POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

LORENZATI RUETSCH Y CIA. S.A.

El objetivo de la Política General de Seguridad de la Información es establecer los lineamientos relativos a la protección de la información de la empresa y los recursos de procesamiento asociados.

La Dirección considera que la adecuada Gestión de la Seguridad de la Información contribuye a la operatoria y continuidad del negocio y a la reducción de riesgos a niveles aceptables. Por lo tanto, se compromete con la prevención de incidentes de seguridad, y la preservación de la confidencialidad, integridad y disponibilidad de la información.

Esta política (y las políticas derivadas), son de aplicación para todo el personal y/o terceros que accedan y/o utilicen información y/o recursos de procesamiento asociados.

Se define que será revisada anualmente por el Directorio. Las actualizaciones serán comunicadas de manera oportuna.

DEFINICIONES DE TÉRMINOS TÉCNICOS:

- **Confidencialidad:** proteger la información contra uso no autorizado. Sólo las personas autorizadas tendrán acceso a la información requerida bajo el criterio de "mínimo privilegio" y “la necesidad de conocer”.
- **Integridad:** minimizar la existencia de errores y/o corrupción en toda la información y garantizar que la misma sea exacta, completa y válida.
- **Disponibilidad:** garantizar que la información esté accesible y pueda ser utilizada cuando sea requerida por personas autorizadas.
-

Los objetivos de Seguridad de la Información se establecen teniendo en cuenta la estrategia de negocio, el entorno (ej. riesgos emergentes), las normativas/leyes y los avances en materia informática.

El Directorio es el responsable de supervisar los objetivos de Seguridad de la Información, los mismos se revisan al menos una vez al año.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

- Se comunican las responsabilidades y derechos en materia de Seguridad de la Información desde el momento del ingreso del personal y/o la contratación del tercero. Se generan acciones de concientización.
- La información se clasificará de acuerdo al grado de sensibilidad y criticidad. El personal y los terceros deberán manejar la información en forma apropiada.
- Los riesgos de seguridad de información son identificados, analizados, evaluados, tratados y monitoreados de acuerdo a criterios avalados por la Dirección.
- Se proporcionan los medios adecuados para implementar los controles aprobados de seguridad de la información con el fin de preservar su confidencialidad, integridad y disponibilidad. Las medidas de seguridad y los controles establecidos son proporcionales a la criticidad de la información a proteger y a su clasificación.
- Se protege la información contra accesos indebidos (Lógicos y Físicos), pérdida o corrupción y se establecen mecanismos de acceso para quienes tengan una legítima necesidad autorizada.
- Los principios de Seguridad de la Información deberán ser incorporados a los sistemas aplicativos en todo el ciclo de vida, incluyendo los procesos de diseño, desarrollo, prueba, mantenimiento y puesta en producción (*).
- Se gestionan los incidentes de seguridad de la información y se trabaja para prevenir los mismos.
- Todas las contrataciones que supongan o requieran acceso o tratamiento de información clasificada como crítica deberán realizarse amparadas por un contrato que incluya cláusulas destinadas a garantizar la salvaguarda de la información.
- Se planifican, implementan y prueban esquemas de redundancia y contingencia de sistemas críticos. Las redes y los sistemas principales se evaluarán de manera periódica para conocer en todo momento su estado de seguridad.
- Se brinda información actualizada sobre el estado de seguridad de la información al Directorio.
- Se atienden los requisitos (Internos y Externos) aplicables relacionados con Seguridad de la Información

ROLES Y RESPONSABILIDADES

La implementación satisfactoria de la Política General de Seguridad de la Información, y las medidas derivadas, **requiere el compromiso de toda la empresa.**

Se definen los siguientes Roles para la Gestión de la Seguridad de la Información:

- **Dirección**: responsable de demostrar liderazgo y compromiso respecto de la Seguridad de la Información y de participar en la toma de decisiones generales en cuestiones relativas a la Seguridad de la Información.
- **ROL: Encargado de Seguridad / CISO** (Chief Information Security Officer) responsable de implementar la estrategia de seguridad en la empresa.
- **Propietarios de la información:** mandos medios que la empresa reconoce como responsables de clasificar, distribuir o autorizar el uso de la información.
- **Custodio**: responsable de administrar las medidas de seguridad.
- **Usuarios:** quienes acceden a la información y hacen uso responsable de la misma para la realización de sus tareas.

