Política de seguridad de la información y protección de datos personales

Information security and personal data protection Policy

DCo RRHH-010

V3 – 11/2025

Índice de Contenido */Content index*

- Propiedad intelectual / *Intellectual property*
- Contexto / *Context*
- Relación con otros documentos de LSQA / *Relationship with other LSQA documents*
- Referencias / *References*
- Alcance / *Scope*
- Declaración de la Dirección / *Top management declaration*
- Compromiso de la Dirección / *Top management commitment*
- Oficial de seguridad de la información */ Information security officer*
- Delegado de Protección de datos personales / *Personal Data Protection Delegate*
- Programa de gestión de la seguridad de la información y la protección de datos */Information security and personal data protection management program*
- Compromiso de todos los integrantes de la Red LSQA / *All members of LSQA Net commitment*
- Consideraciones finales / *Final considerations*

Propiedad intelectual

Disclaimer - Copyright

Copyright © LSQA S.A B.I.C.
Todos los derechos reservados.

Cualquier forma no autorizada de distribución, copia, duplicación, reproducción, o venta (total o parcial) de este contenido, tanto para uso personal como comercial, constituirá una infracción de los derechos de copyright (derecho de autor).

Todo el contenido de LSQA S.A. B.I.C. es "propiedad intelectual" de sus autores, y que por ello está protegido por las leyes que regulan los derechos de autor y de la propiedad intelectual.

Cualquier tipo de reproducción total o parcial de su contenido está totalmente prohibida, a menos que se solicite una autorización expresa, y por escrito a LSQA S.A. B.I.C.

En cualquier caso, se te considerará responsable de dicha acción y sus consecuencias legales, y deberá (bajo amenaza de denuncia y/o litigio) dar el reconocimiento que le corresponde a LSQA S.A B.I.C. y a sus autores. Si no desea solicitar autorización o si ésta le ha sido denegada, considérese no obstante autorizado a mencionar o dirigir a terceros hacia este contenido, hipervínculo o vínculo directo.

Los hechos, opiniones y puntos de vista que expresamos los autores de LSQA S.A. B.I.C., son solamente nuestros, y no tienen por qué coincidir con la política, las ideas, intenciones, planes, estrategias, ni postura oficial de ningún organismo, empresa, compañía, organización, servicio, o persona.

Cualquier uso deberá ser autorizado y notificado previamente a info@lsqa.com

Las observaciones a este documento han de dirigirse a: etica@lsqa.com

Intellectual property

Disclaimer - Copyright

Copyright © LSQA S.A B.I.C.
All rights reserved.

Any unauthorized form of distribution, copying, duplication, reproduction, or sale (in whole or in part) of this content, whether for personal or commercial use, will constitute copyright infringement. (Author rights)

All the content of LSQA S.A B.I.C. is "intellectual property" of its authors and therefore is protected by laws that regulate copyright and intellectual property.

Any type of total or partial reproduction of its content is totally prohibited, unless express authorization is requested, and in writing to LSQA S.A. B.I.C.

In any case, you will be considered responsible for said action and its legal consequences, and you must (under threat of complaint and/or litigation) give the recognition that it corresponds to LSQA S.A B.I.C. and its authors. If you do not wish to request authorization or if it has been denied, consider nevertheless authorized to mention or direct third parties to this content, hyperlink, or direct link.

The facts, opinions and points of view expressed by the authors of LSQA S.A. B.I.C., are solely ours, and do not have to coincide with the policy, ideas, intentions, plans, strategies, or official position of any body, company, company, organization, service, or person.

Any use must be authorized and previously notified to info@lsqa.com

Comments on this document should be addressed to: etica@lsqa.com

Contexto

Organizaciones de todo tipo y tamaño (incluidos los sectores público y privado, comerciales y sin fines de lucro) crean, recopilan, procesan, almacenan, transmiten y eliminan información en muchas formas, incluidas electrónica, física y verbal (por ejemplo, conversaciones y presentaciones).

En un mundo interconectado como el que vivimos, la información y otros activos asociados merecen o requieren protección contra diversas fuentes de riesgo, ya sean naturales, accidentales o deliberadas, ya que representan un altísimo valor para las organizaciones.

La seguridad de la información se logra implementando un conjunto adecuado de controles, que incluyen políticas, reglas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware.

A su vez, la nueva normativa en materia de protección de los datos de carácter personal impone a las organizaciones el ejercicio de una responsabilidad proactiva adoptando las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de esos datos es conforme a la ley.

