

## POLÍTICA DE CIBERSEGURIDAD

La sociedad INGENIERÍA Y COMERCIALIZADORA TRENT LIMITADA, en adelante TRENT, por medio de su administración, en el marco de su competencia general e indelegable de determinar las políticas y estrategias generales de la empresa, y previa revisión y propuesta por parte de los asesores pertinentes, ha aprobado la presente Política de Cumplimiento Normativo en materia de Ciberseguridad (en adelante, la “**Política**”).

La presente *Política* forma parte del “Modelo de Cumplimiento Normativo, de Prevención Penal y de Defensa de la Competencia de TRENT” (en adelante, el “**Modelo de Cumplimiento Normativo**”). El “Código Ético y de Conducta de la empresa” (en adelante, el “**Código Ético y de Conducta**”) es la norma interna que constituye la base de este Modelo de Cumplimiento Normativo. Esta *Política* está alineada con los valores de integridad y transparencia promulgados en dicho Código Ético y de Conducta y constituye un punto de desarrollo de una de sus pautas de comportamiento con el Mercado (la relativa a la Ciberseguridad) y de cada una de sus conductas expresamente prohibidas en la materia.

En consecuencia, esta *Política* ha de ser leída e interpretada conjuntamente con el Código Ético y de Conducta y con las restantes políticas que forman parte del modelo de cumplimiento corporativo y que son igualmente expresión del firme compromiso de TRENT con el cumplimiento de las leyes, en este caso en el ámbito de la regulación de Ciberseguridad.

### 1. DEFINICIÓN Y FINALIDAD

La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Las organizaciones tienen la responsabilidad de proteger los datos para mantener la confianza del cliente y cumplir con la normativa.

En ese marco, la finalidad de esta *Política* es la de situar a la ciberseguridad como uno de los factores clave en la realización de las actividades de la empresa que aseguren la salvaguarda de la confidencialidad, la integridad, la disponibilidad, la trazabilidad, la autenticidad y privacidad de la información y de los activos tecnológicos que la soportan, manteniendo un equilibrio entre los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad.

Asimismo, estos principios deberán estar alineados con los requerimientos normativos y regulatorios vigentes y prevenir los impactos relativos, entre otros, a:

- a) La imagen y reputación de TRENT.
- b) Interrupción de los procesos críticos que soportan el negocio.
- c) Uso indebido de los activos de información.
- d) Pérdida o filtración de datos.

Forma parte de la estrategia de TRENT la implantación y el desarrollo de un Sistema de Gestión de Ciberseguridad basado en normativas y mejores prácticas nacionales e internacionales y sustentado en las capacidades de identificación, protección, detección, respuesta y recuperación de los sistemas de información, aportando para ello la Alta Dirección, los recursos necesarios para su consecución.

TRENT entiende que esta finalidad debe nacer desde el interior del equipo humano que integra la empresa, como señal de identidad, por lo que anima a todas estas personas a incorporarlo en su forma de trabajo, y hacerlo extensivo a todas sus partes interesadas.

## 2. ÁMBITO DE APLICACIÓN

- Todas las entidades pertenecientes a TRENT, atendiendo a sus características propias. A efectos del presente documento, TRENT se considera integrado por todas las sociedades filiales o participadas mayoritariamente respecto de las que, de forma directa o indirecta, se ejerza un control efectivo, independientemente de su localización geográfica, así como por todas las eventuales fundaciones que en el futuro pudieran pertenecerle. Por lo tanto, en todas las referencias que esta *Política* haga a TRENT, se entenderán incluidas todas las sociedades detalladas anteriormente y también las Fundaciones.
- Los miembros de los órganos de administración, directivos y empleados de todas las entidades de TRENT detalladas anteriormente, independientemente del territorio en que se encuentren.
- Aquellos terceros, personas físicas y/o jurídicas, relacionados con TRENT, en aquellos aspectos de esta *Política* que les resulten de aplicación y de los que se espera que desarrollen comportamientos alineados con la misma.
- En el caso de las actividades que TRENT pudiera realizar en el futuro fuera de Chile, esta *Política* habrá de adaptarse a la legislación local más restrictiva que, en su caso, resulte de aplicación.

## 3. PRINCIPIOS GENERALES DE ESTA POLÍTICA

Los siguientes postulados constituyen los principios generales que deben guiar todas las actividades relacionadas a la Ciberseguridad:

- I. Proteger la información soportada sobre los sistemas de información de la empresa.
- II. Garantizar que los activos de TRENT posean un nivel de ciberseguridad adecuados y aplicar los estándares más avanzados en aquellos que soporten la operación de infraestructuras críticas.
- III. Dotar de procedimientos y herramientas que permitan adaptarse con agilidad a las condiciones cambiantes del entorno tecnológico y a las nuevas amenazas que surjan.

- IV. Sensibilizar a todos los trabajadores, proveedores y otras partes interesadas acerca de los riesgos de ciberseguridad, promoviendo una cultura de la ciberseguridad mediante acciones de formación y concienciación. Asimismo, se garantizará que el personal implicado en las tareas relativas a la ciberseguridad dispondrá de los conocimientos, experiencia y capacidades tecnológicas necesarias para cumplir con los objetivos de ciberseguridad de TRENT.
- V. Requerir la existencia de mecanismos de ciberseguridad adecuados para los sistemas de información de terceros que presten servicios a TRENT y sus relacionadas y/o quienes la componen.
- VI. Tener en cuenta criterios de eficiencia y sostenibilidad en la implementación de las medidas de ciberseguridad aplicables.
- VII. Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las amenazas de ciberterrorismo y ciberdelincuencia, para evitar que éstas lleguen a impactar a TRENT, o en caso de que lo hagan, se puedan minimizar sus efectos sobre el negocio.
- VIII. Colaborar con los organismos y agencias gubernamentales relevantes para contribuir a la mejora de la ciberseguridad en el ámbito nacional e internacional.
- IX. Actuar de acuerdo con la legislación vigente, el Código Ético y demás normativa interna de TRENT.
- X. Mantener y promover desde la Alta Dirección de la organización los principios de la presente política.

#### **4. CANAL DE DENUNCIAS**

Toda actividad realizada por funcionarios o terceros que sea susceptible de generar riesgo para la empresa o sus sistemas, que tenga directa o indirecta relación con los delitos cibernéticos o que atenten contra la ciberseguridad, podrán ser denunciados a través de los canales habituales de la empresa, o bien a través de su canal privado de denuncias: [canaldenuncias@TRENT.cl](mailto:canaldenuncias@TRENT.cl).