POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SPN Gestão de Investimentos ltda.

Dez/2024

R. Amauri, 255, 9° andar 01448.000 Jardim Europa, São Paulo, SP, Brasil (5511) 3019.2800

1. INTRODUÇÃO

A Política de Segurança da Informação tem por objetivo estabelecer as regras, procedimentos e controles da GESTORA para proteger as informações sob sua guarda ou de sua propriedade, garantindo que os recursos computacionais e os registros sejam, disponíveis, íntegros, confidenciais, legais, autênticos e auditáveis, de acordo com as leis, regulamentações e autorregulamentações aplicáveis.

São considerados para essa Política todos os programas de informática desenvolvidos pela própria equipe da GESTORA, ou exclusivamente para a GESTORA, tais como e-mails, sistemas instalados nos computadores de propriedade da GESTORA, bem como bancos de dados que a GESTORA utilize para o armazenamento de suas informações.

Os equipamentos e computadores de propriedade da GESTORA, bem como os bancos de dados utilizados pela GESTORA, que forem disponibilizados aos Integrantes GESTORA deverão ser utilizados de forma a atender exclusivamente às finalidades sociais da GESTORA.

Assim sendo, a presente Política deverá ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício, societário ou prestação de serviços.

2. CLASSIFICAÇÃO DOS DADOS

Toda classificação de dados deve ser realizada quando a informação for gerada ou, sempre que necessário, em momento posterior. É preciso saber claramente quais são os dados que estão sendo manipulados e o seu propósito, além de garantir a sua proteção.

O nivelamento da classificação aprovado pelo Comitê de Risco e Compliance, se apresenta da seguinte maneira:

- **Público** - todo o conteúdo de todos os documentos é visualizado por qualquer colaborador da GESTORA.
- **Restrito** - o acesso ao conteúdo é restrito a determinadas áreas ou funções dentro da GESTORA.
- **Sigiloso** - o acesso ao conteúdo é exclusivo às pessoas a quem for atribuída permissão específica.

Grau de sigilo	Impacto causado pela quebra da confiabilidade
Público	Sem impacto
Restrito	Dano médio, podendo ocasionar dano colateral não desejado
Sigiloso	Dano grave/severo, podendo causar sérios danos à instituição (afetando a imagem, gerar prejuízo financeiro, impactar nas operações e inviabilizar objetivos estratégicos).

Como parte do processo de manter o acesso adequado às informações, a Gestora desenvolveu o Mapa de Acessos, documento em que são elencadas todas as pastas disponíveis na rede interna e os respectivos Grupo de Sócios e Colaboradores que podem acessá-las, de acordo com a classificação dos dados disponíveis na pasta e função desempenhada na SPN.

Para a realização da classificação devem ser considerados quatro aspectos importantes, são eles:

- **Integridade** - informação atualizada, completa e mantida por pessoal autorizado.
- **Disponibilidade** - disponibilidade constante e sempre que necessário para pessoal autorizado.
- **Valor** - a informação deve ter um valor agregado para a instituição.
- **Confidencialidade** - acesso exclusivo por pessoal autorizado.

A revisão do mapa ocorre semestralmente, ou quando se fizer necessário.

3. RISCO

A GESTORA entende que o gerenciamento dos riscos em segurança da informação é um processo cíclico e dinâmico que requer uma constante participação de todas as pessoas. Devido ao fato de ser um processo cíclico, está em constante evolução e aprimoramento mediante a comparação dos resultados do processo com os resultados esperados e realização de ajustes para melhorar os resultados.

O processo de gerenciamento do risco está baseado nas seguintes etapas:

- Identificação dos ativos críticos;
- Levantamento e avaliação dos riscos associados a esses ativos;
- Criação de um plano para o tratamento desses riscos;
- Execução do plano de tratamento de riscos.

O processo é cíclico, no sentido de que, após a execução do plano de tratamento de riscos, o novo nível de risco deve ser comparado com o nível avaliado inicialmente.

