GRUPO IAG SAÚDE

Política de Gestão de Incidentes de Segurança da Informação

Versão 1

POLÍTICA INSTITUCIONAL – POI IAG 024

POLÍTICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1 OBJETIVO

Assegurar uma resposta rápida, eficaz, consistente e ordenada aos incidentes de segurança da informação, incluindo a comunicação sobre eventos de segurança da informação.

2. ABRANGÊNCIA

Esta Política se aplica a todos os setores e partes interessadas do Grupo IAG Saúde.

3. SIGLAS E DEFINIÇÕES

Ativo: qualquer coisa que tenha valor para a instituição e precisa ser adequadamente protegida.

Grupo IAG Saúde: holding das empresas Instituto de Acreditação e Gestão em Saúde Ltda (IAG Saúde) e Instituto de Acreditação, Gestão, Consultoria e Sistemas de Informação Ltda (IAG Sistemas), e suas respectivas marcas: DRG Brasil®,

Valor Saúde Brasil® e SigQuali®.

Informação: conjunto de dados que, processados ou não, pode ser utilizado para produção e transmissão de conhecimento, contido em qualquer meio, suporte ou formato.

Incidente de segurança da informação: um ou múltiplos eventos de segurança da informação relacionados e identificados que podem prejudicar os ativos da organização ou comprometer suas operações.

Gestão de incidentes de segurança da informação: exercício de uma abordagem consistente e eficaz para o manuseio de incidentes de segurança da informação.

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação na instituição.

4. DIRETRIZES

A Política de Gestão de Incidentes de Segurança da Informação é parte integrante da Política de Privacidade de Dados e Segurança da Informação e terá as seguintes diretrizes e princípios:

- Estabelecer o processo para detectar, registrar, diagnosticar, responder e solucionar incidentes de segurança da informação;
- Oferecer diretrizes que tenham como foco a manutenção e a continuidade dos serviços em menor tempo possível;
- Oferecer transparência na gestão de incidentes de segurança da informação.

4.1 Papéis e responsabilidades para a realização dos procedimentos de gestão de incidentes

O Comitê de Segurança da Informação, terá como missão o planejamento e a execução de ações que ofereçam respostas eficientes aos incidentes de segurança que apresentem risco à confidencialidade, integridade e disponibilidade dos dados e serviços.

O comitê é composto por:

- Presidência e Coordenação de Análise de Dados e Inteligência de Negócios
- Encarregada de Proteção de Dados
- Coordenação de Compliance
- Diretora de Tecnologia da Informação e Coordenação do Sistema de Gestão de Segurança da Informação
- Coordenação de Análise do Sistema de Informação

O Comitê terá autonomia para garantir as melhores ações de resposta para um incidente, atendendo às necessidades.

As responsabilidades sobre a execução das atividades previstas nesta diretriz caberão aos seguintes responsáveis:

POLÍTICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Presidência:

- Nomear os responsáveis pelos papéis relevantes para a segurança da informação e garantir autoridade e responsabilidade do sistema de gestão de segurança da informação;
- Aprovar e implementar esta política, bem como as demais políticas específicas por tema;
- Acompanhar o desempenho do sistema de gestão de segurança da informação.

Comitê de Segurança da Informação:

- Realizar a análise crítica dos incidentes de segurança da informação e atuar na tomada de decisão para ações relativas ao processo de resposta e tratamento dos incidentes;
- Se aplicável, acionar o Plano de Recuperação de Desastres;
- Se aplicável, acionar os Planos de Plano de Contingência;
- Discutir as alternativas e as recomendações apresentadas, sugerindo os programas e/ou projetos e as ações para a sua implementação;
- Submeter o relatório de incidentes e buscar ações que devem ser tomadas no âmbito da empresa.

Encarregado de Proteção de Dados e Coordenação de Compliance:

- Relatar e incentivar os colaboradores a relatarem, de boa-fé, indícios de ilicitudes e práticas não conformes com normas internas e externas;
- Realizar gestão do canal de ouvidoria e conduzir o processo de investigação dos relatos;

- Identificar e realizar a gestão de riscos de compliance, segurança da informação e proteção de dados relativos cooperativamente com a coordenação de Sistema de Gestão de Segurança da Informação (SGSI);
- Assegurar que a necessidade de ações corretivas seja identificada e as ações implementadas;
- Formalizar a comunicação do incidente de segurança.

