Política de segurança da informação

Documento gerado em 26/11/2024 às 10h41

Metadados

Código	Origem	Elaboração	Última Revisão	Próxima Revisão
PLT.SEG.ADM.006.1	Segurança da Informação	28/05/2019	26/11/2024	26/11/2027

Ficha técnica

Etapa	Responsável	Assinatura
Elaboração	Felipe Mendonça Satito de Melo	Felipe Satito *Assinado eletronicamente por: Felipe Satito Data: 27 de novembro de 2024 11:46 GMT-3*
Revisão	Antonio Sergio da Silva	 *Assinado eletronicamente por: Antonio Sergio da Silva Data: 27 de novembro de 2024 14:42 GMT-3*
Revisão	Thamires Pedra Kemache Franco	 *Assinado eletronicamente por: Thamires Pedra Kemache Franco Data: 27 de novembro de 2024 17:29 GMT-3*
Aprovação	Teresa Cristina Campos Mello	Teresa Cristina Campos Mello *Assinado eletronicamente por: Teresa Cristina Campos Mello Data: 29 de novembro de 2024 09:59 GMT-3*

Objetivo

A Política de Segurança da Informação tem como objetivo destacar o compromisso da Prevent Senior no que tange à guarda e proteção das informações de sua propriedade ou que estiverem sob sua guarda, criando e implementando diretrizes no que toca aos procedimentos de preservação à segurança e integridade da informação.

Aplicabilidade

A Política de Segurança da Informação se aplica à Alta Direção, todos os colaboradores, parceiros comerciais (fornecedores e prestadores de serviços) e terceiros (agentes intermediários) que eventualmente tenham acesso as suas informações e dados.

Definições

- **Evento de segurança da informação:** situações adversas as quais possam colocar em risco a confidencialidade, integridade ou disponibilidade de um ativo da informação.
- **Incidente de segurança da informação:** situações que causaram um impacto à confidencialidade, integridade ou disponibilidade de um ativo da informação.
- **Ativo da informação:** tudo o que possui informações consigo, tais como colaboradores, prestadores de serviços e até objetos como *pendrive*, celular, computadores, leitor biométrico, etc.
- **Classificação da informação:** classificação de determinado dado que orienta o quão é confidencial aquela informação e a respectiva disponibilidade que deverá ser adotada.

- **Vulnerabilidade:** ponto fraco de um determinado processo, controle ou ativo da informação.
- **Chave criptográfica:** arquivo digital que possibilita criptografar ou descriptografar determinada informação.
- **Cadeia de suprimento:** conhecimento das partes necessárias para o recebimento de determinado produto ou serviço.
- **DPO:** sigla que significa *Data Protection Officer*, na qual é o responsável pelos dados da organização e por verificar e aconselhar a Prevent Senior a estar em consonância com as melhores práticas no que tange à proteção de dados e com a Lei nº 13.709/2018.
- **Primeira linha de defesa:** gerentes operacionais que administram os riscos e têm propriedade sobre eles. Eles também são os responsáveis por implementar as ações corretivas para resolver deficiências em processos e controles.
- **Segunda linha de defesa:** estabelece diversas funções de gerenciamento de riscos e conformidade para ajudar a desenvolver e/ou monitorar os controles da primeira linha de defesa. Estabelece essas funções para garantir que a primeira linha de defesa seja apropriadamente desenvolvida, posta em prática e que opere conforme intencionado.
- **Terceira linha de defesa:** representa a figura da auditoria interna, onde provê avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linhas de defesa alcançam os objetivos de gerenciamento de riscos e controle. O escopo dessa avaliação, que é reportada à Alta Direção.
- **Causa raiz:** fator principal que ocasionou determinada ocorrência.
- **Incidente de segurança:** registro de casos no qual haja a confirmação de que houve exploração da vulnerabilidade relacionada a determinado evento.

