DOCUMENTO INSTITUCIONAL

SEGURANÇA DA INFORMAÇÃO

2ª Edição

APRESENTAÇÃO

A Segurança da Informação (SI) exerce um papel cada vez mais relevante para as empresas do Grupo Senior. Por isso a necessidade de proteger as informações e os ativos de informação com relação aos riscos e às ameaças que se apresentam nesta área.

O Grupo Senior, ciente da relevância deste assunto, elaborou este documento, reforçando a transparência e patrocínio ao tema, com o intuito de servir de guia para clientes e mercado.

Carlenio Castelo Branco

Presidente

SUMÁRIO

1. SEGURANÇA DA INFORMAÇÃO

Neste item, serão apresentados conceitos relativos à Política de Segurança da Informação, bem como questões que demonstram a importância de sua elaboração, implementação e divulgação.

1.1 O QUE VISA A SEGURANÇA DA INFORMAÇÃO?

A Segurança da Informação tem um papel estratégico no Grupo Senior e visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição. A integridade, a confidencialidade, a autenticidade e a disponibilidade das informações serão abordadas nos itens a seguir.

1.1.1 O que é integridade das informações?

Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações, e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação, ou exclusão, seja ela acidental ou proposital.

1.1.2 O que é disponibilidade das informações?

Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante um período previamente acordado. Manter a disponibilidade das informações pressupõe garantir a prestação continua do serviço, sem interrupções no fornecimento de informações para quem é de direito.

1.1.3 O que é confidencialidade das informações?

Consiste na garantia de que somente pessoas autorizadas tenha acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento.

1.1.4 O que autenticidade das informações?

Consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

1.2 O QUE É A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO?

A Política de Segurança da Informação é um documento formal, aprovado pela diretoria do Grupo Senior, que tem como propósito implementar as melhores práticas de segurança da informação, tendo por finalidade atribuir responsabilidade, definir direito, deveres, expectativas de acesso e uso, penalidade e promover uma cultura educativa organizacional de segurança e privacidade das informações do Grupo Senior, clientes, fornecedores e de parceiros.

1.3 TÓPICOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação do Grupo Senior é um documento completo e organizado por tópicos. Respeitando a Política de Classificação da Informação, este documento é restrito a colaboradores e terceiros do Grupo Senior.

Abaixo, uma breve descrição de cada controles:

1.3.1 Responsabilidades

Este tópico descreve todos os papéis e responsabilidades gerais da instituição, seus colaboradores e terceiros, vem como a alta administração, sobre o tema de Segurança da Informação no Grupo Senior.

1.3.2 Política de Senhas

Este tópico descreve os requisitos mínimos aceitáveis pelo negócio para configurar senhas de acesso aos ambientes de tecnologia do Grupo Senior.

Controles internos são implantados para exigir que as senhas sejam configuradas com um número mínimo de caracteres, bloqueio por tentativas e periodicidade de alteração, assim como o bloqueio de reutilização de senhas anteriores.

1.3.3 Política de Controle de Acessos

Este tópico descreve diretrizes gerais para acesso a ativos e sistemas de informação. Acessos são segregados entre acesso lógico e acesso físico.

1.3.3.1 Acesso Lógico:

A política de acesso lógico define diretrizes, como:

- Perfis de Acesso;
- Concessão, Revogação, Revisão e Cancelamento de acessos;
- Acessos de Terceiros;
- Acesso Remoto;
- Múltiplo Fator de Autenticação (MFA)

1.3.3.2 Acesso Físico:

A política de acesso físico define diretrizes, como:

- Catracas;
- Cancelas;
- Câmeras de Segurança;
- Profissionais de vigilância;
- Geradores e nobreaks;
- Para-raios;

1.3.4 Política de Uso de Ativos e Dispositivos Móveis

Este tópico descreve diretrizes sobre o uso de ativos corporativos de forma segura a profissional, ética e legal, assim como requisitos de proteção da informação durante o transporte de ativos.

1.3.5 Política de Classificação da Informação

Este tópico descreve diretrizes para a classificação das informações no manuseio, rotulagem, transferência e armazenamento de ativos de informação. O documento interno prevê todas as diretrizes utilizadas para a classificação da informação, assim como suas categorias.