El objetivo del presente documento es ayudar a desarrollar y difundir una cultura positiva sobre la seguridad de la información y la protección de datos personales, ya que ello:

- protege y mejora la reputación y credibilidad de LSQA,
- demuestra el compromiso de LSQA en la gestión de sus riesgos relacionados a seguridad de la información y protección de datos personales, de forma eficaz y eficiente,
- aumenta la confianza de terceros en la capacidad de LSQA en lograr el éxito sostenido.

Context

Organizations of all types and sizes (including public and private, commercial, and nonprofit sectors) create, collect, process, store, transmit and delete information in many forms, including electronic, physical and verbal (e.g., conversations and presentations).

In an interconnected world like the one we live in, information and other associated assets deserve or require protection against various sources of risk, whether natural, accidental, or deliberate, since they represent a very high value for organizations.

Information security is achieved by implementing an appropriate set of controls, including policies, rules, processes, procedures, organizational structures, and software and hardware functions.

At the same time, the new regulations on the protection of personal data impose on organizations the exercise of proactive responsibility by adopting the appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the processing of these data is in accordance with the law.

The objective of this document is to help develop and disseminate a positive culture regarding information security and the protection of personal data, since this:

- *protects and enhances the reputation and credibility of LSQA,*
- *demonstrates LSQA's commitment to managing its risks related to information security and personal data protection, effectively and efficiently,*
- *increases third party confidence in LSQA's ability to achieve sustained success.*

Referencias

- Norma ISO/IEC 27001:2022 - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos.
- Norma ISO/IEC 27002:2022 - Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para controles de seguridad de la información.

- Ley N° 18331 de fecha 11 de agosto de 2008 emitida en Uruguay - Ley de protección de datos personales
- Decreto N° 414/009 de 21 de agosto de 2009 emitida en Uruguay sobre Protección de Datos Personales y Habeas Data.
- Decreto N° 64/020 de 17 febrero de 2020 emitido en Uruguay sobre Reglamentación de los arts. 37 a 40 de la ley 19.670 y art. 12 de la ley 18.331, referente a Protección de datos personales.

References

- *ISO/IEC 27001:2022 "Information technology - Security techniques - Information security management systems – Requirements*
- *ISO/IEC 27002:2022 "Information technology — Security techniques — Code of practice for information security controls".*
- *Law No. 18331 dated August 11, 2008, issued in Uruguay - Personal data protection law.*
- *Decree No. 414/009 of August 21, 2009, issued in Uruguay on Protection of Personal Data and Habeas Data.*
- *Decree No. 64/020 of February 17, 2020, issued in Uruguay on the Regulation of arts. 37 to 40 of Law 19,670 and art. 12 of Law 18,331, regarding Protection of personal data.*

Relación con otros documentos de LSQA

La presente Política de seguridad de la información y protección de datos, se encuentra disponible en el sitio web de LSQA y junto con las siguientes Políticas y Códigos, establece el marco en el que opera LSQA.:

- ✓ Declaración de imparcialidad
- ✓ Política de Calidad - Experiencia del cliente
- ✓ Política de Cumplimiento
- ✓ Política Antisoborno
- ✓ Política Anti-acoso
- ✓ Política de seguridad de los colaboradores
- ✓ Política Ambiental
- ✓ Código de ética y conducta profesional de LSQA (DCo-RRHH-001/ 002)
- ✓ Lineamientos de transparencia de LSQA

Además, la presente Política adhiere y respeta:

- ✓ Código de Ética de IQNET
- ✓ Código y Normas de Conducta Profesional de APSCA disponible en: https://www.theapsca.org/ethics-integrity/

Todas las Políticas de LSQA se encuentran disponibles en:
https://lsqa.com.uy/es/about/commitment

Relation with other LSQA documents

This Information security and data protection Policy is available on LSQA web site, and together with the following Policies and Codes, establishes the framework in which LSQA operates:

- ✓ *Impartiality Declaration*
- ✓ *Quality Policy - Customer experience*
- ✓ *Compliance Policy*
- ✓ *Anti-Bribery Policy*
- ✓ *Anti harassment Policy*
- ✓ *Policy on safety of employees*
- ✓ *Environmental Policy*
- ✓ *LSQA Code of Professional Ethics and Conduct (DCo-RRHH-001/002)*
- ✓ *LSQA Transparency guidelines*

Besides, this Policy adheres to and respects:

- ✓ *IQNET Code of Ethics*
- ✓ *APSCA Code and Standards of Professional Conduct available at:* https://www.theapsca.org/ethics-integrity/

All LSQA Policies are available at:
https://lsqa.com.uy/es/about/commitment

Alcance de aplicación

Todos los integrantes de la Red LSQA deben poner el máximo cuidado y la debida diligencia respecto a la seguridad de la información y la protección de datos personales (tanto por medios electrónicos como en soporte papel), en todas sus actividades profesionales en nombre de LSQA.

