



Visão Geral do Programa de Segurança do Sistema de Informação



MINT



Índice

| | | |
|-------|---|---|
| 1. | Objetivo | 3 |
| 2. | Organização da Segurança da Informação | 3 |
| 3. | Elementos de Segurança da Informação | 3 |
| 3.1. | Programa Escrito..... | 3 |
| 3.2. | Análise de Risco e Segurança | 4 |
| 3.3. | Plano de Resposta a Incidente..... | 4 |
| 3.4. | Conscientização e Treinamento de Segurança | 4 |
| 3.5. | Plano de Continuidade de Negócios / Recuperação de Desastre..... | 4 |
| 3.6. | Garantia de Segurança | 5 |
| 3.7. | Medidas de Proteção e Detecção contra Ameaças e Vulnerabilidades Identificadas..... | 5 |
| 3.8. | Comunicação ao Conselho de Administração | 5 |
| 3.9. | Ciber-seguro | 5 |
| 3.10. | Ciberataques..... | 5 |
| | Apêndice A – Controle de Alterações | 6 |

1. Objetivo

A Política (“Política”) de Segurança da Informação da Cantor (“Grupo”) é um componente crítico necessário que visa permitir e assegurar a confidencialidade, integridade e disponibilidade dos dados e ativos do cliente e da empresa. Além de prever, detectar e reduzir vulnerabilidades, representa a estratégia fundamental incorporada pelo Grupo para alcançar os objetivos de Segurança da Informação. Este documento define esse nível de cuidado.

2. Organização da Segurança da Informação

O Grupo é liderado pelo Diretor de Segurança da Informação (CISO – *Chief Information Security Officer*), o qual é a autoridade aprovadora para todas as questões envolvendo segurança da informação. O CISO proporciona governança do programa da organização de segurança da informação, estabelece e mantém normas, diretrizes e procedimentos que formam a estrutura de controles do programa de segurança. O Grupo trabalha em conjunto com a Tecnologia da Informação (“TI”), Auditoria, Recursos Humanos (“RH”), Departamento de Conformidade (“Conformidade”) e com a Equipe Executiva para garantir aderência e esta Política.

Governança, Risco e Conformidade: Mantêm a postura do risco de ciber-segurança da organização através da avaliação e análise contínua de riscos aos negócios de práticas internas, fornecedores e parceiros. Comunica-se com equipes de segurança do cliente, Auditoria Interna, Conformidade e órgãos reguladores, comunicando nosso perfil de risco e eficiência do programa de segurança. Garantem que investidores-chave tenham as informações que precisam para tomarem as melhores decisões de risco.

Operações de Segurança e Inteligência: Colaboram com parceiros de segurança da indústria e analisam ameaças, garantindo uma postura de ciber-defesa proativa. Coletam e processam dados de eventos de segurança a partir de aplicativos e infraestrutura para identificar ameaças internas e externas ao Grupo. Reagem rapidamente aos incidentes de segurança para minimizar o impacto sobre a entrega de serviços. Avaliam continuamente e aprimoram ciber-defesas para contra-atacar ciber-ameaças em constante evolução.

Segurança e Engenharia de Produto: Trabalham com a organização de Desenvolvimento de Produto para assegurar que controles e recursos de segurança estejam integrados desde o começo a produtos e/ou serviços desenvolvidos internamente e durante o ciclo de vida do produto e/ou serviço visando evitar vulnerabilidades de segurança frente a ameaças.

3. Elementos de Segurança da Informação

3.1. Programa Escrito

O Programa de Segurança dos Sistemas de Informação é regido por uma política em linha com a Estrutura de Ciber-Segurança NIST e por uma série de normas e diretrizes em linha com NIST-800.

3.2. Análise de Risco e Segurança

A postura de risco de ciber-segurança é mantida por meio de avaliação contínua e análise de risco aos negócios a partir de práticas internas, fornecedores e parceiros. Comunicando as equipes de segurança do cliente, Auditoria Interna, Conformidade e órgãos reguladores, nosso perfil de risco e eficácia do programa de segurança.

Áreas-chave que são avaliadas incluem:

- a) Maturidade organizacional
- b) Eficácia de controle
- c) Gerenciamento de Risco de Terceiro

As informações são coletadas e analisadas para auxiliar em tomada de decisões.

