.

6.2.Al Establecer la Relación

Una vez seleccionado un proveedor y establecida la relación con éste bajo cualquiera de las modalidades definidas para ello (compra por cotización, por licitación o compra directa), se deberá contar con un contrato o bien una orden de compra que formalice la relación, de acuerdo con las definiciones establecidas en la Política de Compras de la Compañía.

En el caso de establecer una relación a través de órdenes de compra que involucren servicios que impliquen compartir información, la Compañía y el proveedor deberán contar con un NDA firmado previamente, que proteja dicha información que se compartirá, transmitirá, procesará y almacenará mientras dure la relación comercial. Los NDA podrán ser de tipo “one side” o “recíproco”, de acuerdo a la naturaleza del servicio, de la validación del administrador de Confuturo y dependiendo de las características de la relación comercial. A su vez, éstos deben contar con la revisión y aprobación de parte del área de Fiscalía de la Compañía.

Si por el contrario, se establece una relación a través de un contrato, éste debe seguir las definiciones y normativas internas antes mencionadas, y además contener las cláusulas de seguridad detalladas a continuación, con la misma finalidad de proteger la información que se comparte con el proveedor.

Una vez establecida la relación, se actúa de acuerdo al proceso de gestión de proveedores establecidos por la Subgerencia de Administración y su respectiva normativa asociada.

6.3. Cláusulas de Seguridad en Contratos.

Todos los contratos marco de la Compañía deben contar con las cláusulas de Seguridad de la Información siguientes:

- **Cláusula de Confidencialidad.** Obliga al proveedor a proteger y mantener la confidencialidad de la información compartida entre las partes, implementando las medidas o mecanismos de control necesarios para ello. Del mismo modo, prohíbe la divulgación de información a terceros sin la debida autorización y el mal uso de ésta.
- **Cláusula de Protección de Activos.** Obliga al proveedor a proteger y mantener la integridad de la información compartida entre ambas partes, implementando y documentando los mecanismos de control necesarios para ello.
- **Cláusula de Incidentes de Seguridad.** Obliga al proveedor a informar cualquier incidente de seguridad que provoque o pueda provocar el incumplimiento de la obligación de confidencialidad de la información o de protección de activos establecidas.
- **Cláusula de Auditoría.** Habilita a la Compañía a efectuar auditorías en forma periódica al proveedor, con el fin de verificar el ambiente de control de éste, en relación al servicio prestado o producto entregado.
- **Cláusula de los Planes de Continuidad del Servicio.** Obliga al proveedor a contar con planes y mecanismos que le permitan mantener la continuidad del servicio previamente acordado en caso de contingencias.
- **Cláusula de Propiedad Intelectual, Uso del Nombre y Publicidad.** Obliga al proveedor a respetar y proteger la propiedad intelectual, marca y publicidad relacionada con la Compañía, tanto en los productos desarrollados para la Compañía, como al mismo tiempo garantizar que el proveedor cuenta con los derechos de propiedad de los servicios o productos que ofrece a la Compañía.
- **Cláusula de Protección de Datos.** Obliga al proveedor a dar cumplimiento a la normativa vigente en materia de protección de datos personales y, del mismo modo, realizar el tratamiento de éstos conforme a lo instruido por la Compañía.

Del mismo modo, el área de Seguridad de la Información, a través del Comité de Seguridad de la Información o bien, del Comité de Gestión de Riesgos, podrá solicitar la incorporación de cláusulas adicionales de acuerdo al carácter del servicio prestado o del producto entregado. Lo anterior, de acuerdo al proceso de gestión de riesgos.

6.4. Capacitación y concientización

El dueño del contrato es responsable de validar que los proveedores cuenten con las instancias de concientización y capacitación sobre seguridad de la información para sus colaboradores y asociados.

En este aspecto, podrá solicitar el apoyo del área de Seguridad de la Información u otras relacionadas, con la intención de instruir la forma de trabajo y operación en la Compañía. Del mismo modo, los proveedores o terceros deben respetar y cumplir en todo momento las

definiciones y normativas internas vigentes, ya sean estas en materia de Seguridad de la Información, Ciberseguridad o Riesgo Operacional.