Todos los integrantes de la Red LSQA deben ser custodios del cumplimiento de la presente Política y documentos relacionados.

Asimismo, la presente Política también resulta de obligado cumplimiento para socios de negocios y todas las partes interesadas relacionadas con LSQA.

Scope of application

All members of the LSQA Network must exercise the maximum care and due diligence regarding information security and the protection of personal data (both by electronic and paper media) in all their professional activities on behalf of LSQA.

All members of the LSQA Network must be custodians of compliance with this Policy and related documents.

Likewise, this Policy is also mandatory for business partners, and all interested parties related to LSQA.

Declaración de la Dirección

La Alta Dirección de LSQA declara que:

- asegura y preserva 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; lo cual es prioritario y condiciona la viabilidad en la prestación de cualquiera de nuestros servicios
- garantiza la confidencialidad, integridad, disponibilidad, y confiabilidad de la mencionada información, así como también;
- reconoce la importancia y se encuentra comprometida con la protección de los datos personales de quienes hagan uso de sus servicios y de quienes se relacionen con LSQA de cualquier forma en el marco de sus actividades, por lo que aplicará sus mayores esfuerzos y diligencia en su tratamiento
- garantiza la protección de los datos que se manejan en toda la Red ya que 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.
- es responsable de los tratamientos de datos personales manejados por LSQA.

Top Management Declaration

LSQA S.A. Top Management, declares that:

- *ensures and preserves the security of the information assets that we generate and use in the provision of our services, as well as the information entrusted to us by other interested parties such as collaborators, clients and suppliers, among others, which is a priority and conditions the viability in the provision of any of our services.*
- *guarantees the confidentiality, integrity, availability, and reliability of the aforementioned information, as well as;*
- *recognizes the importance and is committed to the protection of the personal data of those who use its services and those who relate to LSQA in any way within the framework of its activities, so it will apply its greatest efforts and diligence in its treatment.*
- *guarantees the protection of data handled throughout the Network as it is key to ensuring the integrity of our operations, as well as the protection of our brand and reputation in all countries where LSQA operates.*
- *is responsible for the processing of personal data handled by LSQA.*

Oficial de Seguridad de la información

La Alta Dirección de LSQA ha designado un Oficial de Seguridad de la Información, quien se compromete a cumplir con las siguientes funciones:

- Velar por el cumplimiento de las especificaciones establecidas e implementadas en el marco del Programa de gestión de la seguridad de la información y
- Participar en reuniones periódicas (mensuales o quincenales) asesorando a la Dirección de LSQA y a la Función de Cumplimiento de LSQA en materia de seguridad de la información.
- Participar en actividades de desarrollo de competencia y toma de conciencia de integrantes de la Red LSQA sobre aspectos vinculados a seguridad de la información y protección de datos
- Asesorar continuamente a la Dirección de LSQA y a la Función de Cumplimiento de LSQA con respecto a los principales riesgos que está expuesto LSQA, así como también proponer acciones apropiadas al respecto, mediante la ejecución de análisis de riesgos periódicos.
- Coordinar y ejecutar rutinas de control periódicas, relacionadas con seguridad de la información, informar oportunamente a la Dirección de LSQA y a la Función de Cumplimiento de LSQA sobre los resultados de dichas rutinas de control, así como también proponer acciones apropiadas para la mitigación de riesgos y minimización de efectos adversos para LSQA, y hacer seguimiento de la implementación y verificación de la eficacia de las acciones tomadas.
- Monitorear el cumplimiento de especificaciones establecidas e implementadas en el marco del Programa de gestión de la Seguridad de la información y protección de datos personales de LSQA (por ejemplo, mediante la planificación y ejecución de auditorías internas)
- Planificar y monitorear el Plan de Continuidad de Negocio de LSQA con relación a la seguridad de la información.
- Participar y responder ante auditorías externas (en caso de ser necesario).
- Ejercer el rol de “nexo” entre la empresa y organismos/proveedores (en caso de ser necesario).