3.3. Plano de Resposta a Incidente

A BGC desenvolveu procedimentos de resposta a incidente a fim de efetivamente abordar eventos e incidentes de segurança. O plano foca nas fases primárias de resposta a incidente incluindo detecção, análise, contenção, erradicação e recuperação. O plano também descreve uma matriz de escalonamento de incidente, que detalha os procedimentos de notificação apropriados com base na gravidade do incidente.

A BGC fornecerá, imediatamente, notificação NFA em caso de um incidente de ciber-segurança referente aos seus negócios e que resulte em: 1) qualquer perda de fundos de cliente ou contraparte; 2) qualquer perda de capital próprio do Membro; ou 3) o Membro dando notificação aos clientes ou contrapartes sob lei estadual ou federal. A notificação ocorrerá uma vez que BGC tenha confirmado o impacto do incidente.

3.4. Conscientização e Treinamento de Segurança

Todos os colaboradores participam do treinamento em segurança da informação e conscientização sobre tópicos tais como engenharia social, *phishing* e melhores práticas de uso aceitável. Treinamento dado e suprido mediante a contratação de novos colaboradores, bem como de consultores, anualmente.

3.5. Plano de Continuidade de Negócios / Recuperação de Desastre

Mantemos plano de continuidade de negócios comprehensivo e flexível para garantir que funções-chave possa reiniciar operações de forma oportuna em caso de interrupção dos negócios. Mantemos plano de Recuperação de Desastre para nossos aplicativos mais críticos. Os Planos são revisados anualmente a menos que alterações organizacionais significativas ou outras exijam revisão antecipada. Anualmente, executamos testes de componente de nossa infraestrutura de DR e outros testes maiores (como teste de isolamento da central de dados) em parceira com a comunidade usuária dos negócios. Para sistemas de TI, a meta do tempo de recuperação é dentro de 4 horas. Suporte ao cliente está sujeito a arranjos de contingência que garantem que o suporte será contínuo usando nossa interoperabilidade global entre equipes em múltiplos locais.

3.6. Garantia de Segurança

O cenário da segurança muda rapidamente, o que significa que nosso programa e controles de apoio precisam ser regularmente avaliados quanto à eficácia. Tais atividades incluem revisões técnicas e não técnicas, varreduras de vulnerabilidade e teste de penetração.

3.7. Medidas de Proteção e Detecção contra Ameaças e Vulnerabilidades Identificadas

O grupo faz uso de várias salvaguardas para proteger os ativos críticos, incluindo, entre outros:

- a) Controles de segurança física
- b) Criptografia de dados
- c) Detecção de potenciais ameaças
- d) Coleta e Análise de Ameaças
 - i. Controles de acesso com base no princípio do menor privilégio
- e) Ferramentas de prevenção de perda de dados
- f) Controles de filtro de Internet
- g) Varredura de vulnerabilidade e gerenciamento de patch
- h) Restrição de acesso à mídia removível
- i) Restrição de software não autorizado
- j) Restrição de dispositivos móveis

3.8. Comunicação ao Conselho de Administração

Reportamos ao nosso Conselho de Administração sobre o status do ISSP anualmente. Tópicos cobertos incluem novas iniciativas, tendências, bem com o status das metas estabelecidas no ano anterior.

3.9. Ciber-segurança

Mantemos uma política de ciber-segurança.

3.10. Ciberataques

Não temos sofrido qualquer Ciberataque Sev1 ou Sev2 no último ano.

Apêndice A – Controle de Alterações

Esta seção deve ser preenchida para todas as alterações a este documento e apoiadas e evidenciadas pela assinatura do Proprietário.

| Nº da Versão | Autor | Resumo das alterações | Data de Aprovação | Aprovado por |
|--------------|----------------------|---|-------------------|------------------|
| 1.0 | CPowell | Emissão Inicial | Junho/2016 | DStern |
| 2.0 | CPowell | Revisão Menor | Julho/2017 | DStern |
| 2.1 | CPowell | Revisão Anual | Janeiro/2018 | DStern |
| 3 | CPowell | Revisão Anual / Alterações Menores | Dezembro/2018 | DStern |
| 4 | DStern | Revisão Anual e melhorias para se adequar as últimas notificações NFA | Dezembro/2019 | DStern |
| 5 | MEI Lakkis & CPowell | Revisão Anual / Alterações Menores | Novembro/2020 | MEI Lakkis |
| 6 | MEI Lakkis & CPowell | Validação de versão | Abril/2022 | Glauco Nicoletti |