1.3.6 Política de Mesa Limpa e Tela Limpa

Este tópico descreve diretrizes de como manusear, armazenar e proteger informações durante o uso das estações de trabalho disponibilizadas pelo negócio, para evitar que pessoas não autorizadas acessem informações restritas, mantendo o princípio da confidencialidade.

Controles internos são implantados para garantir o bloqueio automático das estações de trabalho, evitando a exposição indevida de dados.

1.3.7 Política de Transferência de Informações

Este tópico descreve diretrizes para garantir que informações referentes ao Grupo Senior e de seus clientes, terceiros e fornecedores, sejam transmitidas de maneira segura.

Controles internos são implementados para garantir a segurança durante a transferência de dados, dentro e fora da infraestrutura da companhia.

1.3.8 Política de Trabalho Remoto

Este tópico descreve diretrizes sobre o trabalho remoto.

Controles internos são implementados para garantir que toda transferência de informações seja através de Rede Privada (VPN).

1.3.9 Política de Backup

Este tópico descreve diretrizes sobre o gerenciamento das rotinas de backup, com o intuito de garantir a proteção de dados contra perda de informação.

Controles internos são implementados para garantir que backups são realizados conforme política, testados periodicamente e armazenados de maneira segura.

1.3.10 Política de Proteção Contra Códigos Maliciosos

Este tópico descreve as diretrizes sobre a utilização de ferramentas para proteção contra ameaças de malware.

Controles internos são implementados para detectar, responder e mitigar a ameaça de maneira imediata.

1.3.11 Política para Gestão de Vulnerabilidades Técnicas

Este tópico descreve diretrizes para a gestão de vulnerabilidades, internas e externas, do Grupo Senior.

Controles internos são implementados para garantir que vulnerabilidades sejam detectadas e mitigadas de acordo com níveis de serviço acordados com o negócio.

Testes de invasão são realizados periodicamente para detectar falhas sistêmicas, sendo um controle secundário para ferramentas de detecção de vulnerabilidades.

1.3.12 Política para Gerenciamento de Eventos

Este tópico descreve diretrizes sobre o gerenciamento de eventos de segurança da informação.

Controles internos são implementados para garantir que todos os eventos de segurança sejam centralizados, gerenciados e monitorados continuamente.

1.3.13 Política para Desenvolvimento de Software

Este tópico descreve diretrizes sobre o desenvolvimento seguro de aplicações, seguindo práticas de mercado. Ambientes produtivos são segregados dos ambientes de homologação e desenvolvimento, garantindo a modificação somente por pessoas previamente autorizadas.

Controles internos são implementados para garantir que atualização de aplicações sejam realizadas através de gerenciamento de mudanças e respeitando a segregação de funções.

O Grupo Senior implementa tecnologias para realizar testes estáticos (SAST) e testes dinâmicos (DAST) durante o processo de desenvolvimento.

1.3.14 Política de Resposta a Incidentes

Este tópico descreve diretrizes para prevenir, tratar e responder adequadamente incidentes de segurança da informação que possam impactar os serviços ou recursos tecnológicos da instituição.

Além disso, a política descreve regras de priorização e severidade com relação a possíveis incidentes de segurança, procedimentos de comunicação com autoridades e clientes, quando necessário.

1.3.15 Política de Continuidade de Negócios

Este tópico descreve diretrizes, procedimentos e estratégias a serem realizados durante eventuais cenários de contingência alinhados com o propósito e metas estratégicas da instituição.

Testes de recuperação de desastres são realizados, com periodicidade semestral, para garantir que a estratégia esteja sempre atualizada.

O Grupo Senior executa seu workload em provedores de cloud globais que seguem normas e padrões consolidados no mercado internacional de certificação de seu Data Center, sob aspecto de tier de segurança e plano de continuidade de negócios. Este workload possui seu backup replicado em no mínimo dois Data Centers, garantindo a prevenção quanto ao risco de perda total de dados, tendo como premissa única e exclusivamente a capacidade de recuperação dos dados em caso de catástrofe classificada como ruína, considerando o tempo de recuperação aplicado por estes players globais.