Information security officer

LSQA Top Management has appointed an Information Security Officer, who undertakes to fulfill the following functions:

- *Ensure compliance with the specifications established and implemented within the framework of the LSQA information security management and*
- *Participate in periodic meetings (monthly or biweekly) advising the LSQA Top Management and the LSQA Compliance Function concerning information security matters.*
- *Participate in activities to develop competence and raise awareness of members of the LSQA Network on aspects related to information security and data protection.*
- *Continuously advise LSQA Top Management and LSQA Compliance Function regarding the main risks that LSQA is exposed to, as well as propose appropriate actions in this regard, through the execution of periodic risk analyses.*

- *Coordinate and execute periodic control routines related to information security, promptly inform the LSQA Top Management and the LSQA Compliance Function about the results of said control routines, as well as propose appropriate actions for risk mitigation. and minimization of adverse effects for LSQA and monitor the implementation and verify the effectiveness of the actions taken.*

- *Monitor compliance with specifications established and implemented within the framework of the LSQA Information Security and personal data protection Management Program (for example, by planning and executing internal audits)*

- *Plan and monitor the LSQA Business Continuity Plan concerning information security.*
- *Participate and respond to external audits (if necessary).*

- *Play the role of “nexus” between the company and organizations/suppliers (if necessary).*

Delegado de Protección de datos personales

La Alta Dirección de LSQA ha designado un Delegado de Protección de datos personales, quien se compromete a cumplir con las siguientes funciones:

- promover, difundir y apoyar la protección de datos personales, garantizando que la misma sea parte del proceso de planificación, definiendo estrategias, planes, políticas y todo aquello que incremente y mejore la seguridad y protección de datos e información.
- asesorar a la Dirección de LSQA en la formulación, diseño y aplicación de la presente política y supervisar su cumplimiento en LSQA así como proponer todas las medidas que entienda pertinentes para adecuar sus prácticas a la normativa y a los estándares internacionales en materia de protección de datos personales y verificar su realización.

Personal data protection delegate

The Top Management of LSQA has appointed a Personal Data Protection Delegate, who undertakes to fulfill the following functions:

- *promote, disseminate, and support the protection of personal data, guaranteeing that it is part of the planning process, defining strategies, plans, policies and everything that increases and improves the security and protection of data and information.*

- *advise the LSQA Management on the formulation, design and application of this policy and supervise its compliance at LSQA as well as propose all the measures it deems relevant to adapt its practices to the regulations and international standards on personal data protection and verify its implementation.*

Compromiso de la Dirección

La Dirección de LSQA se compromete a:

- implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información tomando como referencia 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

Top Management commitment

LSQA Top Management commits to:

- *implement, maintain, and continually improve an Information Security Management System taking as reference the requirements of ISO 27001*
- *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 authorizations / permissions granted by LSQA, guaranteeing their security and confidentiality.*
- *protect and safeguard all data entrusted by interested parties linked to LSQA, as well as the data generated and used in the provision of our services.*
- *provide the necessary support to ensure that the internal specifications established regarding*

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
- asegurar el cumplimiento de la normativa y de los estándares internacionales, permitiéndole a LSQA gestionar los controles y acciones requeridas para garantizar la protección de los datos de carácter personal de los cuales es responsable, en forma concomitante y conjunta con la seguridad de la información.
- 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.
- promover, difundir y apoyar la protección de datos personales, con el apoyo del Delegado de Protección de Datos (DPD), garantizando que la misma sea parte del proceso de planificación, definiendo estrategias, planes, políticas y todo aquello que incremente y mejore la seguridad y protección de datos e información, en debida coordinación con los objetivos en materia de seguridad de la información de LSQA.
- pone a disposición de todas las partes interesadas un canal (dirección de correo electrónico) datospersonales@lsqa.com , para que puedan ejercer sus derechos en referencia a datos personales.

information security and data protection are respected and correctly implemented.

