	POLITICA DE SEGURIDAD DE LA INFORMACION		
	Código: PO-AF-TIS-ASEC		
	Revisión: 1	Fecha revisión: 10/Mar/16	Página 1 de 4

Inteligencia Laboral INARI, S.A. de C.V. a quien en lo sucesivo se le denominara la **Empresa**, proporciona a **[Nombre del empleado]** a quien en lo sucesivo se le denominara el **Empleado** acceso a: documentación diversa, equipo de computación, correo electrónico e Internet, sistemas y funciones de la Red local, con el propósito de facilitar el desempeño de su trabajo.

Por lo que la **Empresa** está en su derecho de imponer restricciones en cuanto al uso del equipo, correo electrónico corporativo, recursos y materiales que el **Empleado** obtiene.

Por lo tanto, con el propósito de conservar la confidencialidad y buen uso de la información, la **Empresa**:

- a) Podrá disponer, reubicar, depurar, auditar o formatear en cualquier momento los equipos de su propiedad, siempre que lo considere pertinente, sin el consentimiento del Empleado.
- b) Se reserva el derecho de proteger su reputación y su inversión en software para computadoras, al aplicar controles internos, los cuales pueden incluir evaluaciones frecuentes y periódicas del uso de software, auditorías anunciadas y no anunciadas a las computadoras de la compañía.

1. USO DE DOCUMENTACION DIVERSA


El **Empleado** tiene prohibido, sin el consentimiento expreso y por escrito de la **Empresa**:

- 1.1 Extraer información por cualquier medio magnético, electrónico o impreso.
- 1.2 Usar para fines distintos al laboral, la documentación que se pone a su disposición o ha creado.

2. USO DE COMPUTADORAS

El **Empleado** tiene prohibido, sin el consentimiento expreso y por escrito de la **Empresa**:

- 2.1 Duplicar software o documentación con derechos de autor.
- 2.2 Crear copias de los programas o de su documentación propiedad de la **Empresa**.
- 2.3 Usar, instalar, cargar o descargar software obtenido de cualquier otra fuente incluyendo Internet.
- 2.4 Cambiar la configuración original de los equipos, incluyendo tapiz y protector de pantalla.
- 2.5 Usar para contraseñas, métodos de encriptación (seguridad) no autorizados y/o desconocidos por la **Empresa**.
- 2.6 Buscar información de manera intencional, obtener copias o modificar archivos, u otra información o clave ("password") que pertenezca a otros usuarios.
- 2.7 Usar para fines distintos al laboral, el equipo y/o servicio computacional que la **Empresa** pone a su disposición.
- 2.8 Usar el equipo y/o servicios para afectar a terceros por cualquier medio (red interna, Internet u otra tecnología).

	POLITICA DE SEGURIDAD DE LA INFORMACION		
	Código: PO-AF-TIS-ASEC		
	Revisión: 1	Fecha revisión: 10/Mar/16	Página 2 de 4

- 2.9 Guardar información personal en cualquier equipo propiedad de la empresa o que pertenezca a la infraestructura de la red.
- 2.10 Colocar información personal en cualquier medio magnético o electrónico propiedad de la **Empresa**, ya que al no ser una necesidad laboral, la **Empresa** no se hará responsable de la pérdida o mal uso que pueda hacerse de ésta.
- 2.11 Solamente el área de Sistemas podrá asignar, instalar, configurar y mantener el equipo de cómputo que usará el personal del grupo, cualquier otra persona queda excluida incurriendo en una falta administrativa y de seguridad e integridad del equipo en caso de daño o extravío.
- 2.12 La **Empresa** no se hace responsable de equipos o dispositivos propiedad del personal o de terceros, así como el uso de la infraestructura de red para estos equipos quedará limitado y bajo reservas del área de Sistemas y bajo disposición de la Dirección General; en tales casos deberá llenar formato de Acuse de Ingreso de Equipo (FO-AF-SIC-AIEE-03).
- 2.13 Cualquier ingreso de equipo que no sea propiedad de la empresa, deberá ser notificado al área de Sistemas y esta misma se reserva el derecho de admisión del equipo. Cualquier equipo que no sea notificado, al área de sistemas tiene el derecho de resguardar el equipo hasta que lo considere necesario.

3. USO DE CORREO ELECTRONICO


El **Empleado** tiene prohibido, sin el consentimiento expreso y por escrito de la **Empresa**:

- 3.1 Usar el servicio de correo electrónico para propósito no laboral, fraudulento, comercial o publicitario, que atenten contra la legalidad, la propagación de mensajes destructivos, mensajes obscenos y que contengan opiniones que atenten contra el honor de terceros.
- 3.2 Difundir y participar en la propagación de "cadenas" de mensajes (Forwards) irrelevantes o propaganda comercial (spam).
- 3.3 Intentar o apoderarse de claves de acceso de otros usuarios, acceder y/o modificar mensajes de otro usuario.
- 3.4 Permitir que otro usuario use la cuenta de correo asignada para fines distintos al laboral, así como divulgar la clave de acceso (contraseña).
- 3.5 Perturbar el trabajo de los demás enviando mensajes que interfieran en el desempeño laboral.