Pilares da segurança da informação

A Política de Segurança da Informação da Prevent Senior baseia-se em três pilares básicos:

- **Confidencialidade:** a informação deverá ser acessada somente por pessoas autorizadas pela empresa.
- **Integridade:** modificações, inserções e supressões da informação só serão realizadas com a autorização da empresa.
- **Disponibilidade:** pessoas autorizadas deverão ter acesso à informação sempre que necessitem, ou seja, sempre que demandado.

Para que os três itens acima possam ser aplicáveis na rotina da empresa é preciso que a informação seja adequadamente gerida e, acima de tudo, protegida contra fraudes, espionagem, roubo, perda acidental, bem como outras ameaças análogas.

Descrição das atividades

Estrutura da gestão de segurança da informação

A estrutura da Gestão de Segurança da Informação está sob a liderança do departamento de Tecnologia da Informação (TI), que se reporta à Alta Direção da Prevent Senior.

Aspectos gerais da gestão de segurança da informação

A Gestão de Segurança da Informação é um dos importantes instrumentos de orientação, implementação e monitoração de controles mitigatórios dos riscos

relacionados aos vazamentos das informações e gerenciamento das vulnerabilidades tecnológicas, processos e humanas nos ativos da informação.

No que tange a vulnerabilidades técnicas, devem ser estabelecidos níveis de controles e monitorações periódicas, que visa potencializar a eficácia da segurança de TI, considerando os seguintes tópicos:

- Gestão de acesso lógico.
- Armazenamento e tratamento da informação digital.
- Transferência de informações digitais.
- Utilização de mídias removíveis.
- Gestão de dispositivos móveis.
- Gestão de acesso remoto.
- Restrições sobre usos e instalações de softwares.
- Gestão de *backup*.
- Proteção contra códigos maliciosos.
- Gerenciamento de vulnerabilidades técnicas.
- Gerenciamento de chaves e criptografias.
- Dentre outros controles relacionados a proteção tecnológica.

Quanto às vulnerabilidades de processos, devem ser considerados os seguintes aspectos:

- Definições de políticas, manuais ou instruções de trabalho.
- Classificação da informação.
- Definições de papéis e responsabilidades.

- Processo para tratamento dos desvios e exceções.
- Proteção e privacidade da informação de identificação pessoal.
- Definições cláusulas contratuais referentes a proteção das informações.
- Relacionamento da cadeia de suprimentos.

Quanto às vulnerabilidades humanas, devem ser estabelecidos controles para os seguintes assuntos, como:

- Gestão de tela e mesa limpa.
- Capacitações periódicas sobre a segurança da informação.
- Orientações e cuidados sobre as engenharias sociais.
- Controle de uso adequado dos ativos da informação.
- Registro e tratamento de evento de segurança da informação.
- Tratamento de informações de acordo com a sua classificação.

Objetivando garantir que os riscos das vulnerabilidades estão sendo mitigados de forma eficaz, as atividades de segurança da informação deverão ser segregadas da primeira linha de defesa, garantindo sua independência e autonomia em caso de identificação de alguma ação ilícita ou incidentes de segurança que precisem ser reportados imediatamente à Alta Direção ou órgãos responsáveis, consequentemente situações que exigem ações imediatas.

Assim, a Gestão de Segurança da Informação atuará como uma área da segunda linha de defesa, auxiliando as áreas da primeira linha de defesa a se manterem em conformidade com o Sistema de Gestão da Segurança da Informação (SGSI), conforme figura a seguir:

Sistema de Gestão da Segurança da Informação (SGSI)

Papéis e responsabilidades

Alta Direção

- Apoiar a cultura de gestão de segurança da informação, solicitando que todos os colaboradores e partes interessadas pratiquem a segurança da informação.
- Aprovar a política de segurança da informação.
- Fornecer recursos suficientes para que os responsáveis pela segurança da informação exerçam seus papéis conforme definido.
- Definir e comunicar as expectativas sobre a segurança da informação.
- Definir o apetite aos riscos relacionados à segurança da informação.
- Estabelecer diretriz à Gestão de Segurança da Informação quando um evento de segurança necessitar de um plano de ação estratégico.

