Proceso	Política de Seguridad de la Información	Referencia:	Revisión:
		AR.PL.01	2.0
Área	Gerencia de Ciberseguridad		

CONTROL DE CAMBIOS DOCUMENTO

REVISION	FECHA	ITEMS ALTERADOS	ELABORADORES	APROBADORES	DUEÑO DEL PROCESO
2.0	25/03/2022	Aprobación para publicación	Alejandro Welsh	Eduardo Martinez	Eduardo Martinez
2.0	22/03/2022	Revisión y actualización de contenido y formato por departamento de Controles Financieros	Alejandro Welsh	Anabella Villagra	Eduardo Martinez
2.0	22/03/2022	Revisión y actualización de contenido por departamento de Legales de Raízen Argentina	Alejandro Welsh	Jerónimo Maciel	Eduardo Martinez
2.0	14/03/2022	Revisión y adecuación de la traducción a contexto Raízen Argentina	Antulio Castañeda	Alejandro Welsh	Eduardo Martinez
2.0	07/03/2022	Traducción Política Seguridad Grupo Cosan	Antulio Castañeda	Alejandro Welsh	Eduardo Martinez
1.0	10/12/2019	Aprobación para publicación	Alejandro Welsh	Ruben Arena	Ruben Arena
0.6	6/12/2019	Actualización sección Seguridad Física. Actualización definición de clasificación Restringida y Confidencial. Almacenamiento cifrado de información Confidencial y	Luis Polo	Alejandro Welsh	Ruben Arena
0.5	28/11/2019	Actualización código de política	Alejandro Welsh	Eduardo Van Ooteghem	Ruben Arena
0.4	21/11/2019	Revisión final para publicación en Intranet	Eduardo Martinez	Valeria Agüero	Ruben Arena
0.3	15/11/2019	Revisión final para publicación en Intranet	Alejandro Welsh	Eduardo Martinez	Ruben Arena
0.3	13/11/2019	Actualización sección Comunicación Dentro y Fuera de la Empresa	Pamela Carranza	Alejandro Welsh	Ruben Arena
0.2	29/10/2019	Revisión Departamento Legales	Claudia Barrea Llovet; Daniela Delfino	Alejandro Welsh	Ruben Arena
0.1	09/10/2019	Revisión completa	Alejandro Welsh	Eduardo Martinez	Ruben Arena
0.0	09/10/2019	Traducción documento Brasil V08	Silvina Bresler	Alejandro Welsh	Ruben Arena

Proceso	Política de Seguridad de la Información	Referencia:	Revisión:
		AR.PL.01	2.0
Área	Gerencia de Ciberseguridad		

CONTENIDO

1	OBJETIVO	3
2	REFERENCIAS	3
3	ALCANCE	3
4	DEFINICIONES	3
5	DESCRIPCION	4
5.1	PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN	4
5.2	ASPECTOS GENERALES	4
5.3	CLASIFICACIÓN DE LA INFORMACIÓN	4
5.4	TIPOS DE INFORMACIÓN.....	5
5.5	NIVELES DE CONFIDENCIALIDAD.....	5
5.6	PROTECCIÓN DE DATOS PERSONALES Y DATOS SENSIBLES	5
5.7	CIBERSEGURIDAD.....	5
5.8	GESTIÓN DE IDENTIDADES Y ACCESOS.....	6
5.9	USO DE CONTRASEÑAS.....	6
5.10	USO SEGURO DE LOS RECURSOS DE TI.....	7
5.11	GESTIÓN DE ACTIVOS.....	7
5.12	GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	7
5.13	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	7
5.14	FORMACIÓN Y CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN	8
5.15	SEGURIDAD DE LA INFORMACIÓN EN LA CONTRATACIÓN DE SERVICIOS	8
5.16	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE	8
5.17	COMUNICACIÓN DENTRO Y FUERA DE LA EMPRESA	8
6	RESPONSABILIDADES	9
6.1	DIVULGACIÓN DE ESTA POLÍTICA.....	9
6.2	VIOLACIONES Y SANCIONES CORRESPONDIENTES.....	9
6.3	REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	9

Proceso	Política de Seguridad de la Información	Referencia:	Revisión:
		AR.PL.01	2.0
Área	Gerencia de Ciberseguridad		

1 OBJETIVO

Establecer pautas y principios generales de seguridad de la información y seguridad cibernética para las empresas de Raízen en un esfuerzo por garantizar que los usuarios cumplan con las normas relativas al tratamiento y protección de la información y los activos de información, así como garantizar la capacidad de Raízen para prevenir, detectar y reducir los riesgos de seguridad de la información.

