Política de Seguridad de la Información

Introducción

La ley 20.393 de Responsabilidad Penal de la Persona Jurídica ha ido creciendo en el tiempo, la última modificación fue la ley de Delitos Económicos. Dicha ley también incorporó la ley 21.459 de delitos informáticos como uno de los delitos de segunda categoría, los que en términos generales son delitos para las empresas cuando existe un vínculo entre la persona jurídica y un colaborador de ella.

El alcance de la presente política abarca toda la información de las empresas del Grupo ICAFAL, considera todos los sistemas de información y los mecanismos que permiten su uso y almacenamiento, independientemente, si es un sistema basado en la nube, software, aplicaciones y/o herramientas tecnológicas propias o de terceros. Esta política se debe bajar en protocolos de cumplimiento de trabajadores, ejecutivos, gerentes, proveedores, contratistas, prestadores de servicios y terceros que establezcan relaciones con el grupo Icafal.

Los objetivos particulares de esta política corporativa de ICAFAL son los siguientes:

- Cumplir la normativa legal relacionada a los delitos informáticos.
- Establecer las directrices generales de Seguridad de la Información y Ciberseguridad para el grupo de empresas Icafal.
- Definir la responsabilidad de las gerencias generales de las diferentes empresas del grupo Icafal, en el cumplimiento de las políticas generales establecidas en este documento.
- Asegurar la información propia y de terceros mediante medidas de control que permitan mitigar los riesgos informáticos según su impacto en las operaciones.
- Definir que el alcance de estas medidas que abarca a todos los trabajadores, ejecutivos, gerentes del grupo de empresas Icafal, proveedores, contratistas y prestadores de servicios de las empresas del grupo Icafal, medidas que deben ser consideradas como base para las cláusulas contractuales y normativas.
- Los datos e información, cualquiera sea su naturaleza, formato y soporte, se deberán tratar con fiel apego a la legislación vigente, controles que deben estar contenidas en los contratos de trabajo, reglamentos internos y protocolos de seguridad y cumplimiento que dicte la Gerencia de Tecnologías de Información de Icafal Gestión.
- Está absolutamente prohibido la divulgación o comunicación a terceros de datos e información de una empresa Icafal sin la autorización previa de la gerencia general.
- Los datos e información definidos como críticos por sus responsables deberán ser protegidos de cualquier riesgo que afecte su reserva, totalidad e integridad.
- La Gerencia de Tecnologías de Información (TI) de Icafal Gestión, es responsable de definir estándares y controles de seguridad generales para los sistemas de

información que utiliza el grupo de empresas Icafal, incluyendo los servicios en la nube.

- Los datos e información una empresa Icafal sólo deberá ser utilizados para las funciones propias del grupo de empresas Icafal.
- Cada trabajador de las empresas del grupo Icafal, sin excepción, es responsable por la custodia y protección de datos e información que utiliza en el desempeño de sus funciones. Asimismo, solo tendrá acceso a los datos e información que sea estrictamente necesaria para la ejecución de sus tareas.
- Cada software utilizado en el grupo de empresas Icafal debe contar con su respectiva licencia.
- Evitar conexiones de internet desde redes públicas y no ingresar a la red corporativa desde estos proveedores de internet.
- Eliminar correos electrónicos de usuarios desconocidos y no acceder a los links desconocidos que contienen estos correos.
- Mantener actualizados los softwares, sistema operativo y antivirus que proporciona Icafal.
- No compartir información de Icafal con “terceros no autorizados”.
- Responder con responsabilidad a los controles de cumplimiento solicitados por el Oficial de Cumplimiento Corporativo.

Roles y responsabilidades

Se establecen los siguientes roles y responsabilidades:

Alta Administración (Directorio Icafal S.A.): es el responsable de establecer políticas, directrices y objetivos estratégicos y de debida diligencia de Icafal S.A., asegurando que éstas se ajustan a las leyes, reglamentos y normas que aplican a su sector e industria. Son los responsables de sancionar los incumplimientos del Modelo de Prevención de Delitos.

