Extrato da Política Geral de Segurança da Informação e Cibersegurança

CIRIONTECHNOLOGIES.COM

1. Objetivo

Esta Política, bem como o corpo normativo que a desenvolve, tem como objetivo proteger os ativos de informação contra modificação, divulgação, destruição acidental ou não autorizada, bem como garantir os princípios gerais de segurança de confidencialidade, integridade e disponibilidade.

2. Referências para a elaboração deste 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
- **Resolução Anatel Nº 740**, de 21 de dezembro 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 alinhada com as principais normas globais de proteção de dados, considerando os marcos legais vigentes nos países onde a companhia mantém operações.

3. Responsabilidades

A Segurança da Informação e a Cibersegurança são responsabilidades compartilhadas por toda a organização. No entanto, a Diretoria de Cibersegurança é a área responsável por garantir a implementação, manutenção e evolução contínua das estratégias, políticas, normas e controles de segurança aplicáveis à organização.

4. Ações de conscientização

A Cirion por meio de suas políticas e procedimentos organizacionais tem por objetivo divulgar e conscientizar todos os colaboradores para a manutenção de uma estrutura sólida de segurança da informação.

Atualmente, são realizados treinamentos obrigatórios internos para disseminação e conscientização da segurança da informação. Além disso, existem campanhas que simulam riscos e ameaças à segurança. Para o público externo, são realizadas publicações em redes sociais e no site da Cirion que contemplam o tema de segurança cibernética com distintas abordagens.

5. Linhas gerais dos procedimentos e controles de segurança

5.1 Classificação e Controle de Ativos

A informação deve ser classificada de acordo com seu nível de criticidade e confidencialidade. Como resultado deste processo e de acordo com a função que desempenha, deverá ser administrada e rotulada para garantir o nível adequado de proteção e evitar sua exposição além do necessário para o desempenho normal das tarefas relacionadas à sua utilização.

5.2 Gestão de Riscos

A organização deve estabelecer um processo contínuo e sistemático de gestão de riscos de segurança da informação, conforme as melhores práticas da ISO/IEC 27001 (e normas específicas como ISO 27005). O objetivo é identificar e avaliar proativamente os riscos que possam afetar a informação e os sistemas, para tratá-los oportunamente.

5.3 Segurança Lógica e Controle de Acesso

A segurança lógica engloba mecanismos e controles para proteger sistemas de informática, aplicações e dados contra acessos não autorizados ou atividades maliciosas. Um elemento central é o controle de acesso, que garante que cada usuário ou sistema obtenha apenas as permissões necessárias para realizar suas funções, nada mais (princípio do menor privilégio).

Todos os sistemas que armazenem ou processem informação devem ter seu acesso estritamente controlado. O nível de controle de acesso exigido para um sistema que armazene ou processe informação, ou a um recurso em particular, é determinado pelo impacto potencial no negócio.

5.4 Segurança em Redes e Comunicações

A infraestrutura de redes e comunicações é a espinha dorsal sobre a qual circula a informação da empresa. Por isso, devem ser implementadas medidas de segurança para proteger as redes internas, perimetrais e as comunicações de dados contra acessos não autorizados, interceptações ou interrupções.

Os controles para gerir os riscos da informação transmitida nas redes da Cirion ou na internet devem cumprir os padrões de segurança estabelecidos.

5.5 Continuidade de Negócio e Recuperação de Desastres

Devem ser definidas medidas para assegurar a Continuidade do negócio diante de situações que afetem ou interrompam o desempenho normal dos serviços da Cirion. Isto proporciona uma estrutura sistemática para preparar-se, responder e recuperar-se de incidentes de maior escala, sejam causados por desastres naturais, falhas tecnológicas catastróficas, ciberataques de grande impacto ou outras crises.

5.6 Conformidade Regulatória e Proteção de Dados Pessoais

Devem ser identificados os requisitos legais e regulatórios em matéria de segurança da informação e proteção de dados pessoais, e garantir a incorporação desses requisitos nas políticas de segurança, no desenho e implementação dos serviços de tecnologia e práticas de auditoria. Todo o pessoal deve compreender e cumprir os termos contratuais aplicáveis.

Qualquer violação de dados pessoais deve ser notificada de forma ágil, observando as orientações e exigências legais previstas nas leis de proteção de dados aplicáveis nos países onde a companhia mantém operações.

5.7 Gestão de Vulnerabilidades

A empresa deve manter um processo estruturado de gestão de vulnerabilidades com o objetivo de reduzir os riscos associados a falhas de segurança nos ativos de informação, contemplando a identificação de vulnerabilidades, avaliação, priorização de riscos, tratamento e correção, monitoramento e documentação.

5.8 Relação com Fornecedores

Todos os contratos com fornecedores e prestadores de serviços devem conter cláusulas que os obriguem a cumprir a Política de Segurança da Informação e Cibersegurança.

5.9 Gestão de Incidentes de Segurança

Devem ser definidos procedimentos e mecanismos para gestão de incidentes de segurança para minimizar seu impacto. Devem contemplar colaboração de áreas que possam participar do processo nas etapas de prevenção, detecção, contenção e resposta, bem como de melhoria contínua e aprendizado.

O pessoal deve reportar atividades suspeitas ou incomuns que possam representar uma ameaça aos ativos de informação da Cirion, acesso não autorizado a informações de clientes ou funcionários ou quaisquer outros incidentes suspeitos de segurança da informação.

6. Notificação de incidentes

Os incidentes podem ser registrados na ferramenta de ITSM da companhia ou notificados através do e-mail <Security.Incidents@ciriontechnologies.com>. Incidentes classificados como críticos devem ser prontamente comunicados aos órgãos reguladores competentes, por meio da plataforma oficial designada para esse fim.

Caso o incidente envolva o comprometimento de dados pessoais, deverão ser observadas e seguidas as orientações e exigências legais previstas nas legislações de proteção de dados aplicáveis nos países onde a companhia mantém operações, como, por exemplo, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - Brasil).

7. Contato

O conhecimento de qualquer violação de segurança deverá ser imediatamente comunicado ao superior imediato (se houver) e a área de Segurança da Informação pelo e-mail <Security.Incidents@ciriontechnologies.com>. Além disso, é possível utilizar o telefone do serviço de suporte, Service Desk, correspondente ao país onde a companhia mantém operações.

8. Aprovações

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