CRCPR

CONSELHO REGIONAL DE CONTABILIDADE
DO PARANÁ

POLÍTICA DE SEGURANÇA CIBERNÉTICA

CRCPR
CONSELHO REGIONAL DE CONTABILIDADE
DO PARANÁ

1 - OBJETIVO

Estabelecer diretrizes, princípios e responsabilidades para a proteção dos ativos de informação, em alinhamento com a Política Nacional de Cibersegurança (Decreto nº 11.856/2023), a Convenção sobre o Crime Cibernético (Decreto nº 11.491/2023) e a Estratégia Nacional de Cibersegurança – E-Ciber (Decreto nº 12.573/2025), bem como com as demais políticas internas do CRCPR.

Para fins desta Política, consideram-se colaboradores: conselheiros, representantes, empregados, estagiários, prestadores de serviço, fornecedores, terceiros e demais pessoas que tenham acesso a informações ou sistemas do CRCPR. Visitantes deverão observar as regras de acesso e segurança enquanto permanecerem nas dependências da entidade.

Assegurar a aplicação dos princípios e mecanismos de proteção às informações institucionais e aos dados pessoais tratados pelo CRCPR. Garantir confidencialidade, integridade, autenticidade e disponibilidade das informações processadas, armazenadas e transmitidas digitalmente.

O CRCPR compromete-se a promover gestão contínua de riscos cibernéticos, prevenir e mitigar vulnerabilidades e ataques, disponibilizar os recursos necessários ao aprimoramento contínuo dos processos de segurança cibernética, garantindo um ambiente tecnológico seguro, com o menor nível de risco possível, incentivar educação, capacitação técnica em segurança cibernética.

2 - DIRETRIZES GERAIS

Esta política integra o sistema de governança, gestão de riscos, segurança da informação e proteção e dados do CRCPR, integrando-se às estratégias institucionais e aos normativos vigentes.

Para mitigar vulnerabilidades nos ativos de informação, o CRCPR adota procedimentos e controles estruturados em pilares que orientam a redução de riscos e fortalecem a proteção dos seus ambientes tecnológicos.

- Autenticação forte, criptografia e controle de acessos;
- Proteção contra softwares maliciosos (malware) e uso de EDR/antivírus corporativo;
- Gestão contínua de vulnerabilidades, incluindo análise de exposição e aplicação de patches;
- Busca proativa e antecipação de ameaças, com base em inteligência de ameaças;
- Monitoramento contínuo de redes, sistemas de detecção incluindo IDS e IPS;
- Resposta estruturada a incidentes cibernéticos;
- Segurança de aplicações, testes e conformidade com padrões seguros de desenvolvimento;
- Segmentação de rede e políticas de continuidade e contingência e backup;
- Gerenciamento seguro de terceiros e fornecedores;
- Conformidade com a classificação de informações do CRCPR;
- Revisão do Inventário de dados;
- Processos formais de comunicação de riscos e incidentes envolvendo dados pessoais;
- Treinamentos e campanhas internas contínuas

Os prestadores de serviço, fornecedores e empresas conveniadas devem adotar procedimentos e controles compatíveis com os riscos envolvidos na prestação de serviços relevantes, preservando, inclusive, a continuidade das operações e negócios do CRCPR.

As informações são classificadas de acordo com a confidencialidade e as proteções necessárias e, devem ser tratadas de forma sigilosa, de acordo com a regulamentação e a legislação vigente, observada a finalidade do tratamento. A empresa dispõe de Política de Classificação de Informações, que se aplica também a esta.

O acesso às informações só deve ser feito se devidamente autorizado, e o acesso deverá ser realizado por meio de credencial, pessoal, intransferível e identificável, conforme a Política de Segurança da Informação.

Quaisquer riscos às informações dos profissionais e empresas registrados no CRCPR devem ser comunicados diretamente à diretoria ou através dos canais de atendimento oferecidos pelo CRCPR ao público externo.

O CRCPR atuará na disseminação da cultura de segurança cibernética, incluindo a conscientização dos seus profissionais e empresas registradas.

A efetividade da Política de Segurança Cibernética é verificada por meio de avaliações independentes periódicas de auditoria interna e externa, incluindo órgãos de controle e reguladores.

Na promoção da transparência em alinhamento com os princípios de acesso à informação e garantia de direitos fundamentais, ficam disponibilizadas no site do CRCPR as orientações de segurança da informação, cibersegurança e proteção de dados.

3 - REVISÃO

Esta Política deverá ser revisada, pelo Comitê de Tecnologia e Segurança da Informação, coordenada pela Gerência Operacional com o apoio da equipe de TIC, sempre que houver alterações relevantes na legislação, infraestrutura tecnológica, riscos institucionais ou normativos relacionados, e sua aprovação caberá ao plenário do CRCPR.

4 - RESPONSABILIDADE

Todos os colaboradores, são responsáveis por zelar pela segurança cibernética e pela proteção das informações às quais têm acesso ao utilizar a rede institucional. Para tanto, comprometem-se a cumprir integralmente esta Política de Segurança Cibernética. Os contratos firmados pelo CRCPR com terceiros incluem cláusulas específicas que asseguram a confidencialidade das informações protegidas por sigilo, bem como o atendimento às legislações e regulamentações vigentes aplicáveis.

5 - MEDIDAS DISCIPLINARES

O descumprimento das diretrizes aqui estabelecidas nesta Política poderá ensejar em medidas disciplinares, administrativas ou contratuais, conforme legislação aplicável.

CRCPR

CONSELHO REGIONAL DE CONTABILIDADE
DO PARANÁ

crcpr.org.br