Gestão de segurança da informação

- Elaborar a política de segurança da informação conforme expectativas da Alta Direção.
- Submeter a política de segurança da informação para aprovação da Alta Direção.
- Comunicar e deixar disponível a versão atualizada da política de segurança da informação.
- Identificar e manter as políticas complementares atualizadas e divulgadas.
- Providenciar treinamentos sobre a segurança da informação na integração de novos colaboradores ou prestadores de serviços.
- Providenciar treinamentos periódicos sobre a segurança da informação e respectivas atualizações para todos os colaboradores e prestadores de serviço.
- Disseminar e manter a cultura de segurança da informação na Prevent Senior.
- Estabelecer, monitorar e comunicar níveis aceitáveis de controles relacionados à segurança da informação.
- Estabelecer um cronograma para realizar testes periódicos (*checklists* e *pentest*) dos controles de segurança da informação.
- Implementar um processo para identificação, registro e tratamento de eventos de segurança da informação.
- Disponibilizar um local seguro para registrar os eventos de segurança e que fique disponível para todos os colaboradores ou prestadores de serviço com acesso aos dados da Prevent Senior.
- Realizar análise de causa raiz e elaborar plano de ação juntamente com o responsável para tratar o evento de segurança da informação.

- Manter os dados relacionados aos eventos de segurança em sigilo.
- Comunicar ao Compliance quando identificar algum evento de segurança que esteja relacionado à fraude, corrupção, ações ilícitas ou situações similares.
- Comunicar a Alta Direção quando ocorrer um evento de segurança com o risco acima do apetite estabelecido ou quando houver a materialização do evento (incidente de segurança).
- Sempre que solicitado pela Auditoria e Controles Internos, fornecer evidências que corroborem com a continuidade de alguma análise ou investigação.
- Realizar reporte periódico à Alta Direção e ao DPO da Prevent Senior sobre os resultados das análises periódicas, eventos de segurança ocorridos no período e o status dos respectivos planos de ação.
- Quando embasado por evidências, assumir provisoriamente atividades técnicas que possuam impacto direto na segurança da informação com a finalidade de adequação do processo.
- Validar aquisição ou desenvolvimento de aplicações quanto à segurança das informações usadas.
- Definir e atualizar junto às áreas operacionais/administrativas matriz de acesso às informações.
- Monitorar ameaças externas e internas à segurança da informação.
- Realizar análises forenses de dispositivos quando detectado alto risco de vazamento ou judicial por outros setores da empresa.

DPO

- Elaborar propostas de melhorias e aprovar a Política de Segurança da Informação.

- Com base em inventário de informações, bem como nos critérios de classificação que figuram na norma específica, realizar a avaliação e, se necessário, ajustar a classificação das informações de propriedade ou que estejam sob a guarda da Prevent Senior.
- Analisar os registros dos eventos de segurança.
- Avaliar e, se necessário, definir ajustes na matriz de segregação de funções a ser apresentada pela área de Gestão de Segurança da Informação.
- Analisar as ocorrências de violação desta Política de Segurança da Informação, encaminhando-as à Alta Direção, quando for o caso.
- Apresentar projetos com a finalidade de aprimorar a segurança da informação da Prevent Senior.
- Determinar a elaboração de levantamentos, relatórios e análises que deem suporte à Gestão de Segurança da Informação e sua tomada de decisão.
- Acompanhar o andamento dos projetos e demais iniciativas relacionadas à segurança da informação.
- Aprovar a nomeação dos proprietários da informação por meio do fluxo de aprovação (Jurídico, TI, Compliance, encarregado).
- Informar ao titular eventuais mudanças de finalidade e tratamento de seus dados.
- Comunicar, sempre que solicitado pela Autoridade Nacional, relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comerciais e industriais.