2 REFERENCIAS

- Política de Segurança da Informação e Cibernética (Política 0.00.00.006 del Grupo Cosan)
- Código de Conducta de Raízen.
- Ley 25.326 – Habeas Data, sus disposiciones complementarias y demás normativa que en el futuro la reemplace, regle o complemente.
- Ley 11.723 - Régimen Legal de la Propiedad Intelectual.
- Resolución de Infraestructuras críticas (1523/2019 Jefatura de Gabinete de Ministros)
- AR.PLT.JUR.E02 - Política de Propiedad Intelectual

3 ALCANCE

Todos los empleados, directores, ejecutivos, accionistas (entre los que se incluye el Board of Directors), prestadores de servicios, colaboradores, consultores, auditores, personal temporario, proveedores, socios comerciales de diversa índole y terceros contratados por Raízen y sus compañías asociadas y/o vinculadas que tengan acceso a activos de la empresa, sus unidades de negocios, subsidiarias y/o compañías asociadas.

4 DEFINICIONES

- **Empleados y Terceros:** empleados, contratistas, subcontratistas y pasantes.
- **Proveedor:** todos los proveedores, socios y proveedores de servicios a terceros que hayan celebrado un contrato de suministro, asociación y/o servicio con empresas de Raízen, así como sus representantes, empleados y subcontratistas.
- **TI:** Área de Tecnología de la Información.
- **Registro:** Término técnico utilizado para describir el registro de transacciones que ocurren cuando se utiliza software.
- **Base de datos:** Recopilación organizada de información, o datos estructurados, generalmente almacenados electrónicamente en un sistema informático.
- **Desarrollo de software:** Es la actividad de creación de programas informáticos, realizada por un desarrollador o grupo de desarrolladores.
- **Software:** Es la parte lógica, el conjunto de instrucciones y datos procesados en servidores y ordenadores. Toda la interacción de los usuarios de computadoras se realiza a través de software.
- **Malware:** Término utilizado para referirse a una variedad de formas de software hostil o intruso.
- **Spywares:** software espía que suele instalarse en el teléfono móvil u ordenador sin el consentimiento del usuario.
- **Botnets:** Red de equipos que han sido infectados por software malicioso y pueden ser controlados remotamente para realizar ataques maliciosos.
- **VPN:** inglés, red privada virtual. Tecnología que permite el acceso remoto a la red corporativa.
- **Dispositivos:** Recursos técnicos que almacenan, procesan o transmiten la información de Raízen.
- **Activo de TI:** Cualquier Recurso o Capacidad de TI.
- **Política:** Establece las decisiones adoptadas por la Compañía respecto a la forma con que se planea llevar un asunto relacionado con sus funciones principales (por ejemplo: política de Compras, política de Calidad, etc.);
- **Norma:** Establece reglas o lineamientos generales sobre determinado asunto o función. Permite formalizar y hacer ejecutiva una política, guiando el accionar en el marco de un alcance definido;

Proceso	Política de Seguridad de la Información	Referencia:	Revisión:
		AR.PL.01	2.0
Área	Gerencia de Ciberseguridad		

- **Procedimiento:** Describe las actividades de un proceso, de un alcance determinado, en forma narrativa (y opcionalmente mediante un flujograma), detallando: dónde (ámbito de aplicación), quién (responsables de realizar acciones: sector / puesto / rol), qué (acciones a realizar), cuándo (momento, plazo de ejecución de acciones), cómo (medios a emplear para realizar las acciones)

5 DESCRIPCION

5.1 PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información cubre cuatro (4) atributos clave, que se destacan a continuación:

- **Confidencialidad:** Garantiza que la información y los activos de información sean accesibles solo por usuarios autorizados durante el período necesario;
- **Disponibilidad:** Asegura que la información y los activos de información estén disponibles para los usuarios autorizados siempre que sea necesario para los procesos comerciales o los clientes;
- **Integridad:** Asegura que la información y los activos de información estén completos e intactos y no hayan sido modificados o destruidos de manera no autorizada o accidental durante su ciclo de vida;
- **Autenticidad:** Garantiza la propiedad de la información y que provenga de la fuente anunciada y no haya sido objeto de cambios indebidos a lo largo de un proceso establecido.

