**ANEXO VI CÓDIGO DE ÉTICA PARA LOS CLIENTES DE CALISOFT SOBRE EL ACCESO A INTERNET.**

**Código de Ética para el uso de las TICs**

El presente Código tiene como objetivo asegurar las medidas que permitan el uso y explotación de las TICs en correspondencia con los principios éticos y jurídicos establecidos en el país.

La Red Tecnológica del Centro Nacional de Calidad de Software se estableció con el objetivo de garantizar y fomentar el intercambio de información entre las diferentes áreas en todas las esferas: científica, educacional, administrativa y social.

Es en función de la consecución de estos objetivos, y con el ánimo de garantizar el uso apropiado de las mencionadas tecnologías, que se establece el presente Código de Ética de estricto cumplimiento para todos los clientes que utilicen la Red de **CALISOFT**:

* El cliente debe velar y garantizar la seguridad de las TICs y los servicios en la red asignados. Utilizarlas sólo en funciones propias de trabajo y/o capacitación. Que las mismas no sean utilizadas por terceras personas y protegerlas de acceso no autorizados, en caso de detectarse un incidente asociado a estos identificadores y direcciones IP, el usuario asume la responsabilidad de las consecuencias derivadas de sus acciones.
* El cliente responderá por la cuenta asignada y darle un uso adecuado, no emplear los recursos asignados con fines lucrativos o ilícitos que se contrapongan con las normas éticas y morales de nuestra sociedad o para hacer manifestaciones en contra de los principios de nuestro País.
* No instalar, ni propagar ningún virus, malware o ransonware, notificar inmediatamente cuando detecte que sus dispositivos han sido infectados y es responsable de no conectarlos a las redes de transmisión de datos vía LAN o GPRS.
* Instalar solo software autorizados por nuestro centro.
* No distribuir información no acorde con los principios revolucionarios a través de la Red.
* No acceder a sitios de minería de criptomonedas, pornografía, juegos en línea, o derivados de los mismos, ni a sitios propios de los servicios especiales de inteligencia militares u otros similares de gobiernos extranjeros.
* No enviar o divulgar por ningún medio documentación de proyectos o código fuente perteneciente a nuestra entidad.
* Cumplir con las medidas de seguridad informática al descargar archivos desde las redes de datos, teniendo especial cuidado con los archivos ejecutables.
* No realizar exploraciones de la red o utilizar tipo de técnica que descubra vulnerabilidades, datos o acciones que afecten a la entidad y al cliente.
* No instalar software para registrar la actividad de otras personas en computadoras ajenas o en la propia, ni utilizar o distribuir programas para ello.
* No utilizar programas o técnicas para escuchar el contenido del tráfico de la red con el objetivo de recuperar contraseñas o vía de acceso a recursos de red.
* No instalar Apps ni software en las computadoras que violenten las medidas de seguridad y el acceso a los servicios asignados. Ejemplo:
* **VPN** que generen cualquier tráfico anómalo en la red.
* **Snifer** que escuchen el contenido del tráfico de la red con el objetivo de recuperar contraseñas o vía de acceso a recursos de red.
* No instalar o usar proxy, accesos remotos u otro tipo de programas para darle acceso a terceros a la red.
* No eliminar o modificar la información contenida en los sistemas, ni distribuir los sistemas con los cuales se trabaja en la entidad sin previa autorización o de forma intencional.
* Mantener activo y actualizar periódicamente el antivirus y los navegadores.
* No acceder a los redes sociales o sitios de interés personal con la cuenta institucional.
* No utilizar las redes y servicios de redes de la entidad para la publicación de contenido ofensivo, incluyendo comentarios acerca de la raza, discapacidades, orientación sexual, pornografía, creencias o prácticas religiosas, contrarrevolución, terrorismo, en perfiles personales en las redes sociales autorizadas.
* No utilizar direcciones de proxys anónimos, al menos que sea necesario y autorizado por el responsable de Seguridad Informática. En caso de ser autorizado, será con la fecha y hora determinada.

El uso no autorizado de las tecnologías de la información y sus servicios asociados constituye una violación de los derechos de la entidad por lo que**, en tales circunstancias, EL PRESTADOR** se reserva la facultad de suspender el uso de internet a los clientes que incumplan con las Políticas de Seguridad Informáticas establecidas para el uso de los servicios en la red de datos y móvil, teniendo en cuenta lo establecido en el Decreto Ley 370/18, Decreto 360/19 y Resoluciones 128/19 y 129/19.

**En casos de incumplimiento del presente Código de Ética,** EL CLIENTE **se obliga a abonar una sanción pecuniaria ascendente al 10 % del valor del contrato, disponiendo para ello de 15 días hábiles posterior a la recepción de la factura, la cual será confeccionada de manera independiente por** EL PRESTADOR**.**

Hago constar mediante mi firma, que conozco las normas para el trabajo y uso de los servicios telemáticos asignados y me comprometo a su estricto cumplimiento.

**Y PARA QUE ASÍ CONSTE**,se suscriben 2 (dos) ejemplares, todos a un mismo tenor y efecto, en La Habana, a los \_\_\_\_\_\_\_ días del mes de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ de 20\_\_\_\_.

|  |  |  |
| --- | --- | --- |
| **POR EL PRESTADOR**  **FIRMA Y CUÑO** |  | **POR EL CLIENTE**  **FIRMA Y CUÑO** |