Auditoria interna

- Incluir no escopo da Auditoria a análise periódica dos processos e controles internos relacionados à segurança da informação.

- Em caso de necessidade, utilizar recursos da Gestão de Segurança da Informação para auxiliar em uma análise ou investigação.

Qualidade

- Alinhar as diretrizes da Qualidade em consonância com esta política.
- Informar a área de Segurança da Informação quando identificar um novo processo.
- Em caso de detecção de alguma vulnerabilidade ou evento que possam se caracterizar um evento de segurança durante as verificações realizadas pelo Departamento da Qualidade, comunicar a Gestão de Segurança da Informação.

Compliance

- Quando houver o reporte de um determinado evento de segurança que esteja relacionado a fraude, corrupção, ações ilícitas ou situações similares, avaliar o caso e realizar a tratativa conforme processo estabelecido.
- Avaliar periodicamente se os processos referentes ao Sistema de Gestão de Segurança da Informação, estão em conformidade com as respectivas leis ou regulamentações aplicáveis.

Departamento de Tecnologia da Informação

- Aplicar os controles relacionados à segurança de TI conforme diretrizes estabelecidos pela Gestão de Segurança da Informação.
- Manter trilhas de auditoria e alertas de segurança das aplicações (*firewall* e antivírus) registradas em local seguro e disponíveis para possíveis análises pelas áreas responsáveis (Auditoria, Controles Internos e Gestão de Segurança da Informação).

- Não disponibilizar informações/dados sem a devida justificativa ou aprovação da Gestão de Segurança da Informação.
- Em caso de identificar um evento de segurança, efetuar o registro imediatamente, deste modo evitando a materialização do incidente.
- Realizar a concessão, revisão e revogação dos acessos lógicos de usuários mediante a contratação, alteração de cargo/função e encerramento de contrato de colaborador ou prestador de serviço.

Departamento de Recursos Humanos

- Comunicar imediatamente o Departamento de TI novas contratações, alterações de cargo/função e encerramento de contrato de colaborador, para ser realizado a concessão, alteração ou a revogação de acesso lógico;
- Auxiliar a Gestão de Segurança da Informação na disseminação da cultura de segurança da informação.
- Aplicar o termo de responsabilidade dos colaboradores devido ao acesso às informações.
- Manter os controles de segurança da informação referente aos dados pessoais dos colaboradores.
- Em caso de identificar um evento de segurança, efetuar o registro de forma imediata, deste modo evitando a materialização do incidente.

Departamento Jurídico

- Elaborar e aprovar os termos de responsabilidade referente ao compromisso de confidencialidade das informações para serem aplicados aos colaboradores e prestadores de serviço.
- Elaborar e aplicar cláusula de confidencialidade em contratos celebrados junto a Prevent Senior.

- Avaliar periodicamente as atualizações de leis e resoluções aplicáveis ao Sistema de Gestão de Segurança da Informação.
- Definir as diretrizes no que tange as sanções administrativas em caso de descumprimento do termo de responsabilidade referente ao compromisso de confidencialidade das informações.

Demais colaboradores

- Cumprir as diretrizes estabelecidas no que tange o Sistema de Gestão de Segurança da Informação da Prevent Senior.
- Participar de treinamentos e campanhas sobre segurança da informação;
- Estar ciente e cumprir as diretrizes contidas na Política de Segurança da Informação e políticas complementares.
- Fazer o bom uso e tratamento dos ativos da informação e respectivos dados contidos neles.
- Assinar o termo de responsabilidade sobre o acesso e uso das informações obtidas no ambiente da Prevent Senior.
- Em caso de detecção de alguma vulnerabilidade ou evento que possam se caracterizar um evento de segurança, efetuar o registro no canal disponibilizado ou comunicar imediatamente a Gestão de Segurança da Informação.