Comité de Ética, Control y Cumplimiento de Icafal S.A.: es el responsable de vigilar la aplicación de las políticas corporativas en Icafal S.A y las filiales del grupo de empresas Icafal en materias pertinentes a la prevención, control y cumplimiento de la ley N°20.393.

Oficial de Cumplimiento Corporativo: como segunda linea de defensa es el responsable de controlar el cumplimiento normativo en el grupo de empresas Icafal, relacionado a la ley 20.393 y sus modificaciones. Las gerencias generales, como primera linea de defensa son responsables de su cumplimiento.

En las revisiones de cumplimiento podrá ser apoyado por los distintos Encargados de Cumplimiento del grupo de empresas Icafal, o mediante auditorías internas. Mantendrá actualizado el MPD y los difundirá en la organización. Reportará los hallazgos al Comité de Ética, Control y Cumplimiento de Icafal SA pudiendo tambien reportar a los Directorios o Alta Administración de cada empresa según corresponda.

Mantendrá actualizado el MPD y los difundirá en la organización. Reportará los hallazgos al Comité de Ética, Control y Cumplimiento de Icafal SA pudiendo tambien reportar a los Directorios o Alta Administración de cada empresa según corresponda.

Encargado de Cumplimiento de Seguridad de la Información: es el responsable del análisis técnico de los riesgos de seguridad de la información del grupo de empresas Icafal, los que deben ser controlados en una matriz de riesgo, estableciendo los controles pertinentes para su mitigación. Estos controles se deben formalizar en Protocolos, que permiten formalizar y exigir su cumplimiento. Asimismo, debe realizar revisiones periódicas al cumplimiento de los controles establecidos. Las revisiones realizadas deben ser reportadas al Oficial de Cumplimiento Corporativo.

Gerencia General: Son la primera linea de defensa, responsables del cumplimiento de estas políticas y de la ejecución de los controles que se determinen en los protocolos de cumplimiento de cada empresa del grupo Icafal. Para tal efecto, asignará a las personas más competentes en los puestos que se requieran para el desarrollo de sus operaciones y facilitará mecanismos de capacitación para el personal de su dependencia. Deberá mantener informado al Directorio o a la Alta Administracion que corresponda, de los hechos relevantes de que esta deba tener conocimiento, y de otras materias que estime conveniente relativas al cumplimiento de la ley 20.393 y su Modelo de Prevencion de Delitos y de otras normativas legales que la afecte.

En términos generales esta política abarca los siguientes temas:

1. Gestión y protección de los equipos tecnológicos
2. Actividades efectuadas por usuarios en:
    a. Red de Intranet e internet
    b. Sistema de correo electrónico
    c. Uso de licencias de software
    d. Respaldo en la nube
3. Medidas de seguridad, procesamiento de información y datos
4. Proveedores de Sistemas de Información.
5. Gestión de los perfiles de los administradores de sistema.

Gestión y protección de los equipos tecnológicos propios y de información

- Cada Gerencia General es responsable de la gestión de sus equipos tecnológicos propios e información, esto incluye la identificación, asignación, contabilización y control de ellos, por lo tanto, cada gerencia debe tener un registro o inventario actualizado de sus equipos tecnológicos.
- La adquisición de equipos tecnológicos, desarrollo de software o sistema de información y servicios de TI a utilizar en Icafal, deben ajustarse a las políticas que la Gerencia de TI de Icafal Gestión defina.

- Antes de iniciar el uso operativo de equipos nuevos, se debe instalar un antivirus. El responsable de la Gerencia General de cada empresa debe solicitar a la Gerencia de TI de ICAFAL Gestión, el respectivo servicio.
- Los equipos tecnológicos de Icafal deben ser usados solo para operaciones propias del grupo de empresas Icafal.