- *support the management of risks associated with information security and data protection, enabling the taking of pertinent actions, in a timely manner, to prevent any type of fraud, sabotage, theft, malicious use, among others and thus minimize adverse impacts.*
- *support the taking of appropriate and timely actions in the event of incidents linked to information security and data protection, to minimize adverse impacts in favour of business continuity.*
- *comply with applicable legislation and good practices regarding information security and data protection.*
- *ensure compliance with regulations and international standards, allowing LSQA to manage the controls and actions required to guarantee the protection of personal data for which it is responsible, concomitantly, and jointly with the security of the information.*

- *promote awareness and appropriate behaviour of all members of the Network in relation to information security and data protection, highlighting the importance of responsible management of information and the consequences of its improper use.*

- *take the necessary actions to continually improve aspects related to information security and data protection throughout the Network.*
- *promote, disseminate and support the protection of personal data, with the support of the Data Protection Delegate (DPD), guaranteeing that it is part of the planning process, defining strategies, plans, policies and everything that increases and improves the protection of personal data. security and protection of data and information, in due coordination with the information security objectives of LSQA.*

- *makes available to all interested parties a channel (email address) datospersonales@lsqa.com , so that they can exercise their rights in reference to personal data*

Programa de gestión de la seguridad de la información y protección de datos personales

Consecuentemente, LSQA ha determinado implementar, mantener y mejorar continuamente un Programa de gestión de la seguridad de la información y protección de datos personales, apoyado por un equipo de expertos en la materia.

Dicho Programa incluye Políticas, Procedimientos y demás documentos internos, que establecen prácticas sistemáticas; roles, autoridades y responsabilidades pertinentes; así como también mecanismos de mitigación de los riesgos identificados; métodos para el control y la evaluación de desempeño de dicho Programa.

Lo métodos de control vinculados a la protección de datos personales permite asegurar la aplicación de **los principios** de: Legalidad, Veracidad, Finalidad Previo consentimiento informado, Seguridad de los datos, Reserva y Responsabilidad.

Asimismo, también busca garantizar los derechos de los titulares de los datos a: Información frente a la recolección de Datos, Acceso, Rectificación, Actualización, Inclusión, Supresión e "Impugnación de valoraciones personales".

Principios generales de protección de datos y criterios de aplicación:

- ✓ **Principio de Legalidad:** las bases de datos que utilice LSQA serán debidamente inscriptas en el registro de la URCDP y se observará en su operación los principios que establece la legislación de protección de datos personales antes identificada.
- ✓ **Principio de Veracidad**: los datos personales que trate LSQA serán veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido y, si fuera necesario, actualizados; adoptándose todas las medidas razonables para que se supriman o rectifiquen sin dilación.
- ✓ **Principio de Finalidad**: los datos personales serán tratados por LSQA para el cumplimiento de fines determinados, explícitos y legítimos y no serán utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

Information security and personal data protection management program

Consequently, LSQA has determined to implement, maintain, and continuously improve an Information security and personal data protection Management Program, supported by a team of experts in the field.

Said Program includes Policies, Procedures, and other internal documents, which establish systematic practices; relevant roles, authorities, and responsibilities; as well as mitigation mechanisms for identified risks; methods for controlling and evaluating the performance of said Program.

*The control methods linked to the protection of personal data ensure the application of **the principles** of: Legality, Veracity, Purpose Prior informed consent, Data security, Reserve and Responsibility.*

Besides, it also seeks to guarantee the rights of data owners to: Information regarding the collection of Data, Access, Rectification, Update, Inclusion, Deletion and "Challenge of personal evaluations".

General data protection principles and application criteria:

- ✓ ***Principle of Legality**: the databases used by LSQA will be duly registered in the URCDP registry and the principles established by the personal data protection legislation identified above will be observed in their operation.*
- ✓ ***Principle of Truthfulness**: the personal data processed by LSQA will be truthful, adequate, fair, and not excessive in relation to the purpose for which they were obtained and, if necessary, updated; taking all reasonable measures to ensure that they are deleted or rectified without delay.*
- ✓ ***Principle of Purpose**: personal data will be processed by LSQA for the fulfillment of specific, explicit, and legitimate purposes and will not be used for purposes different from or incompatible with those for which it was obtained.*

