POLÍTICA DE SEGURANÇA CIBERNÉTICA

GREENBAY INVESTIMENTOS LTDA

MARÇO 2022 – VERSÃO 1.1

SUMÁRIO

1. OBJETIVO E ABRANGÊNCIA 3
2. MODELO ADOTADO 3
3. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA 4
   - 3.1 Identificação e avaliação dos riscos (risk assessment) 4
   - 3.2 Ações de prevenção e proteção 5
   - 3.3 Monitoramento e testes 6
   - 3.4 Plano de resposta 6
   - 3.5 Reciclagem e revisão 7
4. VIGÊNCIA E ATUALIZAÇÃO 7

1. OBJETIVO E ABRANGÊNCIA

1.1 A Política de Segurança Cibernética ("Política") da GREENBAY INVESTIMENTOS LTDA ("Gestora") visa estabelecer as diretrizes necessárias para proteger as informações de sua propriedade e/ou sob sua guarda, assegurando a integridade, privacidade, confidencialidade e disponibilidade dos dados e sistemas de informação utilizados.

1.2 Esta Política aplica-se a todos os sócios, diretores, funcionários, trainees e estagiários da Gestora (em conjunto os "Colaboradores" e, individualmente, o "Colaborador"), prestadores de serviços, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Gestora, ou que a Gestora acesse informações a ela pertencentes.

1.3 Todo e qualquer usuário de acessos computadorizados ou digitais da Gestora tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

1.4 O responsável pelo cumprimento das regras e procedimentos de segurança cibernética é a Diretora de Riscos e *Compliance*.

2. MODELO ADOTADO

2.1 A Gestora optou por não manter time próprio dedicado à segurança cibernética, contingência e outros assuntos relacionados à tecnologia da informação, inclusive para realização de tarefas de suporte (instalações, substituições e configurações), verificações e manutenções periódicas.

2.2 Assim sendo, para implementação e monitoramento da presente Política, a Gestora conta com o suporte e assessoria de empresa terceirizada.

2.3 Os temas relacionados à segurança cibernética serão tratados trimestralmente no Comitê de Riscos e *Compliance*, de forma ordinária, ou mesmo em reunião específica, em casos de eventos extraordinários, para que sejam tomadas de forma tempestiva medidas de recuperação, limitação de danos, e resposta relevante.

3. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

3.1 Identificação e avaliação dos riscos (risk assessment)

3.1.1 No exercício das suas atividades, a Gestora poderá estar sujeita a riscos cibernéticos que ameacem a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Entre os riscos mais comuns, estão:

Malwares: *softwares* desenvolvidos para corromper computadores e redes:

Vírus: *software* que causa danos à máquina, rede, outros softwares e bancos de dados;

Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador;

Spyware: *software* malicioso para coletar e monitorar o uso de informações; e

Ransomware: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoas e número de cartão de crédito:

Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;

Phishing: *links* transmitidos por *e-mails*, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e

Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços; e

Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

3.2 *Ações de prevenção e proteção*

3.2.1 Com a finalidade de mitigar os riscos cibernéticos e proteger seus sistemas, informações, base de dados, equipamentos e o andamento dos seus negócios, a Gestora adota as seguintes medidas de prevenção e proteção:

(i) Controle de acesso adequado aos ativos da Gestora, por meio de procedimentos de identificação, autenticação e autorização dos usuários, ou sistemas, aos ativos da Gestora;

(ii) Estabelecimento de regras mínimas (complexidade, periodicidade e autenticação de múltiplos fatores) na definição de senhas de acesso a dispositivos corporativos, sistemas e rede em função da relevância do ativo acessado. Além disso, os eventos de *login* e alteração de senha são auditáveis e rastreáveis;

(iii) Limitação do acesso de cada Colaborador a apenas recursos relevantes para o desempenho das suas atividades e restrição do acesso físico às áreas com informações críticas/sensíveis;

(iv) Proteção por meio de aplicação de rede virtual privada (VPN) para atividades realizadas de forma remota;

(v) Rotinas de *backup*;

(vi) Criação de *logs* e trilhas de auditoria sempre que permitido pelos sistemas;

(vii) Realização de diligência na contratação de serviços de terceiros, caso necessário, e prezando, pela celebração de acordo de confidencialidade e exigência de controles de segurança na própria estrutura dos Terceiros;

(viii) Implementação de recursos *anti-malware* em estações e servidores de rede, como antivírus e *firewalls* pessoais; e

(xix) Restrição à instalação e execução de *softwares* e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de *allow listing*).

3.3 Monitoramento e testes

3.3.1 A Gestora possui mecanismos de monitoramento das ações de proteção implementadas, para garantir seu bom funcionamento e efetividade.

3.3.2 Nesse sentido, a Gestora mantém inventários atualizados de *hardware* e *software*, bem como realiza verificações periódicas, no intuito de identificar elementos estranhos à Gestora, como computadores não autorizados ou *softwares* não licenciados.

3.3.3 Além disso, a Gestora mantém os sistemas operacionais e *softwares* de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. As rotinas de *backup* são monitoradas diariamente, com a execução de testes regulares de restauração dos dados.

3.3.4 São realizados, periodicamente, testes de invasão externa, bem como análises de vulnerabilidades na estrutura tecnológica, sempre que houver mudança significativa em tal estrutura.

3.3.5 Ainda, a Gestora analisa regularmente os *logs* e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos.

3.4 Plano de resposta

3.4.1 Caso seja identificado um potencial incidente relacionado à segurança cibernética, a Diretora de Riscos e *Compliance* deverá ser imediatamente comunicada.

3.4.2 Num primeiro momento, a Diretora de Riscos e *Compliance* se reunirá com os demais diretores da Gestora para compreender o evento ocorrido, os motivos e consequências imediatas, bem como a gravidade da situação.

3.4.3 Caso os diretores avaliem que o incidente ocorrido pode gerar danos iminentes à Gestora, serão tomadas, em conjunto com os assessores de tecnologia da informação da Gestora, as medidas imediatas de segurança cibernética cabíveis, que podem incluir a redundância de TI, redirecionamento das linhas de telefone para os celulares, instrução do provedor de telefonia para que desvie linhas de dados e e-mails, entre outros.

3.4.4 Na hipótese de o incidente comprometer, dificultar ou mesmo impedir a continuidade das operações da Gestora, serão observados os procedimentos previstos no plano de continuidade do negócio da Gestora.

3.4.5 Além disso, os diretores avaliarão a pertinência da adoção de medidas como (i) registro de boletim de ocorrência ou queixa crime; (ii) comunicação do incidente aos órgãos regulatórios e autorregulatórios; (ii) consulta com advogado para avaliação dos riscos jurídicos e medidas judiciais cabíveis para assegurar os direitos da Gestora.

3.5 *Reciclagem e revisão*

3.5.1 A Gestora manterá o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

4. VIGÊNCIA E ATUALIZAÇÃO

4.1 Esta política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

Versão	**Data**	**Alteração**	**Responsável**
1.0	Outubro/2020	Versão Original	Diretora de Riscos e *Compliance*
1.1	Março/2022	Revisão	Diretora de Riscos e *Compliance*