5.2 ASPECTOS GENERALES

La protección de la información y los activos de información de Raízen debe ser una prioridad constante en todas las áreas de negocio y soporte, con el fin de reducir los riesgos, así como los daños y/o pérdidas que puedan comprometer la imagen y los objetivos de la Compañía.

La protección de la información y los activos de información debe aplicarse de manera compatible con su impacto en Raízen, cubriendo todos los procesos, informatizados o no.

La información bajo la responsabilidad de Raízen debe ser manejada de acuerdo con las leyes y regulaciones internas vigentes y utilizada únicamente para el propósito para el cual fue recopilada, evitando el compromiso de su confidencialidad, integridad, disponibilidad y autenticidad.

Cuando corresponda, y cuando sea posible, los procesos de Raízen garantizarán la segregación de funciones a través de la participación de más de un empleado o equipo de empleados en las actividades, a fin de evitar conflictos de intereses y reducir el riesgo de uso indebido accidental o intencional de los activos y sistemas de información.

Todos los empleados y proveedores de Raízen, según corresponda, deben ser conscientes de que el uso de los activos, sistemas y entornos de información, y sus políticas de contraseñas, pueden ser monitoreados y que los registros pueden ser utilizados para detectar violaciones de esta Política y Normas de Seguridad de la Información, sirviendo como evidencia para la aplicación de medidas disciplinarias, procedimientos administrativos y/o judiciales.

Los riesgos de seguridad de la información, así como las preguntas sobre la Política y los estándares relacionados, deben dirigirse al área de la Gerencia de Seguridad de la Información.

Las tecnologías, marcas, metodologías y cualquier información de Raízen no deben utilizarse para fines personales y deben ser tratadas de acuerdo a los lineamientos de la Política de Propiedad Intelectual.

5.3 CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información creada o recibida debe ser clasificada y protegida a lo largo de su ciclo de vida. El ciclo de vida de la información comprende su creación o recolección, manejo, almacenamiento, transporte y eliminación.

Proceso	Política de Seguridad de la Información	Referencia:	Revisión:
		AR.PL.01	2.0
Área	Gerencia de Ciberseguridad		

5.4 TIPOS DE INFORMACIÓN

- **Información estructurada:** Creada, accedida y mantenida en sistemas, como la información utilizada en SAP o sistemas heredados (sistemas más antiguos que permanecen en funcionamiento, generalmente con bases de datos o sistemas operativos obsoletos). Corresponde a la Dirección de TI en conjunto con el área de Controles Internos clasificar los niveles de confidencialidad relacionados con los perfiles de acceso, transacciones, pantallas, informes y conjuntos de información.
- **Información no estructurada:** Están fuera de los sistemas corporativos, pero se almacenan en el entorno de TI, tales como: correos electrónicos, documentos generados en editores de texto / presentaciones / hojas de cálculo, documentos impresos o manuscritos. Corresponde al Gerente de Área y al empleado responsable custodiar los informes, presentaciones, hojas de cálculo, carpetas, mensajes de correo electrónico, manuscritos y otros documentos en papel clasificándolos con el nivel de confidencialidad apropiado, de acuerdo con las recomendaciones de esta Política.

5.5 NIVELES DE CONFIDENCIALIDAD

Debajo se listan los niveles recomendados de confidencialidad (Público, Restringido, Confidencial y Secreto).

La clasificación de la información (nivel de confidencialidad) es responsabilidad del área que la generó.

- **Información pública:** puede estar disponible sin restricciones. El conocimiento de esta información por parte de cualquier individuo no afecta los objetivos de la Compañía.
- **Información Restringida:** solo puede ponerse a disposición de los empleados y proveedores de la Empresa. La información de este nivel de confidencialidad es operativa y su conocimiento por parte de terceros no afecta los objetivos comerciales.
- **Información Confidencial:** Información que solo debe acceder personal autorizado. El conocimiento de esta información por personas no autorizadas podría ocasionar perjuicios financieros, operativos o de imagen, e incluso redundar en sanciones administrativas, civiles y penales para Raízen o sus clientes. El gerente responsable debe indicar explícitamente qué roles pueden tener acceso.
- **Información Secreta:** información cuyo uso y acceso está restringido a un grupo específico de empleados nominalmente designados, y no puede ser divulgada a personas no autorizadas, en su totalidad o en parte, en ningún formato. Comprende temas, documentos, imágenes o cualquier material estratégico, altamente sensible y crítico. La indisponibilidad, divulgación o alteración no autorizadas causa graves daños a los objetivos comerciales.