4. USO DE INTERNET

El **Empleado** tiene prohibido, sin el consentimiento expreso y por escrito de la **Empresa**:

- 4.1 Usar las computadoras y el Internet para actividades de negocios privados o uso personal.
- 4.2 Gestionar directa o indirectamente conexiones que formen "puertas traseras" a otras organizaciones, grupos de la comunidad, etc., que permitan acceso a la red de la Empresa sin autorización.
- 4.3 Usar el uso de aplicaciones proxy o de terceros a fin de vulnerar los filtros de seguridad.

 INTELEGENCIA LABORAL	POLITICA DE SEGURIDAD DE LA INFORMACION		
	Código: PO-AF-TIS-ASEC		
	Revisión: 1	Fecha revisión: 10/Mar/16	Página 3 de 4

- 4.4 Usar el servicio de Internet para conseguir materiales profanos u obscenos (pornografía de cualquier clase), que aboguen por actos ilegales o que aboguen por violencia o discriminación hacia otras personas.
- 4.5 Descargar de Internet archivos de música o video en cualquier formato, o conectarse a estaciones de radio, televisión o video on-line.
- 4.6 Descargar o usar cualquier programa de mensajería instantánea (chat).
- 4.7 Gestionar o conectarse a videoconferencias sin autorización expresa de la Empresa.
- 4.8 Suscribirse sin autorización a boletines electrónicos, foros o portales utilizando la cuenta corporativa.
- 4.9 Compartir o divulgar contraseñas para acceso a la red o elementos compartidos en la red de la empresa.
- 4.10 La **Empresa** se reserva el derecho para permitir el acceso a la red Ethernet o Wireless a cualquier persona, mediante el área de Sistemas.
- 4.11 En equipos de terceros, quedo prohibido realizar cualquier tipo de actualización de hardware o software usando la infraestructura de red de la **Empresa**.

5. CONFIDENCIALIDAD DE LA INFORMACION

La **Empresa** se obliga y compromete a no hacer mal uso, ni divulgar de ninguna manera la información personal de los usuarios o del **Empleado**, subsistiendo este deber de secreto, aun después de que finalice la relación de la **Empresa**.


El **Empleado** se compromete a cumplir todas las disposiciones relativas a la política de la **Empresa** en materia de uso y manejo de información, y a no divulgar de ninguna manera o por ningún medio la información que reciba o genere a lo largo de su relación de trabajo con la **Empresa**, subsistiendo este deber de secreto, aun después de que finalice dicha relación, tanto si esta información es de su propiedad, como si pertenece a un cliente de la misma, o a alguna otra Sociedad que nos proporcione el acceso a dicha información, cualquiera que sea la forma de acceso a tales datos o información y el soporte en el que consten, quedando absolutamente prohibido obtener copias sin previa autorización.

El **Empleado** está de acuerdo en que la Información que reciba o genere a la **Empresa** seguirá siendo propiedad de la **Empresa** y se compromete a usar dicha información únicamente de la manera y para los propósitos autorizados

El **Empleado** se obliga a responder por los daños y perjuicios directos que sufra la **Empresa** por el incumplimiento de las disposiciones de estas políticas,

Este instrumento no otorga, de manera expresa o implícita, ningún derecho intelectual o de propiedad industrial pero si tiene la finalidad de asegurar el cumplimiento de las leyes en materia de derechos de autor

El **Empleado** acepta que el incumplimiento de cualesquiera de las obligaciones que constan en el presente documento, intencionadamente o por negligencia, podrían implicar en su caso, las sanciones disciplinarias correspondientes por parte de la **Empresa**, la

	POLITICA DE SEGURIDAD DE LA INFORMACION		
	Código: PO-AF-TIS-ASEC		
	Revisión: 1	Fecha revisión: 10/Mar/16	Página 4 de 4

posible reclamación de la misma por los daños económicos causados y/o la rescisión del contrato de trabajo.

Esta política constituye el acuerdo total entre las partes y sustituye a cualquier otro entendimiento previo, oral o escrito que haya existido entre ambas partes.

Leída la presente política, enteradas las partes de su contenido y de las obligaciones que contraen, lo firman de conformidad en Querétaro, Querétaro el día _____ de 2014.

EMPLEADO

EMPRESA

LEGAL

COLOCAR PUESTO

REPRESENTANTE

TESTIGO

DESARROLLO HUMANO