Gestión y protección de equipos móviles, dispositivos de almacenamiento móvil y equipos tecnológicos de terceros

- La Gerencia de TI de Icafal Gestión, previa solicitud de una gerencia general del grupo de empresas Icafal, está autorizada a configurar cualquier equipo tecnológico de terceros y a controlar su uso en conformidad con la presente política. La Gerencia General autorizará las aplicaciones y bases de datos a las cuales pueden acceder los usuarios con equipos de terceros.
- Las personas que ingresen equipos de terceros y que tengan acceso a la red y a los sistemas de información de Icafal, deben acogerse a esta política de seguridad de información con el fin de garantizar una gestión y administración adecuada de las cuentas de usuario y contraseñas. Esta obligación debe ser incorporada mediante un anexo de contrato.
- Los equipos tecnológicos de terceros, como mínimo, deben tener instalado software antivirus.
- El usuario de equipos tecnológicos de terceros deberá realizar copias de seguridad periódicas, pudiendo solicitar el apoyo de la Gerencia de TI de Icafal Gestión cuando lo requiera.
- Los equipos tecnológicos de terceros no deben contener software sin licencia. Todo nuevo software que necesite ser instalado para uso de la empresa, debe ser solicitado por la Gerencia General a la Gerencia de TI de Icafal Gestión.
- Debe privilegiarse el uso de equipos tecnológicos de Icafal. El uso de equipos de terceros debe ser una excepción y cuando ello ocurra los propietarios de esos equipos deben contar con las licencias de las aplicaciones usadas y un antivirus. Esta obligación, al igual que otras de este documento, debe estar expresada en un anexo de contrato.

Red de Intranet e internet

- El servicio de Intranet/Internet de Icafal tiene por objeto realizar exclusivamente las funciones propias de cada cargo.
- Cada miembro de Icafal será responsable del uso de sus credenciales de usuario al ingreso de los diferentes sistemas de información que consulte en internet.
- Los perfiles de acceso deben corresponder sólo a las necesidades operacionales de los usuarios.
- Se debe evitar el uso de cuentas genéricas, innominadas o compartidas.

Sistema de correo electrónico

- El correo electrónico corporativo es para uso exclusivo de actividades relacionadas con las funciones de cada cargo, por lo tanto, la información ahí contenida es de propiedad de Icafal.
- La Gerencia de TI de Icafal Gestión, es responsable de la creación de los nuevos usuarios de correo electrónico previa solicitud de la Gerencia General respectiva, asimismo se notifican las desvinculaciones de un usuario para el bloqueo inmediato de la cuenta.
- La contraseña de acceso al correo electrónico debe ser segura para evitar accesos no autorizados y si se accede al correo a través de una red pública o no segura, no se debe marcar la opción de recordar contraseña.
- Se deben abrir sólo correos electrónicos de remitentes conocidos, sin embargo, para correos de remitentes conocidos que involucren transacciones financieras o recursos se debe realizar una doble validación de identidad (por ejemplo: una llamada telefónica).
- Se deben analizar cuidadosamente los archivos adjuntos antes de abrirlos, aunque el remitente sea conocido, los correos pueden ser suplantados.
- En los correos que provean un link, se debe dar especial atención a la revisión de la dirección web, pueden tener letras o caracteres de más o de menos, y caracteres que se parecen entre sí, para suplantar un sitio.
- El correo no deseado o spam debe ser eliminado y no emitir respuestas.
- Los usuarios tienen prohibido difundir software o contenidos que vulneren los derechos de autor.

Uso de sistemas de información y licencias de software

- Los usuarios sólo pueden instalar y utilizar software/hardware o acceder a servicios provistos por Icafal por medio de la Gerencia de TI de Icafal Gestión, para ello debe ingresar una solicitud a la Mesa de Ayuda, esta solicitud debe contar con la autorización de la Gerencia responsable del solicitante.
- La Gerencia de TI de Icafal Gestión, debe mantener identificados a los usuarios con acceso a los sistemas de información corporativos.
- La Gerencia General de cada empresa Icafal es responsable de autorizar para sus respectivos usuarios, tanto la creación de nuevas cuentas como también de informar oportunamente del bloqueo de éstas, para cada sistema de información. Además, son responsables de definir y autorizar, para sus respectivos usuarios, los accesos a los datos contenidos en sistemas de información, considerando para ello los riesgos de acceso a la información y de segregación de funciones.