5.6 PROTECCIÓN DE DATOS PERSONALES Y DATOS SENSIBLES

Raízen se toma en serio la protección de datos personales y datos sensibles y las medidas de seguridad establecidas en esta Política son esenciales para garantizar el cumplimiento de la legislación sobre protección de datos personales.

5.7 CIBERSEGURIDAD

Raízen aplica controles de seguridad de la información para garantizar su ciberseguridad, con el objetivo de garantizar la disponibilidad, confidencialidad, integridad y autenticidad de la información y los activos de información en sus entornos tecnológicos.

Con el fin de contribuir en la implementación de los lineamientos establecidos en esta política y los controles, procesos y procedimientos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad de Raízen, se adoptan por defecto las mejores prácticas disponibles en el mercado:

Proceso	Política de Seguridad de la Información	Referencia:	Revisión:
		AR.PL.01	2.0
Área	Gerencia de Ciberseguridad		

- Medidas de autenticación capaces de individualizar a los usuarios que acceden a los activos, sistemas y entornos de información de Raízen;
- Uso de cifrado, enmascaramiento y ofuscación, cuando corresponda, para el almacenamiento de información relevante y sensible, incluidos datos personales, en activos de información, sistemas y entornos de Raízen y proveedores;
- Soluciones de prevención y detección de intrusiones y acceso no autorizado a los activos, sistemas y entornos de información de Raízen;
- Pruebas y escaneos periódicos para la detección de fallas y vulnerabilidades en los procedimientos, controles, sistemas y entornos de Raízen;
- Soluciones de protección contra software malicioso (*malware, spyware, troyanos, virus, botnets*, etc.) que puedan afectar a activos, sistemas y entornos de información del Grupo;
- Sistemas de monitoreo de registros de actividades (logs), realizadas por el Centro de Defensa Cibernética;
- Control de acceso por parte de los usuarios que hacen uso de los sistemas y entornos de Raízen;
- Segregación y segmentación de los diferentes entornos de red proporcionados a sus empleados, proveedores y clientes por Raízen o proveedores contratados por éste, cuando corresponda y validados por el área de Seguridad de la Información;
- Mantenimiento de copias de seguridad de la información.

5.8 GESTIÓN DE IDENTIDADES Y ACCESOS

Los procesos de concesión, alteración y exclusión del acceso a los activos de información, sistemas de información y/o entornos de Raízen son llevados a cabo por el área competente previa aprobación formal del gestor del solicitante y del respectivo titular del sistema y/o perfil, siempre que sea necesario para el desempeño de las actividades.

El acceso privilegiado que implica responsabilidades adicionales para el usuario se otorga con criterios más estrictos, a través del cumplimiento de reglas específicas.

Se deben mantener las siguientes reglas para administrar los derechos de acceso del usuario:

- **Registro:** aprobación y/o concesión de derechos de acceso a los usuarios;
- **Gestión de privilegios:** Se deben determinar jerarquías claras para cada sistema y cada jerarquía debe ser aprobada formalmente;
- **Gestión de usuarios:** Como se mencionó anteriormente, cada sistema debe tener procedimientos claros para la aprobación y el método de concesión de acceso a este sistema con registros de auditoría;
Los derechos de acceso de los usuarios están sujetos a revisión periódica.

5.9 USO DE CONTRASEÑAS

La contraseña es responsabilidad de cada persona, quien debe considerar las siguientes reglas:

- La contraseña es personal e intransferible;
- Se prohíbe el uso de contraseñas corporativas en computadoras y dispositivos móviles personales o de terceros;
- Se debe evitar el almacenamiento de contraseñas en los navegadores web;
- Las contraseñas de acceso a los sistemas corporativos no deben anotarse ni almacenarse en medios físicos y digitales (por ejemplo, correo electrónico, hojas de cálculo, cuadernos, archivos de red, etc.);
- Se deben usar diferentes contraseñas para diferentes servicios. Las contraseñas privadas de uso privado deben ser diferentes de las contraseñas corporativas;
- Si el empleado sospecha que la contraseña ha sido descubierta, debe solicitar un cambio y/o bloqueo inmediato;

Proceso	Política de Seguridad de la Información	Referencia:	Revisión:
		AR.PL.01	2.0
Área	Gerencia de Ciberseguridad		

- Está prohibido utilizar el nombre de cualquier empresa, productos o servicios de Raízen, y números secuenciales en la formación de la contraseña.

