POLÍTICA DE SEGURANÇA CIBERNÉTICA

PNCA ADMINISTRAÇÃO DE RECURSOS LTDA.

DEZEMBRO/2024

www.pncainvestimentos.com.br
Avenida das Américas, 4200, Bloco 01, Sala 305 - Centro Empresarial Barra Shopping, Barra da Tijuca, Rio de Janeiro/RJ CEP: 22640-907

1. DO OBJETO

A presente Política dispõe acerca das regras e procedimentos para o programa de segurança cibernética, visando a:

- Garantir a confidencialidade, integridade e disponibilidade das informações da PNCA Administração e de informações de terceiro por ela administrada, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;

- Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;

- Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;

- Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;

- Conscientizar, educar e treinar os colaboradores por meio de normas e procedimentos internos aplicáveis as suas atividades diárias; e

- Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

2. CONCEITOS

A Segurança Cibernética constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos. Seguem alguns conceitos:

- Confidencialidade: garantia de que a informação é acessível somente as pessoas autorizadas.

- Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

www.pncainvestimentos.com.br
Avenida das Américas, 4200, Bloco 01, Sala 305 - Centro Empresarial Barra Shopping, Barra da Tijuca, Rio de Janeiro/RJ CEP: 22640-907

- Riscos Cibernéticos: Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

- Malwares:

  - Vírus: software que causa danos a máquina, rede, softwares e banco de dados;

  - Cavalo de Troia: 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;

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

- Engenharia Social:

  - 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;

  - 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.

- Fraudes externas e invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

- Ataques DDoS 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 enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

3. O PROGRAMA DE SEGURANÇA CIBERNÉTICA.

A **PNCA Administração** estruturou um programa baseado em cinco principais funções contra ataques cibernéticos. O programa foi desenhado em conjunto entre a empresa de

www.pncainvestimentos.com.br
Avenida das Américas, 4200, Bloco 01, Sala 305 - Centro Empresarial Barra Shopping, Barra da Tijuca, Rio de Janeiro/RJ CEP: 22640-907

tecnologia de informação que presta serviços para a **PNCA Administração** e a área de risco e Compliance, e nos termos do guia de segurança cibernética da ANBIMA.

- Identificação/avaliação de riscos (risk assessment): A **PNCA Administração** deverá identificar os riscos internos e externos, os ativos de hardware e software e processos que precisam de proteção. O Guia de Segurança Cibernética da ANBIMA definiu que os ataques mais comuns de criminosos cibernéticos (*cybercriminals*) são os seguintes:

    - Malware (e.g. vírus, cavalo de troia, spyware e ransomware);
    - Engenharia Social; Pharming; Phishing scam; Vishing; Smishing;
    - Acesso pessoal;
    - Ataques de DDoS e botnets; e
    - Invasões (advanced persistent threats).

- Ações de prevenção e proteção: A **PNCA Administração** estabelece um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles.

    - O acesso aos diversos serviços de informática, como sistemas, e-mail, rede local, entre outros, ocorre mediante autenticação do usuário através de seu nome de usuário (login) e senha (password).
    - Os notebooks utilizados pela equipe da **PNCA Administração** estão configurados para uso pessoal, sem chave de criptografia.
    - Aparelhos "mobiles" com a configuração de acesso aos e-mails podem ser bloqueados ou mesmo "resetados" pela equipe de TI remotamente.
    - Os arquivos contendo informações relacionadas à empresa e as suas atividades são armazenados em um servidor de arquivos que é restrito, de acordo com a definição dos grupos de segurança definidos pelos gestores de TI;
    - O sistema de correio eletrônico utilizado pela empresa, bem como os endereços atribuídos aos usuários, é exclusivamente para uso profissional e, portanto, relacionados às atividades da empresa;
    - Os acessos externos à rede interna da **PNCA Administração** somente poderão ser feitos com a utilização de clientes VPN que estabelecem a conexão segura entre as partes;
    - Todos os equipamentos de TI (desktops, notebooks, impressoras, redes sem fio, etc) são devidamente registrados, e utilizando-se somente softwares licenciados e protegidos por senhas;
    - Todos as estações de trabalho contam com solução de proteção antivírus.