- ✓ **Principio de Previo consentimiento Informado**: los datos personales solamente serán tratados por LSQA cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado o cuando dicho tratamiento se encuentre amparado en alguna otra base legal de legitimación, que habilite el tratamiento sin requerir el consentimiento del titular
- ✓ **Principio de Seguridad de los datos**: los datos personales serán tratados por LSQA de tal manera que se garantice su seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas.
- ✓ **Principio de Reserva**: quienes en cualquier carácter y legítimamente, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales bajo responsabilidad de LSQA, están obligados a utilizarlos en forma reservada y exclusivamente para las operaciones autorizadas, estando prohibida toda difusión de los mismos a terceros, debiendo guardar estricto secreto profesional, incluso luego de extinguirse la relación con LSQA, cualquiera sea la naturaleza de ésta.
- ✓ **Principio de Responsabilidad**: LSQA en ejercicio de una responsabilidad proactiva adoptará las medidas técnicas y organizativas para dar cumplimiento a los principios anteriormente señalados y que le permitan estar en condiciones de demostrar dicho cumplimiento.
- ✓ **Gestión de derechos de los titulares de los datos**: LSQA establecerá como medida de privacidad desde el diseño, los mecanismos necesarios para asegurar el ejercicio de los derechos de los titulares de los datos personales, en los plazos previstos en la normativa, a cuyos efectos aprobará y aplicará el Procedimiento de Gestión de Derechos (PG027).
  Si cualquier parte interesadas desea ejercer sus derechos en relación con la protección de datos personales, en referencia a la Ley Uruguaya 18.331, puede enviar su consulta a datospersonales@lsqa.com, indicando nombre, apellido y dirección de correo de contacto.
- ✓ **Análisis de riesgos y Evaluación de Impacto en la Protección de Datos (EIPD)**: previo al inicio de todo tratamiento de datos de carácter personal, LSQA llevará a cabo un análisis de

- ✓ ***Principle of Prior Informed Consent****: personal data will only be processed by LSQA when the owner has given free, prior, express, and informed consent or when said treatment is protected by some other legal basis of legitimacy, which enables the treatment without requiring the consent of the owner.*

- ✓ ***Data Security Principle****: personal data will be treated by LSQA in such a way that its security is guaranteed, including protection against unauthorized or illicit processing and against accidental loss, destruction, or damage, through the application of technical measures. and appropriate organisations.*
- ✓ ***Principle of Reservation:*** *those who, in any capacity and legitimately, have access to or intervene in any phase of the processing of personal data under the responsibility of LSQA, are obliged to use them in a reserved manner and exclusively for authorized operations, and any dissemination of the same is prohibited. to third parties, and must maintain strict professional secrecy, even after the relationship with LSQA has expired, whatever its nature.*
- ✓ ***Principle of Responsibility****: LSQA, in the exercise of proactive responsibility, will adopt technical and organizational measures to comply with the above-mentioned principles and that allow it to be in a position to demonstrate said compliance.*
- ✓ ***Management of the rights of data owners****: LSQA will establish as a privacy measure from the design, the necessary mechanisms to ensure the exercise of the rights of the owners of personal data, within the deadlines provided in the regulations, for which purposes will approve and apply the Rights Management Procedure (PG027). If any interested party wishes to exercise their rights in relation to the protection of personal data, in reference to Uruguayan Law 18,331, they can send their query to datospersonales@lsqa.com , indicating name, surname and contact email address.*

- ✓ ***Risk analysis and Data Protection Impact Assessment (DPIA)****: prior to the start of all personal data processing, LSQA will carry out a risk analysis to identify and manage the risks to*

riesgo que permita identificar y gestionar los riesgos para los derechos de las personas, minimizándolos hasta niveles que puedan considerarse aceptables y revisándolos en forma periódica y al menos cada dos (2) años y en cualquier otra oportunidad en que exista un cambio significativo en los sistemas de información y/o en los tratamientos de datos personales. Asimismo, LSQA llevará a cabo una Evaluación de Impacto en la Protección de Datos (EIPD) en los casos expresamente previstos en la normativa o cuando del análisis realizado resulte probable que el tratamiento suponga un riesgo significativo para los derechos de las personas.

- ✓ **Gestión de vulneraciones de seguridad para la protección de datos**: LSQA implementará los mecanismos apropiados para la correcta identificación, registro, resolución y notificación de los incidentes de seguridad que afecten datos de carácter personal, dando cumplimiento a las formalidades y plazos previstos en la normativa legal y reglamentaria aplicable, a cuyos efectos aprobará y aplicará el Procedimiento de Gestión de Incidentes de Seguridad (PG023)