Uma versão pública está disponível para todos os clientes e mercado: https://www.senior.com.br/politica-de-seguranca-da-informacao

1.4 COMO SE DÁ O PROCESSO DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

O Grupo Senior realiza, periodicamente, treinamentos e eventos de conscientização sobre o tema de Segurança da Informação e Privacidade de Dados, para todos os colaboradores e terceiros.

Abaixo, uma lista processos de conscientização:

- Treinamento de *Onboard*;
- Semana de Segurança da Informação;
- *Lives*;
- Campanhas de *phishing*;
- Posts na rede social corporativa.

1.5 A QUEM DEVE SER DIVULGADA A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO?

A Política de Segurança da Informação é divulgada para todos os colaboradores do Grupo Senior, assim como terceiros.

Uma versão pública está disponível para todos os clientes e mercado: https://www.senior.com.br/politica-de-seguranca-da-informacao

1.6 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA FORNECEDORES

O Grupo Senior realiza, de maneira formal e estruturada, o gerenciamento de fornecedores da organização. Com isso, é necessário a aceite da Política de Segurança da Informação para Fornecedores, previamente à assinatura do contrato de prestação de serviços, para estar apto a fornecer produtos/serviços ao Grupo Senior.

A Política de Segurança da Informação para Fornecedores está disponível para todos: https://d2nytdlptrqhdi.cloudfront.net/wp-content/uploads/2024/04/25180109/PL011.pdf

1.7 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA CONSULTORES CREDENCIADOS

O Grupo Senior realiza, de maneira formal e estruturada, o gerenciamento de consultores credenciados que atuam em nome da companhia. Todos os consultores atuam sob um contrato de prestação de serviços, com cláusulas de confidencialidade e não divulgação de informações às quais possam vir a ter acesso, assim como cláusulas de confidencialidade relacionadas ao tema de privacidade de dados pessoais.

Para garantir que todos os consultores credenciados atuem conforme a Política de Segurança, auditorias são realizadas pela equipe de Segurança da informação, com periodicidade acordada com a organização.

2. PRIVACIDADE E PROTEÇÃO DE DADOS

Neste item, serão apresentados conceitos relativos à Política de Privacidade de Dados, bem como questões que demonstram a importância de sua elaboração, implementação e divulgação.

2.1 ENCARREGADO PELA PROTEÇÃO DE DADOS

O Grupo Senior nomeou um profissional como Encarregado pela Proteção de Dados Pessoais (DPO). Este profissional tem o papel de informar e aconselhar a companhia em relação ao tema de privacidade, controlar a conformidade com a LGPD (Lei Geral de Proteção de Dados) e com as políticas internas, prestar conselhos referentes à avaliação do impacto da proteção de dados, acompanhar o seu desempenho e servir de ponte para a ANPD (Autoridade Nacional de Proteção de Dados) em questões relacionadas com o tratamento de dados pessoais. Para mais informações sobre o DPO, acesse o nosso site: https://www.senior.com.br/portal-de-privacidades.

2.2 O QUE É A POLÍTICA DE PROTEÇÃO DE DADOS?

A Política de Proteção de Dados é um documento formal, aprovado pela diretoria do Grupo Senior, que tem como propósito implementar as melhores práticas de privacidade de dados pessoais, tendo por finalidade atribuir responsabilidade, definir direito, deveres, expectativas de acesso e uso, penalidade e promover uma cultura educativa organizacional de privacidade das informações do Grupo Senior, clientes, fornecedores e de parceiros.

2.3 AVISO DE PRIVACIDADE

O aviso de privacidade é uma comunicação clara e objetiva, pelo qual o Grupo Senior, atuando na posição de controlador, transparece ao titular a forma como o tratamento de dados pessoais é realizado, quais os tipos de dados pessoais são coletados, as finalidades para quais são coletados, a hipótese legal que autoriza o tratamento, os terceiros com ais podem ser compartilhados dados e as medidas que são adotadas para protege-los.