5.10 USO SEGURO DE LOS RECURSOS DE TI

- Los recursos de TI corporativos deben utilizarse con fines profesionales.
- Los sistemas deben tener control de acceso para garantizar el uso solo a usuarios o procesos autorizados.
- La persona responsable de autorizar o confirmar la autorización deberá estar claramente definida y registrada.
- Las estaciones de trabajo, los equipos de escritorio y los equipos portátiles deben estar protegidos contra daños o pérdidas, así como contra el acceso, el uso o la exposición indebidos.
- Siempre que sea posible, dé preferencia al uso de la impresora con función de control de acceso, es decir, necesita identificación para imprimir el documento.
- Los dispositivos móviles de los proveedores solo se pueden utilizar en la red corporativa después del análisis del área de Tecnologías de la Información. Estos dispositivos deben tener soluciones de seguridad instaladas y actualizadas (ej.: endpoint security).
- No se permite almacenar información corporativa en medios extraíbles y/o servicios personales de almacenamiento en la nube.
- La red corporativa debe utilizarse exclusivamente para los fines para los que se permite el acceso. Se prohíbe el uso de la red corporativa para almacenar archivos no relacionados con actividades profesionales.
- El correo electrónico e Internet solo deben utilizarse para actividades corporativas de manera responsable, efectiva y legal.
- En ningún caso se tolerará el acceso a sitios web con contenidos ilícitos o que amenacen la dignidad humana, como terrorismo, pedofilia, xenofobia, sexual, racista, discriminatorio, etc.
- El acceso remoto a la red corporativa (a través de VPN) solo se permite mediante el uso de un doble factor de autenticación.

5.11 GESTIÓN DE ACTIVOS

El inventario de activos debe mantenerse y actualizarse constantemente cubriendo activos de información clave como: sistemas, aplicaciones, bases de datos y servidores.

El hardware debe comprarse solo a proveedores aprobados y mantenerse teniendo en cuenta las siguientes pautas:

- Solo se deben aplicar configuraciones de software aprobadas al nuevo hardware;
- Los usuarios finales deben cuidar adecuadamente cualquier hardware que se les haya entregado;
- El hardware perdido y/o robado debe ser reportado inmediatamente;
- El hardware al final de su vida útil debe desecharse de forma segura.

5.12 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Raízen debe establecer un proceso estructurado de monitoreo, análisis e identificación de vulnerabilidades, amenazas e impactos en los activos de información, de modo que se identifiquen los controles apropiados y se pruebe periódicamente la efectividad.

5.13 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Raízen adopta procedimientos, requisitos y controles específicos para la prevención y respuesta a incidentes ocurridos.

Los procedimientos, controles y requisitos para los proveedores deben estar alineados con los niveles de complejidad, amplitud y precisión de Raízen.

Proceso	Política de Seguridad de la Información	Referencia:	Revisión:
		AR.PL.01	2.0
Área	Gerencia de Ciberseguridad		

5.14 FORMACIÓN Y CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Como parte de su compromiso, Raízen adopta acciones e iniciativas para promover la formación, concientización y evaluación de los empleados en materia de seguridad de la información, reforzando los lineamientos declarados en esta política.

5.15 SEGURIDAD DE LA INFORMACIÓN EN LA CONTRATACIÓN DE SERVICIOS

Los procesos y controles necesarios para reducir los riesgos asociados a las iniciativas de tercerización, incluidos los acuerdos de computación en la nube, deben formar parte de los acuerdos comerciales entre los proveedores y las empresas de Raízen.

Las empresas de Raízen se reservan el derecho de evaluar si el proveedor cumple con los requisitos de seguridad de la información basados en estándares y buenas prácticas de mercado.

Los contratos con terceros garantizarán que el equipo o subcontratistas de la organización externa cumplan con los documentos regulatorios de seguridad de la información de Raízen.

5.16 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE

La política de adquisición de software debe respetar todos los derechos de autor de software informático y los términos de todas las licencias de software de las que las empresas de Raízen son parte.

Las empresas de Raízen deben administrar sus activos de software y garantizar solo el uso de software legal en sus estaciones de trabajo y servidores.