- ✓ **Privacidad desde el Diseño**: en forma previa al inicio del tratamiento y durante todo su desarrollo, LSQA implantará el estándar de "Privacidad desde el Diseño" con el objetivo de cumplir con los requisitos definidos en la reglamentación de la normativa legal y siguiendo sus orientaciones, a efectos de que la protección de datos se encuentre presente desde las primeras fases de concepción de las bases de datos, las operaciones de tratamiento, las aplicaciones, los sistemas informáticos y en general cualquier proyecto que involucre datos de carácter personal.
- ✓ **Privacidad por Defecto**: LSQA aplicará las medidas técnicas y organizativas apropiadas a los efectos de garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

the rights of the people, minimizing them to levels that can be considered acceptable and reviewing them periodically and at least every two (2) years and at any other time when there is a significant change in the information systems and/or in the processing of personal data. Besides, LSQA will carry out a Data Protection Impact Assessment (DPIA) in the cases expressly provided for in the regulations or when the analysis carried out shows that the processing is likely to pose a significant risk to the rights of individuals.

- ✓ ***Management of security breaches for data protection:*** *LSQA will implement the appropriate mechanisms for the correct identification, registration, resolution, and notification of security incidents that affect personal data, complying with the formalities and deadlines provided for in the regulations. applicable legal and regulatory regulations, for which purposes it will approve and apply a Security Incident Management Procedure (PG023).*

- ✓ ***Privacy by Design****: prior to the start of the treatment and throughout its development, LSQA will implement the "Privacy by Design" standard with the aim of complying with the requirements defined in the legal regulations and following its guidelines, so that data protection is present from the first phases of conception of databases, processing operations, applications, computer systems and in general any project that involves personal data.*

- ✓ ***Privacy by Default****: LSQA will apply the appropriate technical and organizational measures to guarantee that, by default, only the personal data that are necessary for each of the specific purposes of the treatment are processed.*

Compromiso de los todos los integrantes de la Red LSQA

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.

Todo el personal de LSQA así como todos los terceros colaboradores que le presten servicios con acceso a datos personales bajo su responsabilidad, tienen la obligación de conocer y cumplir lo previsto en la presente Política así como en las normas y procedimientos que la desarrollen. Asimismo tienen el deber de colaborar en la mejora y requisitos en materia de protección de datos evitando y aminorando los riesgos a los que se encuentra expuesta la información y los datos personales bajo responsabilidad de LSQA.

En especial, es responsabilidad de todo el personal de LSQA, del personal temporario, terceras partes debidamente autorizadas y en general, de toda persona física o jurídica que legítimamente acceda a información personal bajo responsabilidad de LSQA, el reportar y registrar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo con los procedimientos correspondientes.

Los colaboradores de LSQA tienen la obligación de participar en las actividades de formación vinculadas a seguridad de la información y protección de datos personales cuando corresponda.

Finalmente, se exhorta a las personas que actúen en representación de LSQA sin formar parte de su organización, que observen las disposiciones de esta Política y se esfuercen para promover su cumplimiento en las sociedades a las que pertenezcan y desde las que representen a LSQA.

All members of LSQA Net commitment

LSQA urges all members of the LSQA Network to be custodians of the commitments made in relation to information security and in relation to the protection of data of all kinds.

All LSQA staff, as well as all third-party collaborators who provide services with access to personal data under their responsibility, have an obligation to know and comply with the provisions of this Policy as well as the rules and procedures that develop it. They also have the duty to collaborate in the improvement and requirements regarding data protection, avoiding and reducing the risks to which the information and personal data under the responsibility of LSQA are exposed.

In particular, it is the responsibility of all LSQA staff, temporary staff, duly authorized third parties and, in general, any natural or legal person who legitimately accesses personal information under the responsibility of LSQA, to report and record security violations. of information, confirmed or suspected in accordance with the corresponding procedures.

LSQA collaborators have an obligation to participate in training activities related to information security and protection of personal data when applicable.

Finally, people acting on behalf of LSQA without being part of its organization are urged to observe the provisions of this Policy and to make efforts to promote compliance in the societies to which they belong and from which they represent LSQA.