- El acceso a los sistemas de información deberá contar con los privilegios o niveles de acceso suficientes para garantizar la seguridad total de la información de Icafal.
- La Gerencia de TI de Icafal Gestión debe hacer uso legal de los productos de software e información, y mantener control de las licencias de software, además está facultada para examinar cualquier equipo de Icafal con el objeto de validar este control.

Medidas de seguridad, procesamiento de información y datos

- En cuanto a la seguridad de los sistemas:
  - La Gerencia de TI de Icafal Gestión, debe identificar, producir, mantener y revisar periódicamente los Logs y registros de eventos de seguridad, excepciones y fallas de los sistemas de información de Icafal.
  - La Gerencia de TI de Icafal Gestión, debe programar revisiones independientes de seguridad de la información, para obtener un diagnóstico de los riesgos, identificando las debilidades y amenazas que permitan asumir estrategias para asegurar la información y el cumplimiento de acuerdo con la normativa vigente. La periodicidad de estas revisiones dependerá de la Alta Administración.
- En cuanto a la seguridad física de los equipos:
  - La Gerencia de TI de Icafal Gestión, será responsable de la seguridad física de los equipos en Icafal, restringirá los accesos a los servidores, redes, sistemas, aplicaciones y datos. Asimismo, será responsable de mantener personal especializado en cuestiones de seguridad.
  - Las áreas de acceso restringido se deben mantener cerradas y limitar el acceso solo al personal autorizado.
  - La Gerencia de TI de Icafal Gestión, deberá proveer protección contra desastres naturales, ataques maliciosos o accidentes a servidores, redes, sistemas, aplicaciones y datos.
- En cuanto al uso de contraseñas:
  - La administración y el uso exclusivo de contraseñas es responsabilidad de cada usuario.
  - Las claves de acceso deben ser modificadas periódicamente.
  - El uso de la contraseña es personal e intransferible, no debe ser compartida con nadie.
  - La contraseña se debe proteger, por lo tanto, no se deben escribir en papel o en un documento donde quede evidencia de ésta. Asimismo, las contraseñas no se pueden compartir por correo electrónico, redes sociales o mensaje de texto. Del mismo modo, no puede revelarse la contraseña en conversaciones y comunicaciones escritas u orales.

Proveedores de Sistemas y Tecnologías de Información

- Los Proveedores contratados para proveer insumos, equipos, servicios de TI, deben ser gestionados de acuerdo con las políticas, normas y procedimientos vigentes. Cualquier compra relacionada a sistemas y tecnologías de información, debe ser validada y evaluada técnicamente por la Gerencia de TI de Icafal Gestión, previo a su aprobación final en la respectiva empresa del grupo Icafal.
- Todas las relaciones de servicio con proveedores que den soporte a la información de Icafal, deberán documentarse a través de un contrato que asegure que los proveedores adoptan controles de seguridad de la información, este contrato debe ser visado por el área legal de Icafal.
- El proveedor debe cumplir lo establecido en la ley N°21.459 de delitos informáticos junto con proteger los datos de carácter personal, que Icafal proporcione, ingrese, mantenga y salga de sus servidores. También deberán cumplir todas las leyes que a futuro se dicten con respeto a la responsabilidad penal de la persona jurídica Ley N°20.393.

Gestión de los perfiles de los administradores de sistema.

- Los contratos de trabajo de personas con perfil “administrador”, deberán contener un compromiso de confidencialidad o no divulgación en lo que respecta al tratamiento de la información de Icafal.
- La Gerencia de TI de Icafal Gestión, será responsable de asignar los accesos privilegiados a los sistemas de información, los que deberán ser restringidos y controlados.
- Los trabajadores con perfil de “administrador” de la Gerencia de TI de Icafal Gestión, no deben realizar actividades de operación y registro en los sistemas de información, salvo exista una urgencia operacional, en la que este último deba intervenir en forma excepcional. En este caso, se debe registrar el usuario, el responsable de la Gerencia de TI que realizó la operación y el detalle de la misma y, en conjunto, se debe firmar este registro, indicando la conformidad del proceso.
- Los trabajadores con perfil “administrador” de la Gerencia de TI de Icafal Gestión, deben tener un “trabajador back-up” en el área, Ahora lo que viene no es menor, el desafío es grande y constante: "Cómo mantener el MPD actualizado, integrado al sistema de riesgos, al control interno y asegurar evidencia de su operación ante cualquier eventualidad".
- Debe existir un reemplazo que permita dar continuidad a la operación, en caso de desvinculación u ausentismo. Las actividades críticas no pueden ser realizadas solo por un responsable, siempre deben ser conocidas por más de un responsable.

