NOTA SOBRE LA CONFIDENCIALIDAD Y SEGURIDAD

Reale Chile Seguros Generales S.A. garantiza gestionar las comunicaciones recibidas aplicando la máxima confidencialidad en todas las etapas; también garantiza la confidencialidad sobre la identidad de la persona que realiza la denuncia, excluyendo el riesgo de represalias y/o discriminación que pudieran producirse por efecto de la misma.

La identidad del autor de la denuncia está protegida por la Compañía, excepto en los casos en que:

- la denuncia sea realizada de mala fe, con el fin de dañar o perjudicar a la persona denunciada, y por esto se pueda concretar el delito de calumnia o injuria en virtud de la ley;
- en la denuncia se ponga de manifiesto hechos y/o circunstancias que, a pesar de ser ajenos al ámbito de la empresa, hagan procedente y/o deban ser denunciados ante las Autoridades Judiciales;
- en cualquier otra hipótesis en la cual la identificación de la identidad de la persona que realiza la denuncia sea esencial para el cumplimiento de obligaciones y/o deberes legales.

Sin perjuicio de las excepciones mencionadas anteriormente, la identidad de la persona que realiza la denuncia no puede ser revelada sin su consentimiento expreso y todos los que participan en la gestión de la misma tienen que cumplir con la obligación de confidencialidad.

Reale Chile Seguros no permite ninguna forma de represalia o discriminación contra la persona que denuncia, determinadas por motivos directa o indirectamente relacionados con la denuncia; asimismo la Compañía prohíbe cualquier forma de represalia o discriminación contra quienes colaboran en las actividades de investigación y comprobación de los hechos denunciados.

La constatación de las situaciones antes detalladas será sancionada de acuerdo con el Reglamento interno de orden, higiene y seguridad.

La observancia de las directrices y protecciones previstas por el sistema de gestión de las denuncias y la aplicación de eventuales sanciones, en caso de incumplimiento, se extienden también a las relaciones entre la Compañía y los terceros, de conformidad a lo previsto en los respectivos contratos.

Las denuncias también pueden hacerse de forma anónima.

En este caso, la plataforma Whistleblowing permite al denunciante interactuar con la función que gestiona las denuncias, incluso sin tener que revelar su identidad, con el fin de permitir la recopilación de informaciones adicionales, cuando sea útil para la gestión del caso.

Infraestructura y seguridad

El software de gestión de denuncias de irregularidades, en línea con las mejores prácticas en materia de whistleblowing, garantiza niveles muy altos de seguridad tanto para el demandante como para la infraestructura.

Seguridad del demandante y de las denuncias

- Cifrado asimétrico de los contenidos de texto y archivos adjuntos: el cifrado no requiere acciones específicas por parte de los usuarios. El sistema criptográfico garantiza que los mensajes y los archivos adjuntos relativos puedan ser leídos exclusivamente por el remitente y el destinatario mediante la combinación de la "clave criptográfica pública y privada".
- Posibilidad de acceder mediante una smart card.
- Acceso regulado de acuerdo con las medidas de seguridad más estrictas en este ámbito: el acceso a las denuncias se permite exclusivamente a través de credenciales (para usuarios registrados) o introduciendo los códigos asociados con la denuncia (para usuarios no registrados).

Seguridad de la aplicación

Separación de la denuncia de la identidad del demandante, según lo previsto por los más altos estándares en materia de whistleblowing. La privacidad del demandante está garantizada por el software, que proporciona una separación completa entre el proceso de registro y el proceso de denuncia, para una correcta separación de los datos; de hecho, en la denuncia enviada, no se indica el nombre del demandante. Permanece la posibilidad del Responsable de la gestión de denuncias de activar el procedimiento mediante el cual el sistema asocia la identidad del demandante con la denuncia, motivando la solicitud, cuando se considere necesario y en los casos previstos por la Política de la Compañía en este asunto (capítulo 9 del Procedimiento de gestión denuncias). Esta acción se notifica automáticamente al demandante y se registra en el sistema.

Servidores específicos DigitalPA: máxima protección de los datos y de los niveles de seguridad, garantizados tanto por la certificación DigitalPA ISO 27001/2014 como por la infraestructura del servidor farm con certificación ISO 27001/2014.

Firewall hardware y software integrado: cada plataforma posee un firewall integrado con reglas muy estrictas, que limitan el acceso y las acciones a las tareas exclusivas dedicadas al software; los firewall se integran y potencian aún más la seguridad.

Certificado SSL: se puede acceder al software de whistleblowing exclusivamente a través del acceso HTTPS (Secure Sockets Layer).

IP y certificado SSL específicos para cada cliente.

Validaciones input usuario: la plataforma se basa en un enfoque de validación input del usuario. Mediante reglas extremadamente estrictas, el usuario se verifica tanto a nivel client como a nivel servidor.

Prevención CSRF: todas las solicitudes gestionadas por la plataforma están protegidas por token CSRF.