Consideraciones finales

- La política de seguridad de la información y protección de datos personales se encuentra a disposición de todo el personal de LSQA y sus partes interesadas, y se publica a través de canales de comunicación internos y externos, según sea apropiado.
- La presente política podrá incorporarse como parte de los contratos legalmente ejecutables con empleados, clientes, subsidiarias / socios y proveedores/socios de negocio según los riesgos evaluados y las recomendaciones de los asesores legales de LSQA.
- La presente política se encuentra siempre sujeta a cambios que redunden en una mejor comprensión y la incorporación de mejores prácticas de cumplimiento. Si usted como usuario desea sugerir mejoras lo invitamos a escribirnos a etica@lsqa.com
- LSQA se reserva siempre el derecho de establecer o no establecer vínculos comerciales y de cualquier tipo con aquellas personas y organizaciones que adhieran a los principios, valores y requisitos de la presente política.
- Cualquier modificación u alteración del presente documento con el fin de atenuar los criterios de LSQA en materia de cumplimiento sin autorización expresa de la Dirección será considerado una falta grave.
- Si usted no es usuario de esta política, pero desea considerarla como base para el desarrollo de las políticas de cumplimiento en las organizaciones o ámbitos en los que participe con gusto le extenderemos una licencia para el uso, solicitando la misma a etica@lsqa.com

Final considerations

- *The Security information and personal data protection Policy is available to all LSQA personnel and stakeholders and is posted through internal and external communication channels, as appropriate.*
- *This policy may be incorporated as part of legally enforceable contracts with employees, customers, branches / partners, and suppliers/business partners based on the risks assessed and the recommendations of LSQA's legal advisors.*
- *This policy is always subject to changes that result in a better understanding and the incorporation of better compliance practices. If you as a user wish to suggest improvements, we invite you to write to us at etica@lsqa.com*
- *LSQA always reserves the right to establish or not establish commercial links of any kind with those people and organizations that adhere to the principles, values, and requirements of this policy.*
- *Any modification or alteration of this document in order to attenuate the LSQA criteria in terms of compliance without the express authorization of the Top Management will be considered a serious offense.*
- *If you are not a user of this policy, but wish to consider it as a basis for the development of compliance policies in the organizations or areas in which you participate, we will gladly issue you a license for its use, by requesting it to etica@lsqa.com*

Vigencia

El presente documento ha sido aprobado por el CEO de LSQA – Dr. Ing. Santiago Vázquez, el 01 de Noviembre de 2025.

Validity

This document has been approved by LSQA CEO – Dr. Eng. Santiago Vázquez, on November 1st, 2025.

Nuestras oficinas – Our Offices

LSQA URUGUAY
Av. Italia 6201
Edificio "Los Tilos" piso 1, 11500,
Montevideo, Uruguay
Tel: (+598) 2600 0165
Email: info@lsqa.com

LSQA PARAGUAY
Edificio Trading Park - Piso 9,
Avda. Aviadores del Chaco Nro. 3207,
Barrio Salvador del Mundo Asunción,
Paraguay
Tel: (595) 21 444 128

LSQA ARGENTINA
Piedras 625, C1070. CABA - Argentina
Tel.: (+5411) 4342-3442, 43422465

LSQA CHILE
Balmaceda 921, Oficina 27. Talagante, Chile
Tel: +56 228154197 / +56 228154274
/ +56 966460595

LSQA PERÚ
Centro Empresarial Centrum Jr. Monte Rosa
256 Of. 702,
Chacarilla - Santiago de Surco, Perú
Tel: (+511) 505 4952

LSQA ECUADOR
Centro Empresarial Colón Empresarial 1-
Oficina 107 Guayaquil, Ecuador
Tel: (+593) 982801150
alcantara@lsqa.com

LSQA BRASIL
Oficina de Representación SANTEC. Avenida
da Integração Aírton Senna, 650. Vila dos
Ingás II Postal Code: 56.328-010.
Tel: (+55) 87 8811- 0616
danielsantec@yahoo.com.br

OFICINA REGIONAL PARA CENTROAMÉRICA
Avda. 12 y Calle 33, Los Yoses Sur
De KFC 100 m Este, 400 m Sur, 25 m Este San
José, Costa Rica
Tel.: (+506) 2524 2560

LSQA MÉXICO
23 Poniente # 704, Colonia El Carmen, CP
72530, Puebla, Pue. México
Tel: + 52 1 2222128403, 55 54431054,
55 3908 4508.

LSQA ESPAÑA
Madrid, España
Tel: + 34 655269461

LSQA ITALY
Via Camerata Picena 385, 00138 ROMA (RM),
Italia
Tel: (+39) 06.88644843
bruno.desimone@qualityitalia.org

LSQA SERBIA
Dravska 11. 11000 Beograd. Serbia
Tel: (+381) 11 380 7160

LSQA MIDDLE EAST LTD
7 El Lewaa Hussein Said St. El Haram, Giza,
Egypt
Phone: +20 106 884 0840
sayed@lsqame.com

LSQA

Member of

IQNET