Segurança Cibernética

A "*Política de Segurança Cibernética*" foi constituída com base nos princípios e diretrizes buscando assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Esta mesma política é revisada e aprovada anualmente a promover a continuidade de seus princípios.

Objetivo

Possibilitar o gerenciamento da segurança da CREDI-SHOP, estabelecendo regras e padrões para proteção da informação, estabelecendo diretrizes necessárias para definição e implementação de mecanismos que guiarão e suportarão as atividades relativas à Segurança Cibernética.

A quem destina/Público-Alvo

A todos que devem ter conhecimento sobre suas responsabilidades a estar em conformidade com a política, normas e procedimento de segurança da informação e que estes possam colaborar com a proteção das informações.

Diretrizes da Segurança Cibernética

1. **Confidencialidade e Responsabilidade:** Todos que possuem relacionamento com a CREDI-SHOP possuí contrato de confidencialidade e responsabilidade;
2. **Treinamento e Conscientização:** Prover treinamento de segurança cibernética a todos colaboradores, prestadores de serviços e terceiros, assim como disseminar a cultura de segurança cibernética e informações a usuários finais sempre que necessário;
3. **Classificação da Informação:** Toda informação criada, obtida, de clientes e/ou empresas parceiras deve ser classificada conforme o seu nível de confidencialidade e receber o tratamento adequado com base em sua classificação (confidencial / interna / pública);
4. **Cópias de Segurança:** As informações utilizadas nas operações da CREDI-SHOP devem possuir cópias de segurança, bem como obedecer aos critérios de proteção em função da criticidade das informações nelas contidas, atender aos requisitos operacionais, legais, históricos e de auditoria.
5. **Resposta a Incidente:** A CREDI-SHOP provê mecanismos e canais de comunicação para que todo e qualquer incidente de segurança ou qualquer constatação de não aderência as normas, políticas e boas práticas de segurança cibernética sejam reportadas.
6. **Controle de Perímetro de Segurança:** Os ativos da CREDI-SHOP são mantidos em áreas seguras, segregados, protegidas por perímetro de segurança definido, com barreiras apropriadas e recursos para controle de acesso lógico e físico.
7. **Gerenciamento Vulnerabilidade:** Periodicamente é realizado testes e varreduras de identificação e correção de vulnerabilidades no ambiente da CREDI-SHOP;
8. **Proteção Software Malicioso:** Todos os dispositivos da CREDI-SHOP possuem programa de proteção contra software malicioso;
9. **Autenticação:** Todos os colaboradores, prestadores de serviços e terceiros é identificado por identificador único ("nome de usuário" ou "login");

10. **Controle de Acesso:** O acesso às informações e sistemas são realizados por meio de autorização do gestor respeitando segregação de função;
11. **Vazamento da Informação:** A CREDI-SHOP possuí política estabelecendo boas práticas quanto ao uso do correio eletrônico, transferência, afastamento e desligamento de colaboradores, prestadores de serviços e terceiros, dos procedimento e responsabilidades para gestão e operação dos recursos de processamento das informações;
12. **Rastreabilidade:** Os sistemas da CREDI-SHOP possuem trilhas de auditoria habilitadas;
13. **Continuidade do Negócio:** A CREDI-SHOP possui recursos que possibilitam a continuidade das operações.