

Política de seguridad de la información y protección de datos

La Dirección de LSQA declara que:

- asegurar y preservar la seguridad de los activos de información que generamos y utilizamos en la prestación de nuestros servicios, así como también la información que nos confían otras partes interesadas como ser colaboradores, clientes y proveedores, entre otros; es prioritario y condiciona la viabilidad en la prestación de cualquiera de nuestros servicios
- garantizar la confidencialidad, integridad, disponibilidad, y confiabilidad de la mencionada información, así como también garantizar la protección de los datos que se manejan en toda la Red es clave para asegurar la integridad de nuestras operaciones, así como también la protección de nuestra marca y reputación en todos los países donde LSQA opera.

La Dirección de LSQA se compromete a:

- implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información acorde a los requisitos de ISO 27001
- asegurar que los activos de información, incluyendo datos de partes interesadas, estén protegidos contra acceso, divulgación y modificaciones no autorizados, respetando los acuerdos establecidos y /o compromisos asumidos con las distintas partes interesadas, garantizando su seguridad y confidencialidad
- asegurar que los activos de información estén disponibles a los usuarios que lo requieran según autorizaciones / permisos otorgados por LSQA garantizando su seguridad y confidencialidad
- proteger y salvaguardar todos los datos confiados por partes interesadas vinculadas a LSQA, así como también los datos generados, y utilizados en la prestación de nuestros servicios
- brindar el apoyo necesario para asegurar que las especificaciones internas establecidas respecto a seguridad de la información y protección de datos sean respetadas e implementadas correctamente
- apoyar la gestión de riesgos asociados a seguridad de la información y protección de datos, posibilitando la toma de acciones pertinentes, de manera oportuna, para prevenir cualquier tipo de fraude, sabotaje, robo, uso mal intencionado, entre otros y así minimizar impactos adversos
- apoyar la toma de acciones apropiadas y de manera oportuna en caso de incidentes vinculados a seguridad de la información y a protección de datos, para minimizar impactos adversos en pro de la continuidad del negocio.
- cumplir con la legislación aplicable y las buenas prácticas en materia de seguridad de la información y protección de datos
- promover la toma de conciencia y comportamiento adecuado de todos los integrantes de la Red en relación con la seguridad de la información y la protección de datos, destacando la importancia del manejo responsable de la información y las consecuencias de su uso indebido
- tomar las acciones necesarias en pro de mejorar continuamente los aspectos vinculados a la seguridad de la información y protección de datos en toda la Red.

LSQA exhorta a todos los integrantes de la Red LSQA a ser custodios de los compromisos asumidos en relación con la seguridad de la información y en relación con la protección de datos de toda índole.

Lugar / Place:

Fecha / Date:

Nombre / Name:

Cargo / Position:

Firma / Signature:

Policy of information security and data protection

LSQA Top Management declares that:

- ensure and preserve the security of the information assets that we generate and use in the provision of services, as well as the information entrusted to us by other interested parties such as employees, clients and suppliers, among others; It is a priority and conditions the viability in the provision of any of our services
- guaranteeing confidentiality, integrity, availability, and reliability of the aforementioned information, as well as guaranteeing the protection of the data handled throughout the Network is key to ensure the integrity of our operations, as well as the protection of our brand and reputation in all countries where LSQA operates

LSQA Top Management commits to:

- implement, maintain, and continuously improve an Information Security Management System according to ISO27001 requirements
- ensure that information assets, including data of interested parties, are protected against unauthorized access, disclosure and modifications, respecting the established agreements and /or commitments assumed with the different interested parties, guaranteeing their security and confidentiality
- ensure that information assets are available to users who require it according to appropriate authorizations / permissions given by LSQA, guaranteeing their security and confidentiality
- protect and safeguard all the data entrusted by interested parties related to LSQA, as well as the data generated, and used in the provision of our services
- provide the necessary support to ensure that internal specifications established regarding information security and data protection, are respected and correctly implemented
- support the risk management related to information security and data protection, enabling taking pertinent actions, in a timely manner, to prevent any type of fraud, sabotage, theft, malicious use, among others, and so minimize adverse impacts
- support taking appropriate actions in a timely manner in the event of incidents related to information security and data protection, to minimize adverse impacts towards business continuity.
- accomplish with applicable legislation and with good practices regarding information security and data protection
- promote awareness and appropriate behaviour of all Net members in relation to information security and data protection, highlighting the importance of responsible handling of information and the consequences of its improper use
- take the necessary actions in order to continuously improve aspects related to information security and data protection throughout the Net.

LSQA encourages all members of the LSQA Net to be custodians of the commitments assumed in relation to information security and in relation to the protection of data of all kinds.

Montevideo - Uruguay

22/ 09/ 2021

Ing Jorge Arismendi

CEO - LSQA