Prestadores de serviços

- Cumprir as diretrizes estabelecidas no que tange o Sistema de Gestão de Segurança da Informação da Prevent Senior.
- Participar de treinamentos e campanhas sobre segurança da informação.
- Estar ciente e cumprir as diretrizes contidas na Política de Segurança da Informação e políticas complementares.

- Fazer o bom uso e tratamento dos ativos da informação e respectivos dados contidos neles.
- Considerar em contrato a responsabilidade sobre o acesso e uso das informações obtidas no ambiente da Prevent Senior.
- Em caso de detecção de alguma vulnerabilidade ou evento que possam se caracterizar um evento de segurança, comunicar imediatamente a Gestão de Segurança da Informação.

Eventos de segurança da informação

Os eventos de segurança da informação são situações adversas, que estão sob suspeita, relacionados à segurança de sistemas de informação, levando à perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

Após o registro do evento, que poderá ser realizado por qualquer colaborador, esta atividade é de responsabilidade da Gestão de Segurança da Informação.

Os eventos de segurança da informação deverão seguir as seguintes etapas:

- **Identificação:** a identificação de um evento de segurança pode ocorrer em qualquer momento por colaborador ou terceiro da Prevent Senior, ao identificar a situação e avaliar qual princípio está exposto (Confidencialidade, Integridade e Disponibilidade).
- **Registro do evento:** ato de formalizar e comunicar às áreas competentes o evento identificado. Nesta etapa será validado o conteúdo do evento, bem como avaliação, grau de risco e impacto que a situação oferece.
- **Análise de causa raiz:** após a confirmação de que realmente houve o evento de segurança (independente se o risco materializou), deve ser feita a análise de causa raiz, possibilitando, assim, elaborar um plano de ação eficaz pelos responsáveis por esta ação.

- **Execução do plano de ação:** após realizada a análise e criado o plano de ação, é necessário realizar a mitigação do problema, conforme as melhores práticas.

- **Acompanhamento do plano de ação:** a Gestão de Segurança da Informação tem como responsabilidade acompanhar a correção da falha ou vulnerabilidade identificada na etapa da análise de causa raiz. Importante destacar que todas as conclusões dos planos de ação deverão ser sustentadas por evidências e as respectivas documentações serão tratadas como informação confidencial. Seu acesso será restrito, exceto para análise do Departamento de Auditoria e Controles Internos ou determinações judiciais.

- **Retorno ao responsável pelo evento:** o responsável que identificou e registrou o evento deverá ser comunicado sobre o status da ocorrência.

- **Reporte periódico:** a Gestão de Segurança da Informação deverá definir um período de reporte dos eventos de segurança da informação para a Alta Direção e DPO. Em casos os quais o evento resultou em um Incidente de Segurança, o reporte deverá ser imediato.

Treinamentos de segurança da informação

Objetivando implementar e manter a cultura de segurança da informação na Prevent Senior, o departamento de Gestão de Segurança da Informação tem a responsabilidade de definir o conteúdo e a estratégia para aplicar os treinamentos aos novos colaboradores e prestadores de serviços.

Deve-se considerar também as campanhas e treinamentos periódicos a todos os colaboradores e prestadores de serviços da Prevent Senior, procurando, assim, manter atualizada a cultura de segurança da informação. Em relação à execução dos treinamentos, fica a escolha da estratégia adotada pelo Departamento de Gestão de Segurança da Informação.

Anexos

- Política de Tratamento de Dados pessoais em conformidade com LGPD.
- Política de Riscos de Segurança da Informação.

Histórico de alterações conforme versionamento

Versão	Descrição da alteração	Responsável
1	Revisão do texto e reenvio devido ao prazo de vigência do documento em sistema	Felipe Satito

---

SGQ - Núcleo de Gestão de Documentos, Prevent Senior, 2024.

A work by R Markdown

UUID:988406b2-27c4-4203-95d0-d5d32af3f19d