Este aviso de privacidade pode ser consultado no seguinte endereço: https://www.senior.com.br/politica-de-privacidade

2.4 POLÍTICA DE COOKIES

O Grupo Senior disponibiliza para titules, clientes, fornecedores e mercado, uma Política de Cookies, que tem por finalidades aprender como os usuários interage com o conteúdo, identificar quais recursos mais procurados, contar os visitantes de uma página e melhorar a experiência para o visitante.

A Política de Cookies pode ser consultada no seguinte endereço: https://www.senior.com.br/politica-de-cookies

2.5 CONTATO COM TITULARES

O Grupo Senior disponibiliza, em seus sites, um formulário para que titulares de dados possam entrar em contato com a companhia e/ou solicitar que seus direitos sejam compridos, entre eles:

- Confirmação da existência do tratamento;
- Acessos aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- Portabilidade dos dados;
- Eliminação dos dados pessoais tratados como o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei;
- Informações das entidades públicas e privadas com as quais o Grupo Senior realizou o compartilhamento dos dados;
- Informações sobre a possibilidade de não fornecer o consentimento e sobre a consequência da negativa;
- Revogação do consentimento;

O formulário de contato com o Encarregado pela Proteção de Dados pode ser consultado no seguinte endereço: https://www.senior.com.br/portal-lgpd

2.6 MAPEAMENTO DE DADOS PESSOAIS E REGISTRO DE ATIVIDADES DE PROCESSAMENTO (ROPA)

O mapeamento de dados, ou ainda, o inventário de dados, *data mapping* ou *data flow,* é um documento que reflete o caminho percorrido pelo dado pessoal dentro da organização, incluindo processos, procedimentos e tecnologias pelos quais o dado transita.

O Grupo Senior mantém um inventário de dados, atualizando constantemente, assim como mantém o Registro das Atividades de Tratamento (ROPA), com o intuito de transparecer a maneira como é realizada a coleta do dado, quais as operações de tratamento realizado e como é feita a exclusão do dado pessoal.

2.7 ANÁLISE DE IMPACTO SOBRE DADOS PESSOAIS (AIPD)

A Análise de Impacto sobre Dados Pessoais (AIPD), ou ainda, Relatório de Impacto sobre Proteção de Dados (RIPD), é um relatório que tem como função demonstrar como o Grupo Senior avalia os riscos nas operações de tratamento de dados pessoais e adota medidas para mitiga-los.

3. CONFORMIDADE E CERTIFICAÇÕES

O Grupo Senior, como uma forma de demonstrar o seu compromisso com o tema, implementa, mantém e melhor continuamente o Sistema de Gestão de Segurança da Informação (SGSI.

3.1 ISO 27001

A norma ISO 27001 é o padrão e referência internacional para a gestão da Segurança da Informação. Tem como princípio geral a adoção pela organização de um conjunto de requisitos, processos e controles internos, com o objetivo a gestão e a mitigação de riscos.

A Grupo Senior possui o seu Sistema de Gestão de Segurança da Informação (SGSI) certificado pela norma ISO 27001, com o seguinte escopo: **Sistema de Gestão de Segurança da Informação que suporta a Infraestrutura, Desenvolvimento de Aplicações, Entrega e Manutenção de soluções em SaaS.**

Abaixo, a lista de controles implementados pela organização:

3.1.1 Política de Segurança da Informação

O Grupo Senior mantém uma Política de Segurança da Informação, divulgada internamente e treinada por todos os colaboradores. Este documento é restrito para colaboradores e descreve todas as práticas e condutas que devem ser seguidas durante as atividades profissionais pela companhia.

3.1.2 Organização da Segurança da Informação

O Grupo Senior implementou e melhora continuamente uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da companhia.

3.1.3 Segurança em Recursos Humanos

O Grupo Senior possui processos internos de recursos humanos para assegurar que funcionários e partes externas entendam as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.

3.1.4 Gestão de Ativos

O Grupo Senior possui processos e ferramentas adequadas para identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos mesmos.

3.1.5 Controle de Acesso

O Grupo Senior implementou, opera e melhora continuamente o processo de controle de acessos a informações e ativos de informações, com o objetivo de limitar o acesso de pessoas não autorizadas.