Prohibiciones

Los trabajadores, ejecutivos y gerentes deberán realizar todas sus funciones y actividades ajustadas a las leyes vigentes y a nuestro Modelo de Prevención de Delitos. En este sentido, no pueden:

- Copiar y almacenar software que vulneran la ley de propiedad intelectual.
- Instalar software de sitios gratuitos en equipos de Icafal.
- Compartir los accesos a los sistemas (usuario y contraseña) entre trabajadores de Icafal, esta información es personal.
- Publicar información de Icafal en sitios de internet públicos, carpetas virtuales o cualquier sistema de publicación de documentos no oficiales de Icafal
- Acceder sin autorización a sistemas de información, o a la red de Icafal, o vulnerar los perfiles de usuario que le fueron concedidos.
- Vulnerar los derechos de privacidad de terceras personas.
- Suplantar la identidad de otro usuario en el acceso a los sistemas de información.
- Dañar los datos o realizar cualquier acción que pueda impedir el acceso legítimo a ellos. Lo anterior puede ocurrir al introducir virus por no respetar las medidas de prevención.
- Realizar cualquier conducta contraria a la ley, sobre la que se pueda tener acceso por la red.
- Distribuir material que cause daño a los sistemas, redes o servidores.
- Instalar cualquier software o hardware sin la autorización de la Gerencia de TI de Icafal gestión.
- Realizar cualquier actividad contraria a los intereses de Icafal, tal como publicar información reservada, acceder sin autorización a información.
- Utilizar la red para realizar cualquier actividad de recaudación de fondos.
- Iniciar cualquier actividad que pueda comprometer la seguridad de los servidores de Icafal.
- Autorizar o dar permiso a una persona no conectada a la red de Icafal para que la utilice ilegalmente o revelar a terceras contraseñas de acceso.
- Acceder a equipos tecnológicos, hardware y software de Icafal, desde ubicaciones remotas, sin la autorización de la Gerencia de TI de Icafal Gestión.
- Usar la información de las distintas aplicaciones de Icafal para fines personales o particulares.

Sanciones

Las sanciones son las estipuladas en los contratos de trabajo y Reglamento Interno de Orden, Higiene y Seguridad y que dicen relación con el cumplimiento de la ley 20.393 relativa a responsabilidad penal de las personas jurídicas.

El grupo de empresas Icafal ejercerá las acciones de prevención para mitigar la ocurrencia de delitos informáticos, realizará las denuncias a la justicia cuando corresponda,

responsabilizando a las personas o empresas que hubiesen permitido la materialización de estos delitos, de acuerdo con la gravedad de estos.

Glosario

Miembros de ICAFAL: Se entiende que son los trabajadores, ejecutivos, contratistas, prestadores de servicios de ICAFAL y terceros no vinculados directamente a ICAFAL, pero que presten su servicio y utilicen tecnología de información, o equipos de ICAFAL y de personas externas que utilicen la red de información de ICAFAL

Trabajador con perfil "usuario": es la persona que solicita acceso para realizar tratamiento sobre la información resguardada por el "Trabajador con perfil de administrador" de la información.

Trabajador con perfil "administrador": persona encargada de resguardar la información y administrar las definiciones establecidas por el propietario de la información.

Tercero no autorizado: es la persona natural o jurídica externa, no reconocida y no aprobada por la alta administración de ICAFAL para obtener información interna.

Equipos tecnológicos: Se entiende que son equipos tecnológicos los computadores de escritorio y equipos portátiles (Notebook, Tablet, Celulares), impresoras y escáner.

Proveedores: Se entiende que son proveedores de servicios, consultores externos y socios comerciales.

Datos informáticos: Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

Sistema informático: Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.