A informação resultante dessa comparação deve ser utilizada para iniciar novamente o processo.

O processo é dinâmico também no sentido de que os ativos críticos de informação mudam ao longo do tempo e, portanto, devem ser avaliados periodicamente para manter a sua identificação atualizada com os processos de negócio.

4. TESTES DE PENETRAÇÃO REGULARES DE SEGURANÇA

A realização de testes de penetração (pentests) na GESTORA, tem como objetivo identificar e corrigir vulnerabilidades de segurança em sistemas, redes e aplicações.

Planejamento e Escopo:

- Definir o escopo do pentest, incluindo os sistemas, redes e aplicações a serem testados.
- Estabelecer os objetivos do pentest, como identificar vulnerabilidades críticas, avaliar a eficácia dos controles de segurança e testar a resposta a incidentes.
- Obter aprovação formal do escopo e dos objetivos do pentest pelo Comitê de Risco e Compliance.

Responsabilidades

- **Comitê de Risco e Compliance**:
  - Aprovar o escopo e os objetivos dos pentests.
  - Revisar e aprovar os relatórios de pentest e os planos de ação para mitigação de vulnerabilidades.

- **Departamento de TI**:
  - Coordenar a execução dos pentests e garantir a conformidade com as políticas de segurança.
  - Implementar as correções e realizar testes de verificação das vulnerabilidades identificadas.
- **Provedores de Pentest**:
  - Conduzir os testes de penetração de acordo com o escopo e os objetivos definidos.
  - Fornecer relatórios detalhados e recomendações para mitigação das vulnerabilidades.

5. ESTRUTURA ORGANIZACIONAL

5.1 COMITÊ DE RISCO E COMPLIANCE

5.1.1 Responsabilidades

- Discutir, elaborar e aprovar as políticas, normas e procedimentos gerais relacionados à Segurança da Informação;
- Designar, definir ou alterar as atribuições da função de Segurança da Informação;
- Analisar os riscos identificados e aprovar os controles requeridos para o tratamento de tais riscos.
- Apoiar a implantação de soluções para eliminação ou minimização dos riscos;
- Estabelecer uma relação consistente das estratégias de negócios e da Tecnologia da Informação com os aspectos de segurança;
- Gerenciar a realização de Análise Crítica do SGSI (Sistema de Gestão de Segurança da Informação);
- Tratar todos os assuntos relacionados à segurança;
- Definir responsabilidades e autoridades relacionadas a ela;
- Definir necessidades para os negócios da GESTORA, no aspecto da Segurança;
- Comunicar aos componentes da estrutura organizacional da GESTORA quanto à importância de atender aos objetivos e requisitos legais relacionados ao SGSI.
- Garantir o atendimento às políticas de gestão e aos objetivos do SGSI;
- Aprovar as iniciativas para a melhoria contínua do Sistema;
- Prover recursos para a gestão, operação e monitoramento adequado das atividades do SGSI;
- Suportar perante toda a organização as iniciativas da função de Segurança da Informação;
- Garantir a contínua manutenção da Política de Segurança da Informação;
- Garantir a contínua análise e realimentação dos resultados da gestão de riscos ao SGSI.

R. Amauri, 255, 9° andar 01448.000 Jardim Europa, São Paulo, SP, Brasil (5511) 3019.2800

Faz parte do comprometimento do Comitê de Segurança as aprovações dos documentos oriundos do SGSI, aprovação de aquisição de recursos para a melhoria do Sistema e clareza dos objetivos do SGSI através da Política de Segurança da Informação.

Eventualmente, para reforçar esse comprometimento, e-mails oriundos do Comitê de Segurança podem ser enviados à corporação.

O **Comitê do SGSI** é responsável por definir as medidas disciplinares cabíveis em caso de não cumprimento das políticas e procedimentos da Segurança da Informação.

A **Diretoria de Risco e Compliance** é responsável por rever o impacto trabalhista do Framework de Segurança para os funcionários, contratados, terceirizados, trabalhadores temporários e aqueles designados por terceiros para executar trabalhos nas instalações da GESTORA.