O gerenciamento de acesso é realizado respeitando o princípio de segregação de funções para os seguintes controles:

- Concessão de acessos;
- Cancelamento de acessos;
- Revisão de acessos;
- Revogação de acessos;

3.1.6 Criptografia

O Grupo Senior implementa controles criptográficos para proteção de suas informações e seus ativos de informação e assegurar o uso efetivo e adequado para manter a confidencialidade, autenticidade e a integridade da informação.

3.1.7 Segurança Física e do Ambiente

O Grupo Senior implementou, opera e melhora continuamente controles de acesso físicos para prevenir o acesso não autorizado, dano e interferência nos recursos de processamento de informações e nas informações da organização.

3.1.8 Segurança nas Operações

O Grupo Senior implementa e melhora continuamento seus processos internos para garantir a operação segura e correta dos recursos de processamento da informação.

Controles técnicos e processos são implementados para garantir a segurança nas operações da organização, são eles:

- Gestão de Mudanças;
- Gestão da Capacidade;
- Proteção Contra Malware;
- Cópias de Segurança (Backup);
- Registro e monitoramento de eventos (*logs*);
- Gestão de vulnerabilidade técnica;
- Auditorias de conformidade operacional.

3.1.9 Segurança nas comunicações

O Grupo Senior implementa controles técnicas que asseguram a proteção das informações em redes e dos recursos de processamento de informações que as apoiam.

Controles técnicos e processos são implementados para garantir a segurança nos serviços de comunicação, são eles:

- Controles de acesso a redes;
- Segregação de redes;
- Políticas para transferência de informações;
- Segurança em mensagens eletrônicas (e-mails);
- Cláusulas contratuais de confidencialidade e não divulgação das informações.

3.1.10 Requisitos de Segurança de Sistemas de Informação

O Grupo Senior implementa e melhora continuamente requisitos para garantir que a segurança da informação seja integrante de todo ciclo de vida dos sistemas de informação.

Controles técnicos e processos são implementados para garantir a segurança durante todo ciclo de vida aplicações, são eles:

- Análise e especificação dos requisitos de segurança da informação;
- Proteção de transações em aplicativos;
- Política para desenvolvimento seguro de software;
- Análise crítica sobre mudanças operacionais;
- Segregação entre ambientes;
- Testes estáticos e dinâmicos de aplicações.

3.1.11 Relacionamento na Cadeia de Suprimentos

O Grupo Senior implementou e melhora continuamente o processo de relacionamento com fornecedores, com o intuito de garantir a proteção das informações e dos ativos de informação da organização.

Como boa prática operacional, o organização criou e mantém atualizada, uma política de segurança da informação para fornecedores, que pode ser consultada no seguinte endereço: https://d2nytdlptrqhdi.cloudfront.net/wp-content/themes/senior-2019/content/pdf/PL011.pdf

3.1.12 Gestão de Incidentes de Segurança da Informação

O Grupo Senior implementou e melhora continuamente um processo de resposta a incidentes, com o objetivo de assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

3.1.13 Continuidade da Segurança da Informação

O Grupo Senior implementou e melhora continuamente um processo de continuidade operacional de ambientes de tecnologia, com o objetivo de assegurar que as operações continuem resilientes após impacto.

3.1.14 Conformidade

O Grupo Senior implementou controles internos para assegurar a conformidade com obrigações legais, estatutárias ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.

O certificado ISO 27001 foi emitido pelo órgão certificado Bureu Veritas, com aceitação internacional pelo selo UKAS (*United Kingdom Accreditation Service*).

3.2 SOC 1 Tipo II

O relatório SOC 1 tem como intuito avaliar a estrutura de controles internos da empresa, focados em auditoria financeira, ou seja, que impliquem, de alguma forma, no balanço financeiro dos clientes. É medido sob três aspectos:

- Gerenciamento de Acessos;
- Gerenciamento de Mudanças;
- Gerenciamento de Operações de TI.

O Grupo Senior possui o relatório SOC 1 Tipo II, emitido por Auditoria Independente, para o produto **HCM (Gestão de Pessoas) em SaaS**.