1. OBJETIVO DEL DOCUMENTO

Definir la política general de Seguridad Informática de las empresas que conforman Argenti Lemon (AL), a través de la cual se establecen los objetivos y principios de la empresa con respecto a la Seguridad Informática.

2. ALCANCE:

Esta política cubre a la totalidad de los activos informáticos de AL, incluida la información almacenada, procesada, transmitida o impresa por cualquier sistema de procesamiento electrónico de datos o red.

Está directamente involucrada en la presente Política todas las áreas dependientes de la Gerencia General.

Asimismo, intervienen también todos los usuarios de AL que acceden a las redes utilizadas, a los sistemas aplicativos, y a cualquier entorno informàtico; además de terceras personas físicas o jurídicas que desarrollen actividades para AL.

3. DEFINICIONES PREVIAS

A los efectos de una mejor interpretación del contenido de la presente, se definen los siguientes conceptos:

- Propietario de la Información: se considera como tal a la persona responsable principal de una aplicación o directorio de uso compartido.
- Seguridad de la Información: es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnol gicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de los datos y la información.
- Usuarios: son las personas autorizadas a acceder a la información, para realizar las tareas propias de su función (existe el compromiso detallado del mismo en el documento "Compromiso de Usuario".
- Administrador: es la persona perteneciente a la División Sistemas que administra los accesos a los recursos informáticos.
- Activos Informáticos: son aquellos recursos de información, recursos de software físicos y servicios que son propiedad de AL.
- Amenazas: son sucesos ambientales o acciones humanas que podrían ocurrir y producir daños en la integralidad, confidencialidad o disponibilidad de los activos informáticos. Ej.: espionaje, sabotaje, fallas de hardware o software, interrupción de energía, fraude informático.
- Riesgo: es el potencial impacto que una falla de seguridad tendrá en la empresa y la probabilidad de ocurrencia de dicha falla.
- Vulnerabilidad: es cualquier componente de un activo informático susceptible de ser atacado o utilizado por alguna amenaza para producir un daño de la integridad, confidencialidad o disponibilidad de los activos informáticos.

4. DESARROLLO

4.1 Objetivos de la Política:

- Definir la política a aplicar para el control de acceso a los datos, redes, sistemas, programas y archivos e implementar la misma.
- Proteger la información crítica, sensible o confidencial de forma tal que sí lo puedan acceder a ella las personas autorizadas a tal efecto.
- Asegurar la integridad de la información y la protección de los recursos informáticos.
- Establecer el circuito administrativo bajo el cual deberán tratarse las solicitudes de creación de nuevos directorios residentes en la red o modificar los derechos de acceso a los ya existentes, asignar o modificar permisos de acceso a entornos aplicativos, etc.
- Definir valores mínimos para los parámetros de seguridad y los requerimientos mínimos de seguridad lógica por cada nuevo proyecto de informática, según la sensibilidad de la información que maneja.
- Estimular la cultura de seguridad informática en todo el personal de Argenti Lemon. Creando y manteniendo una conciencia de la necesidad de seguridad informática como una parte integral de las actividades operativas rutinarias.
- Asegurar que todos los colaboradores y terceros están advertidos y cumplan con la presente política, con normas y legislaciones en Seguridad Informática.

4.2 Principios generales de la seguridad informática:

Es necesario satisfacer tres conjuntos básicos de requisitos a efectos de lograr una seguridad efectiva en materia de tecnología informática:

- **Confidencialidad:** se refiere al acceso a la información y a su protección; prevenir los accesos no autorizados.
- **Integridad:** se refiere a impedir que la información resulte inexacta o incompleta.
- **Disponibilidad:** se refiere a asegurar que la información esté disponible para atender las necesidades del negocio.