La presente política reviste el carácter de norma reglamentaria, y en el caso de desviaciones, con toda la información pertinente se podrán definir sanciones disciplinaras enmarcadas dentro del Código de Ética.
Las excepciones a la Política de Seguridad de la Información o derivadas, serán tratadas por el CISO y debidamente informadas.

DATA SECURITY POLICY

LORENZATI RUETSCH Y CIA. S.A.

The objective of the Data Security Policy is to provide a guideline to protect the information of the company and the related processing resources.

The Board of Directors consider that the correct Data Security Management contributes to the operation and the continuation of business and to the reduction of risks to acceptable levels. Therefore, they are committed to prevent security issues and preserve the confidentiality, integrity and availability of data.

This policy, as well as the ones related, are applicable to all personnel and/or third parties who have access and/or use data and/or associated processing resources. It is established that this policy will be reviewed annually by the Board of Directors. Updates will be informed at the appropriate time.

DEFINITION OF TECHNICAL VOCABULARY

- **Confidentiality:** to protect data against unauthorized use. Only authorized people will have access to the information by following the “least privilege” and “need to know” criteria.
- **Integrity:** Minimize errors and/or corruption of information and guarantee that it is accurate, complete and valid.
- **Availability:** guarantee that the information is accessible and can be used when required by authorized people.

The Data Security objectives are established according to the business strategy, the environment (e.g. emerging risks), regulations/laws and the information technology developments.

DATA SECURITY POLICY

The Board of Directors is in charge of monitoring the Data Security objectives, which are reviewed at least once a year.

DATA SECURITY PRINCIPLES

- The responsibilities and rights about Data Security are communicated as soon as new employees and/or third party personnel are hired. Awareness actions are introduced about this issue, too.
- The information will be classified according to the degree of sensitivity and criticality levels. Personnel and third parties must handle the information appropriately.
- Data security risks are identified, analyzed, evaluated, treated and monitored according to the criteria approved by the Board of Directors.
- All the necessary means are provided to introduce approved data security controls in order to preserve the data´s confidentiality, integrity and availability. The established security measures and controls are related to the criticality of the data to be protected.
- The information is protected against improper access, logical and physical, loss or corruption and access mechanisms are established for those who have a legitimate authorized need.
- The Data Security Principles must be added to the systems throughout the cycle, including the design, development, testing, maintenance and production processes (*).
- Personnel manage data security incidents and work to prevent them.
- All contracts that involve or require access to critical classified data must sign a contract that includes clauses intended to guarantee the data security.

- Redundancy and contingency layouts for critical systems are planned, introduced and tested. The main networks and systems will be evaluated periodically to assess their security status at all times.
- Updated information about the security status of the data is provided to the Board of Directors.
- The applicable internal and external requirements related to the Data Security are taken into account.

ROLES AND RESPONSIBILITIES

The success of the Data Security Policy, and related measures, **depends on the commitment of the entire company.**

The following roles were defined for the Data Security Management:

- **Board of Directors:** responsible for demonstrating leadership and commitment regarding the Data Security and for taking part in general decision on Data Security issues.
- **ROLE:** Security Manager/CISO (Chief Information Security Officer) is responsible for introducing the security strategy in the company.
- **Information owners:** middle management that the company recognizes as responsible for classifying, distributing and authorizing the use of data.
- **Data Custodian:** responsible for managing security measures.
- **Users:** those who have access to the data and use it properly to perform their tasks.

DATA SECURITY POLICY

This policy is a regulatory norm and, in case of deviations, disciplinary sanctions could be taken with all the available information according to the Code of Ethics. Exceptions to the Data Security Policy, or the derivative ones, will be treated by the CISO and duly informed.

Update Date: August 2022 • Version 001