Se hará disponible para lectura y toma de conocimiento de cada proveedor una copia de la Política de Seguridad de la Información además del presente documento a través de un link incluido en el contrato Marco y NDA respectivo, según corresponda.

En casos puntuales que se requiera mayor detalle o validación, dicha Subgerencia o el Administrador de Contrato (quien actúa como contraparte con el proveedor respectivo) podrán tomar contacto con otras áreas internas en busca de apoyo y aclaración de dudas a los proveedores o terceros.

6.5. Supervisión y revisión

El dueño del contrato debe revisar y controlar periódicamente el nivel de los servicios y cumplimiento de las cláusulas de seguridad de parte de los proveedores y los informes y registros generados por ellos en este ámbito. El CSI debe definir con qué proveedores y periodicidad se deberá procurar evidencia de auditorías de seguridad que se relacionen con los servicios/productos prestados/entregados.

Todos los incidentes de seguridad relacionados con el trabajo del proveedor deben ser comunicados inmediatamente por el dueño del contrato, de acuerdo al Procedimiento de Gestión de Incidentes.

En caso de incidentes o riesgos, éstos podrán ser reportados por el dueño del contrato, con el fin de

6.6. Al Finalizar la Relación

Al finalizar el vínculo profesional o comercial con el proveedor, se debe actuar de acuerdo a las definiciones establecidas por la Subgerencia de Administración. Complementariamente, se debe velar por la eliminación de todos los derechos de acceso otorgados y la devolución de todo tipo de activos de propiedad de la Compañía a ésta misma, en especial los activos de información, en el caso de operar bajo la modalidad de orden de compra. Por el contrario, en el caso de operar bajo la modalidad de contrato, se debe actuar conforme al fiel cumplimiento de los acuerdos establecidos en éste.

En adición, una vez finalizada la relación, tendrán vigencia al menos por un año las condiciones establecidas en el NDA y la cláusula de confidencialidad correspondiente, tanto en la modalidad de orden de compra como en la modalidad de contrato, respectivamente.

VII. INCUMPLIMIENTOS Y EXCEPCIONES

Cualquier incumplimiento a lo estipulado en el presente documento será revisado por el Oficial de Seguridad de la Información y tratado en conjunto con la Subgerencia de Administración o bien con la Gerencia de Recursos Humanos y Administración, de acuerdo a lo establecido en la normativa interna de la Compañía. Del mismo modo, cualquier situación no contemplada en el

presente documento será analizada por el Oficial de Seguridad de la Información, informada al Comité de Seguridad de la Información y validada con el Comité de Gestión de Riesgos y/o instancias superiores, según se determine.

VIII. MODIFICACIONES Y ACTUALIZACIONES

1) Noviembre / 2019 - El documento es aprobado por el Comité de Seguridad de la Información.

2) Diciembre / 2021 – Actualización del documento. Se modifica:
   a. Dependencia del subproceso de Seguridad de la Información, acorde con el cambio de dependencia de dicha función en la Compañía.
   b. Se incorporan el apartado Introducción, y se reformulan los apartados Propósito y Alcance.
   c. Se modifican y/o actualizan los apartados: Documentos de referencia, Relación con proveedores y terceros,
   d. Se incorpora el título Directrices y Lineamientos Generales y se reorganizan en contenido del documento de acuerdo a los nuevos apartados: Previo a Establecer la Relación, Al Establecer la Relación, Al Finalizar la Relación.
   e. Se incorpora el título Incumplimientos y Excepciones.
   f. Se incorpora el apartado Roles y Perfiles y en particular el rol del Administrador de Contrato.
   g. Se alinea con lo establecido en la Política de Compras y Procedimiento de Gestión de Compras de la Compañía.

Debido al cambio de estructura se reclasifica el documento en el proceso "Gestión Control Interno" anteriormente pertenecía al proceso "Tecnología de la Información" TI05-05 Reglamento Seguridad de la Información para Proveedores"