4.3 REQUISITOS DE LA SEGURIDAD INFORMÁTICA:

4.3.1 Confidencialidad: Se define la confidencialidad como “la práctica de revelar los datos únicamente de acuerdo con las políticas y las normas establecidas a tal efecto”.
Los individuos son responsables de sus acciones y están obligados a responder por ellas.
Inicialmente, debe autorizarse a los individuos sobre la base del Principio del Menor Privilegio. Es decir que debe dárseles una autorización mínima de acceso al sistema, con autorizaciones adicionales para tareas específicas, determinadas por el Gerente del área.
Ningún individuo en particular debe estar autorizado para cumplir una funci n sin que otros puedan monitorear o confirmar una actividad; esto permite promover verificaciones cruzadas disminuyendo las posibles acciones fraudulentas.

4.3.2 Integridad: Se define como “la satisfacción de las necesidades de AL en materia de tecnología informática, con los sistemas funcionando correcta y consistentemente, y sin que los datos sean destruidos, corrompidos o modificados en forma no autorizada”.
Tanto los sistemas como los datos deben estar adecuadamente protegidos para asegurar que no se vulnere su disponibilidad, su exactitud o su integridad.
El uso de auditorías produce pistas que preservan la obligación de cada individuo de responder por sus acciones.
4.3.3 Disponibilidad: Se define como “el hecho de que tanto los datos y el sistema como sus recursos y servicios están disponibles cuando se requieran, manteniéndose en forma constante el más alto grado de acceso sin interrupciones”.
Toda información importante debe ser mantenida mediante copias de seguridad.

4.4 RESPONSABILIDADES RESPECTO A LA SEGURIDAD INFORMÁTICA

- Se definirán claramente las responsabilidades para la protección de cada uno de los activos informáticos asignándose “propietarios” de cada uno de los activos informáticos de la empresa.
- Otorgar los derechos de acceso a directorios y archivos a los distintos usuarios, según instrucciones recibidas del propietario de los mismos.
- Ingresar, eliminar o modificar las propiedades de acceso de los usuarios de directorios, archivos o programas aplicativos, según las instrucciones del propietario.
- Limitar el acceso a la red al personal del AL, según las necesidades de cada uno de ellos para el desarrollo de sus funciones, así como también para las personas externas al AL que están llevando a cabo tareas en la empresa, como ser el acceso a archivos e impresoras en red para auditores externos, entornos de trabajo de prueba para proveedores de software, etc. Para estos casos se debe dirigir al Documento de "Acuerdo de Confidencialidad de Proveedores y Contratistas".

4.5 NORMAS DE APLICACIÓN

Ver:

- Normas de Uso de Equipos Informáticos y Sistemas de Información.
- Normas de Uso de E-mail e Internet.
- Normas de Seguridad Lógica.

4.6 NORMATIVAS LEGALES RELACIONADAS

Todas las definiciones del presente código están alineadas con los requerimientos particulares de las siguientes normativas legales:

- Ley 25326 sobre Protección de los Datos Personales (Ley de Habeas Data) y reglamentación del art culo 43 de la C. N.
- Ley11.723 sobre Propiedad Intelectual, sus modificaciones (Ley 25.036).
- Ley 24.776 sobre Secretos Comerciales.

4.7 RESPONSABILIDADES

En el caso de incumplimiento de la presente política, la Compañía se reserva el derecho de tomar las acciones disciplinarias correspondientes de acuerdo al vínculo con el usuario, a saber:

- Disciplinarias de cualquier grado si el usuario fuera empleado de la Compañía, los mismos serán notificados de la presente en forma fehaciente.
- El derecho a suspender toda relación comercial (en el caso de proveedores, terceros, contratados, etc.) que violen la presente política.
- Los terceros / proveedores que desempeñen tareas dentro de la empresa, deben ser notificados de la presente política, incorporando al contrato o que conste en la contratación de los mismos.
- Asimismo, todos los casos podrán quedar sujetos a accionar judicial por responsabilidad civil o penal y/o reclamo por daños.

La Gerencia de RRHH, es la responsable de tomar las medidas disciplinarias correspondientes ante el incumplimiento de la presente POLÍTICA.