O **Comitê do SGSI** é responsável por rever os aspectos legais do Framework de Segurança e, quando necessário, prover o suporte legal para a função de Segurança da Informação nos tratamentos aos incidentes entre outros.

Adicionalmente, **o Comitê do SGSI** é responsável por garantir que o Framework de Segurança esteja em conformidade com as leis e requerimentos regulatórios e informar quando for necessário a inclusão de novos controles para cumprimento de leis e regulamentações, de acordo com o escritório jurídico definido para o apoio à decisão. Especificamente, também é responsável pela identificação de requerimentos legais e regulatórios relacionados com a proteção da privacidade.

O **Security Officer** é responsável pela segurança da informação e deve assegurar o gerenciamento adequado do SGSI para a GESTORA.

A **Área de TI** é responsável pela identificação, apresentação, sustentação, escolha, implantação e manutenção dos controles tecnológicos que apoiam a proteção da informação de todos os departamentos dentro da GESTORA. A sua atuação é vital para a Segurança da Informação e deve estar alinhada com os objetivos de cada um dos departamentos e com os objetivos do negócio.

5.2 SECURITY OFFICER

5.2.1 Responsabilidades

- Produzir diretivas de segurança, regras e padrões a serem usados pelos colaboradores. Estes padrões de segurança local devem levar em conta aspectos como, por exemplo:
    - Necessidades dos negócios da GESTORA;
    - Regulamentações e leis locais;
    - Padrões de Segurança alinhados pelo Comitê de Segurança de acordo com os requisitos e necessidades de Segurança da Informação da GESTORA;
- Desenvolver e promover programas de conscientização de segurança;
- Garantir que todos os gestores estejam cientes de suas próprias responsabilidades relacionadas à Segurança da Informação;
- Certificar-se que o processo de Gestão de Pessoas leva em conta os aspectos de Segurança da Informação ao contratar novos empregados ou em rescisão de contratos de trabalho;
- Revisar periodicamente o nível de segurança de sistemas internos, emitindo avisos após estas revisões. Analisar criticamente, em intervalos periódicos, o progresso dos planos de melhoria resultantes em conjunto com os gestores envolvidos;
- Manter-se atualizado com relação à tecnologia, legislação e novas ameaças;
- Analisar criticamente os incidentes de segurança mais significativos e gerenciar e/ou acompanhar as ações relacionadas à sua solução. Qualquer incidente de segurança mais importante deve resultar em uma análise realizada sob a autoridade do Security Officer;
- Representar a empresa, interna e externamente, nos assuntos relacionados ao SGSI;
- Gerenciar os processos do SGSI, na busca da melhoria contínua e alinhamento com a Diretoria;
- Realizar a coleta de dados e informações para a realização da Análise Crítica pelo Comitê de Segurança;
- Dar retorno dos resultados das análises críticas feitas pela direção, aos envolvidos visando providências;
- Acompanhar o sistema de ações corretivas e preventivas do SGSI;
- Garantir a contínua manutenção e atualização dos indicadores de desempenho dos processos do SGSI, estimulando melhorias e mudanças de metas;
- Definir e implantar um plano anual de melhorias de segurança;
- Certificar-se de que a Política de Segurança da Informação da GESTORA está implantada;
- Elaborar um mapa de recursos de segurança e mantê-lo atualizado;
- Efetuar o levantamento e análise dos riscos e mantê-lo atualizado;

- Assegurar que os padrões e os procedimentos de segurança definidos sejam respeitados e certificar-se também de que as medidas definidas sejam eficientes e estejam de acordo com as exigências, sem perder o foco dos indicadores estabelecidos;
- Definir e atualizar os indicadores de segurança da informação, que devem contemplar os riscos a que os sistemas de informação estão expostos.