Las copias de software de terceros, con derechos de autor del desarrollador del software, a menos que estén expresamente autorizadas, están prohibidas.

Los sistemas y aplicaciones desarrollados internamente o por especificación de las empresas de Raízen deben cumplir con el código de desarrollo seguro y garantizar:

- La evaluación del impacto en la privacidad debe completarse para los cambios importantes de software;
- Los requisitos de seguridad del software deben documentarse como parte del proceso de desarrollo;
- Los cambios de software deben estar sujetos a procedimientos de control;
- Solo los usuarios autorizados pueden implementar cambios de software;
- Garantía del concepto de segregación de funciones tanto para las actividades empresariales como para la administración de TI;
- Autenticación garantizada y configuración de seguridad para contraseñas de acceso;
- Segregación de entornos para el desarrollo, prueba y producción;
- La contratación de servicios de mantenimiento y desarrollo de aplicaciones debe contener requisitos de seguridad (por ejemplo, utilizando una plantilla de RFP o un documento específico del contrato);
- Garantía de evaluación de seguridad en código antes de promoción para entornos productivos.

5.17 COMUNICACIÓN DENTRO Y FUERA DE LA EMPRESA

Sólo los empleados designados como voceros o interlocutores válidos con los medios de comunicación están habilitados a escribir o realizar publicaciones y declaraciones en nombre de la empresa en sitios web, redes sociales, foros de discusión abiertos y públicos o cualquier otro medio.

- Los asuntos de Raízen deberán tratarse con precaución, tanto dentro como fuera del ámbito de su/sus establecimientos, en espacios públicos, ante la presencia de visitantes, en conversaciones telefónicas, en charlas con compañeros y durante el contacto con proveedores.

Proceso	Política de Seguridad de la Información	Referencia:	Revisión:
		AR.PL.01	2.0
Área	Gerencia de Ciberseguridad		

- En ningún caso se discutirá información confidencial o secreta en áreas abiertas o espacios compartidos.
- En caso de dudas, contactarse con la Dirección de Asuntos Externos y Relaciones Gubernamentales.

6 RESPONSABILIDADES

Es responsabilidad de todos los Empleados y Terceros garantizar el cumplimiento de esta Política.

6.1 DIVULGACIÓN DE ESTA POLÍTICA

Esta política se divulga a todos los Empleados y Terceros de Raízen en los canales de comunicación de la empresa (por ejemplo, Intranet, Biblioteca de conocimiento del lugar de trabajo, POC, etc.).

6.2 VIOLACIONES Y SANCIONES CORRESPONDIENTES

En caso de incumplimiento y/o violación de la presente política, Raízen podrá aplicar sanciones - incluida la desvinculación del personal - como así también reclamar los daños y perjuicios que pudieren derivarse de tal incumplimiento o violación y formular las denuncias correspondientes.

El infractor podrá ser notificado, y la transgresión deberá ser comunicada inmediatamente al gerente del sector y al Gerente de Seguridad de la Información, quien a su vez procederá con las comunicaciones a la Dirección y/o Presidencia según corresponda y dará curso al inicio de un incidente de seguridad reportándolo al equipo de Ciberseguridad a fin de que se adopten las acciones correspondientes y las medidas adecuadas para mitigar el riesgo en forma rápida y eficiente.

Los terceros infractores, si los hubiere, estarán sujetos a sanciones comerciales contractuales razonables, incluida la terminación contractual inmediata, con la aplicación de las sanciones derivadas de la terminación, sin perjuicio de la acción de indemnización y otras medidas legales aplicables.

Los indicios de incumplimiento o dudas sobre el cumplimiento de esta Política deberán ser comunicados al responsable inmediato del empleado, departamento de recursos humanos, auditoría interna, Compliance Officer, gerente de Ciberseguridad o a través del canal de Ética llamando al **0800-345-4327**

Raízen no tolera ninguna represalia contra ninguna persona, interna o externamente, que informe de buena fe una violación o sospecha de violación de esta Política o su Código de Conducta, y se garantiza la confidencialidad sobre la identidad de cualquier persona que informe cualquier violación. La práctica de represalias está sujeta a medidas disciplinarias que pueden resultar incluso en la desvinculación del empleado de Raízen o la terminación de un contrato, según sea el caso.

6.3 REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política debe revisarse una vez al año, y cualquier cambio debe ser aprobado por el director de TI.