Extracto de la Política General de Seguridad de la Información y Ciberseguridad

CIRIONTECHNOLOGIES.COM

1. Objetivo

Esta Política, así como el cuerpo normativo que la desarrolla, tiene como objetivo proteger los activos de información contra la modificación, divulgación, destrucción accidental o no autorizada, así como garantizar los principios generales de seguridad de confidencialidad, integridad y disponibilidad.

2. Referencias para la elaboración de este documento

- **ISO/IEC 27001:2022** Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- **ISO/IEC 27002:2022** Information security, cybersecurity and privacy protection — Information security controls
- **ISO 22301:2019** Security and resilience — Business continuity management systems — Requirements
- **CIS Controls v8** – Center for Internet Security Critical Security Controls for Effective Cyber Defense
- **ITIL® 4 – ITIL Foundation**, AXELOS Global Best Practice
- **Resolución Anatel Nº 740**, de 21 de diciembre de 2020
- The **NIST Cybersecurity Framework** (CSF) 2.0
- **Sarbanes-Oxley Act of 2002 (SOX)**, Public Law 107–204
- Payment Card Industry Data Security Standard (**PCI DSS**) v4.0, PCI Security Standards Council, 2022

Esta política está alineada con las principales normas globales de protección de datos, considerando los marcos legales vigentes en los países donde la compañía mantiene operaciones.

3. Responsabilidades

La Seguridad de la Información y la Ciberseguridad son responsabilidades compartidas por toda la organización. Sin embargo, la Dirección de Ciberseguridad es el área responsable de garantizar la implementación, el mantenimiento y la evolución continua de las estrategias, políticas, normas y controles de seguridad aplicables a la organización.

4. Acciones de concientización

Cirion, a través de sus políticas y procedimientos organizacionales, tiene como objetivo difundir y concientizar a todos los colaboradores sobre el mantenimiento de una estructura sólida de seguridad de la información.

Actualmente, se realizan capacitaciones internas obligatorias para la difusión y concientización sobre la seguridad de la información. Además, se llevan a cabo campañas que simulan riesgos y amenazas a la seguridad.
Para el público externo, se publican contenidos en redes sociales y en el sitio web de Cirion que abordan el tema de la seguridad cibernética desde distintas perspectivas.

5. Lineamientos generales de los procedimientos y controles de seguridad

5.1 Clasificación y Control de Activos

La información deberá ser clasificada en función de su nivel de criticidad y confidencialidad. Como resultado de este proceso y de acuerdo con la funcionalidad que cumple deberá ser administrada y rotulada con el fin de garantizar el adecuado nivel de protección y evitar su exposición más allá de lo necesario para el normal desempeño de las tareas relacionadas en su utilización.

5.2 Gestión de Riesgos

La organización debe establecer un proceso continuo y sistemático de gestión de riesgos de seguridad de la información, de acuerdo con las mejores prácticas de ISO/IEC 27001 (y estándares específicos como ISO 27005). El objetivo es identificar y evaluar proactivamente los riesgos que puedan afectar a la información y los sistemas, para tratarlos de forma oportuna.

5.3 Seguridad Lógica y Control de Acceso

La seguridad lógica abarca los mecanismos y controles para proteger los sistemas informáticos, aplicaciones y datos frente a accesos no autorizados o actividades maliciosas. Un elemento central de ello es el control de acceso, que garantiza que cada usuario o sistema obtiene únicamente los permisos necesarios para realizar sus funciones, y nada más (principio de mínimo privilegio).

Todos los sistemas que almacenen o procesen información deben tener su acceso estrictamente controlado. El nivel de control de acceso requerido para un sistema que almacene o procese información, o a un recurso en concreto, viene determinado por el impacto potencial en el negocio.

5.4 Seguridad en Redes y Comunicaciones

La infraestructura de red y comunicaciones forma la columna vertebral sobre la cual circula la información de la empresa. Por ello, deben implementarse medidas de seguridad para proteger las redes internas, perimetrales y las comunicaciones de datos frente a accesos no autorizados, intercepciones o interrupciones.

Los controles para gestionar los riesgos para la información que se transmite en las redes de Cirion o en internet deben cumplir con los estándares de seguridad establecidos.

.

5.5 Continuidad del Negocio y Recuperación ante Desastres

Se deben definir medidas para asegurar la Continuidad del negocio ante situaciones que afecten o interrumpan el normal desempeño de los servicios de Cirion. Esto proporciona una estructura sistemática para prepararse, responder y recuperarse de incidentes de mayor escala, ya sean causados por desastres naturales, fallos tecnológicos catastróficos, ciberataques de gran impacto u otras crisis.

5.6 Cumplimiento Normativo y Protección de Datos Personales

Se deben identificar los requerimientos legales y regulatorios en materia de seguridad de la información y protección de datos personales y asegurar la incorporación de los requerimientos en las políticas de seguridad, en el diseño e implementación de los servicios de tecnología y prácticas de auditoría. Todo el personal debe comprender y cumplir con los términos contractuales aplicables.

Cualquier violación de datos personales deberá ser notificada de forma ágil y observar las orientaciones y exigencias legales previstas en las leyes de protección de datos aplicables en los países donde la compañía mantiene operaciones.

5.7 Gestión de Vulnerabilidades

La compañía debe mantener un proceso estructurado de gestión de vulnerabilidades con el objetivo de reducir los riesgos asociados a fallas de seguridad en los activos de información, contemplando la identificación de vulnerabilidades, evaluación, priorización de riesgos, tratamiento y corrección, monitoreo y documentación.

5.8 Relación con Proveedores

Todos los acuerdos con proveedores y prestadores de servicios deben contener cláusulas que los obliguen a cumplir con la Política de Seguridad de la Información y Ciberseguridad.

5.9 Gestión de Incidentes de Seguridad

Se deben definir procedimientos y mecanismos para la gestión de los incidentes de seguridad para minimizar su impacto. Estos deben contemplar la colaboración de áreas que puedan formar parte del proceso en las etapas de prevención, detección, contención y respuesta, así como de mejora continua y aprendizaje.

El personal debe reportar actividades sospechosas o inusuales que puedan representar una amenaza para los activos de información de Cirion, acceso no autorizado a la información de clientes o empleados, o cualquier otro incidente sospechoso de seguridad de la información.

6. Notificação de incidentes

Los incidentes pueden registrarse en la herramienta de ITSM de la compañía o notificarse a través del correo electrónico <Security.Incidents@ciriontechnologies.com>. Los incidentes clasificados como críticos deben ser comunicados de forma inmediata a los organismos reguladores competentes, mediante la plataforma oficial designada para tal fin.

En caso de que el incidente implique el compromiso de datos personales, deberán observarse y cumplirse las orientaciones y exigencias legales previstas en las leyes de protección de datos aplicables en los países donde la compañía mantiene operaciones, como, por ejemplo, la Ley General de Protección de Datos Personales (Ley nº 13.709/2018 - Brasil).

7. Contato

El conocimiento de cualquier violación de seguridad deberá ser comunicado de inmediato al superior directo (si lo hubiera) y al área de Seguridad de la Información al correo electrónico <Security.Incidents@ciriontechnologies.com>. Además, es posible utilizar el número de

teléfono del servicio de soporte, Service Desk, correspondiente al país donde la compañía mantiene operaciones.

8. Aprovações

O extrato da Política Geral de Segurança da Informação e Cibersegurança foi aprovado pelo CISO da companhia em 08/07/2025.