5.3 GESTORES

5.3.1 Responsabilidades

- Responsabilidade funcional sobre as suas áreas de operação;
- Responsabilidade de manter atualizada a definição dos ativos de informação e notificar em qualquer alteração no inventário de ativos de sua área;
- Implantar e monitorar a eficácia de procedimentos, instruções de trabalho e documentos quanto à proteção da Segurança da Informação;
- Informar/comunicar ao SGSI todos os fatos relacionados a riscos e incidentes relacionados às áreas de operação sob sua responsabilidade;
- Contribuir para implantação dos objetivos do SGSI e efetuar as medições necessárias por processos;
- Implantar as oportunidades de melhoria;
- Planejar a adoção de procedimentos do SGSI e monitorar sua eficácia;
- Garantir a contínua eficácia dos controles implantados para atender os requisitos do SGSI.

5.4 COLABORADORES

Todos os funcionários, terceiros e prestadores de serviço com funções dentro da estrutura da GESTORA.

5.4.1 Responsabilidades

- Responsabilidade de notificar qualquer alteração no inventário de ativos de sua área;
- Conhecer e seguir os procedimentos pertencentes ao SGSI;
- Recomendar melhorias no SGSI para melhoria do processo geral de Segurança da Informação;
- Identificar qualquer incidente de segurança e reportá-lo ao seu gestor/contato direto dentro da GESTORA. No caso de terceirizados e prestadores de serviço reportar diretamente para o Departamento de Segurança da Informação;

R. Amauri, 255, 9° andar 01448.000 Jardim Europa, São Paulo, SP, Brasil (5511) 3019.2800

- Todos os colaboradores têm a responsabilidade de proteger as informações a que tiverem acesso.

6. USO DE DISPOSITIVOS MÓVEIS PESSOAIS E CORPORATIVOS

1. **Autorização e Registro:**
   - Todos os dispositivos móveis utilizados para acessar informações da GESTORA devem ser previamente autorizados e registrados pelo departamento de TI.
   - Dispositivos pessoais devem ser cadastrados e aprovados antes de serem utilizados para fins corporativos.
2. **Configuração de Segurança:**
   - Dispositivos móveis devem ter configurações de segurança adequadas, incluindo senhas fortes, criptografia de dados e bloqueio automático após um período de inatividade.
   - É obrigatório o uso de software de segurança aprovado pela GESTORA, como antivírus e firewalls.
   - Dispositivos móveis devem ser mantidos atualizados com as últimas versões de sistemas operacionais e aplicativos de segurança.
   - Atualizações de segurança devem ser aplicadas imediatamente após a liberação.

3. **Monitoramento e Auditoria:**
   - **O departamento de TI deve monitorar e auditar regularmente os acessos remotos para identificar e responder a atividades suspeitas ou não autorizadas.**
   - **Logs de acesso remoto devem ser mantidos e revisados periodicamente para garantir a conformidade com as políticas de segurança.**

7. MONITORAMENTOS E TESTES

A GESTORA deve assegurar o funcionamento correto e contínuo dos mecanismos de controle descritos acima.

A GESTORA mantém inventários de hardware e software, verificando-os com frequência para identificar elementos estranhos à instituição. A Área Responsável da GESTORA deve diligenciar para manter os sistemas operacionais e softwares de aplicação atualizados.

A área de TI é responsável ainda por monitorar diariamente as rotinas de backup, executando testes regulares de restauração dos dados.

8. REVISÃO

A GESTORA deverá manter o programa de Segurança da Informação continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

Também realizará campanha de conscientização com o fim de garantir que todos os Colaboradores tenham as habilidades necessárias para proteger as informações como parte de suas responsabilidades por meio do Programa previsto na Política de Treinamento e Reciclagem da GESTORA.

O Responsável pela Segurança da Informação, em conjunto com o Comitê de Risco e Compliance, realizará a revisão e atualização desta Política periodicamente, no mínimo anualmente ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada.

R. Amauri, 255, 9° andar 01448.000 Jardim Europa, São Paulo, SP, Brasil (5511) 3019.2800