- Monitoramento e testes: A **PNCA Administração** realiza testes periódicos para detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e

www.pncainvestimentos.com.br
Avenida das Américas, 4200, Bloco 01, Sala 305 - Centro Empresarial Barra Shopping, Barra da Tijuca, Rio de Janeiro/RJ CEP: 22640-907

identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados. Incluem-se, alguns parâmetros:

- verificação dos logins dos colaboradores;
- alteração periódica de senha de acesso dos colaboradores;
- segregação de acessos;
- manutenção trimestral de todo os hardwares;
- Rotinas de backup: (i) versionamento dos arquivos de aproximadamente 30 dias nos próprios servidores, sendo executado duas vezes ao dia; (ii) backup diário realizado na plataforma Microsoft Onedrive (nuvem) onde os backups são armazenados em datacenters redundantes no EUA.

Obs.: Os sistemas, serviços, dados, informações (incluindo as Informações Sigilosas) disponíveis na **PNCA Administração** ou por esta disponibilizados para serem usados pelos colaboradores não devem ser interpretados como sendo de uso pessoal. Todos os colaboradores têm ciência de que o uso está sujeito à monitoramento periódico, inclusive em equipamentos pessoais acessados durante o horário de trabalho, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pela Área de Gestão de Riscos e de Compliance e/ou por prestador de serviços externo.

- Criação do plano de resposta: A **PNCA Administração** possui um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário.

  Para efeito desta política, um incidente de segurança é definido como qualquer evento adverso, decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades, relacionado à segurança de um ativo que pode prejudicar quaisquer princípios da Segurança da Informação.

  Toda ocorrência, bem como as informações recebidas de terceiros, deverá ser avaliada pela equipe de Tecnologia da Informação para a determinação da criticidade e impacto causados nas operações.

  Uma vez que a equipe de Tecnologia da Informação tenha sido acionada devido a um potencial incidente, este deverá convocar Comitê Executivo da Arena Capital.

  Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento. Na hipótese de vazamento de Informações sigilosas ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Em caso de necessidade, poderá ser contratada empresa especializada para combater ao evento identificado.

Caso o evento tenha sido causado por algum colaborador, deverá ser avaliada a sua culpabilidade, nos termos da Política de Compliance e Código de Ética e Conduta.

Eventos que envolvam a segurança das informações sigilosas ou que sejam decorrentes de quebra de segurança cibernética deverão formalizados em relatório para deliberação durante o Comitê de Compliance. O evento ocorrido, e quanto as medidas corretivas adotadas e a deliberação do comitê deverão, ainda que sumariamente, constar no Relatório de Controles Internos.

- Reciclagem e revisão: A **PNCA Administração** mantém o programa de segurança cibernética continua e/ou anualmente atualizado, conforme aplicável, identificando novos riscos, ativos e processos e reavaliando os riscos residuais, através de:

  - Acompanhamento periódico com as equipes e estações de trabalho para manter os sistemas atualizados.
  - Orientação para conservação e manutenção de equipamentos.
  - Troca e manutenção sustentável dos equipamentos visando não somente a performance da equipe, mas também descarte/troca consciente.

4. CONSIDERAÇÕES FINAIS

Todas as dúvidas sobre as diretrizes desta Política podem ser esclarecidas com a área de Compliance através do e-mail: contato@arenainvestimentos.com.br

5. CONTROLE DE VERSÕES

- **Versão**
  Data: 12/12/2024

www.pncainvestimentos.com.br
Avenida das Américas, 4200, Bloco 01, Sala 305 - Centro Empresarial Barra Shopping, Barra da Tijuca, Rio de Janeiro/RJ CEP: 22640-907