Coordenação do Sistema de Gestão de Segurança da Informação:

- Identificar e realizar a gestão de riscos de segurança da informação e proteção de dados cooperativamente com a Encarregada de Proteção de Dados e Coordenação de Compliance;
- Assegurar que as diretrizes de confidencialidade, integridade e disponibilidade da informação sejam observadas e cumpridas durante o processo de recuperação / continuidade do negócio;
- Gerenciar o controle de acesso emergencial ao ambiente de contingência;
- Bloquear ameaças e ataques.

Coordenação de Análise do Sistema de Informação:

- Trabalhar cooperativamente com a coordenação de Sistema de Gestão de Segurança da Informação (SGSI).

Todos os usuários:

- Seguir, de forma colaborativa, as orientações fornecidas em relação a segurança da informação do Grupo IAG Saúde, bem como às normas e procedimentos internos.

- Utilizar de forma ética e consciente os recursos computacionais e informacionais.
- Relatar, de boa-fé, indícios de ilicitudes e práticas não conformes em relação à segurança da informação e demais normas internas e externas.

Todos os fornecedores e parceiros:

- Implementar, cumprir e fazer cumprir políticas, boas práticas e padrões técnicos atuais e eficazes para a segurança e proteção das informações e dados pessoais;

- Comunicar ao Grupo IAG Saúde no e-mail (dpo@grupoiagsaude.com.br), no prazo de 24 horas a ocorrência ou suspeita de ocorrência, de incidente de segurança, devendo informar: (i) dia e horário da ocorrência, (ii) relação dos tipos de dados afetados, (iii) número e relação de todos os titulares afetados, (iv) descrição das possíveis consequências do evento, (v) indicação das medidas tomadas para reparar o dano e evitar novos incidentes.

4.2 Canais para Comunicação do Incidente

É dever de todos relatar, de boa-fé, indícios de ilicitudes e práticas não conformes em relação à segurança da informação.

Os instrumentos disponíveis para comunicação são:

- E-mail do DPO/Encarregado de proteção de dados: dpo@grupoiagsaude.com.br
- Canal de Ouvidoria disponível no site institucional (Contato e Ouvidoria – Grupo IAG Saúde (grupoiagsaude.com.br). Através deste canal poderá escolher fazer um relato anônimo ou identificar-se. As informações nele registradas serão recebidas pela área de Compliance, assegurando sigilo absoluto e o tratamento adequado de cada situação, sem qualquer conflito de interesses.

4.3 Análise e Tratativa do Incidente

O Encarregado pelo Tratamento de Dados Pessoais juntamente com o Comitê de Segurança da Informação deverá avaliar internamente o incidente – natureza, categoria e quantidade de dados afetados, consequências concretas e prováveis.

A partir da análise do incidente, ações corretivas devem ser definidas, documentadas e gerenciadas pelos seus responsáveis. A avaliação e decisão sobre eventos da segurança da informação são categorizados e priorizados levando-se em consideração os graus de risco por meio dos seguintes critérios:

Alto (Impacto Grave) – Incidente que afeta sistemas relevantes ou informações

críticas, com potencial para gerar impacto negativo sobre a receita ou clientes.

Médio (Impacto Significativo) – Incidente que afeta sistemas ou informações

não críticas, sem impacto negativo à receita ou clientes; investigações de colaboradores

com validade limitada devem ser tipicamente classificadas neste nível.

Baixo (Impacto Mínimo) – Possível incidente, sistemas não críticos;

investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

Todo processo de análise e tratativa do incidente será registrado no *REG IAG 323 – Relatório de Investigação e Tratamento de Incidentes*.

4.4 Comunicação do Incidente

A comunicação tem como objetivo informar os clientes, internos e externos, atingidos pelo incidente, por meio de canais de comunicação pré-estabelecidos;

A comunicação deverá ser direcionada aos públicos interno e externo, de acordo a pertinência para cada tipo de público.

Em caso de incidentes envolvendo dados pessoais onde o Grupo IAG Saúde se caracteriza na condição de Operador, o Encarregado de Tratamento de Dados Pessoais, deverá comunicar o incidente ao Controlador em até um dia útil, contado da data do conhecimento do incidente e compartilhar o *REG IAG 323 – Relatório de Investigação e Tratamento de Incidentes*, mesmo que ainda parcial, contemplando itens como: descrição do relato, resumo do incidente de segurança, definição dos envolvidos no incidente, análise da causa raiz e implementação de ações corretivas, resultado da apuração.

Assim que concluído o *REG IAG 323 – Relatório de Investigação e Tratamento de Incidentes*, a versão final deverá ser compartilhada com o Controlador.

Diante de um incidente de segurança em que o Grupo IAG Saúde se caracteriza como Controlador, o Comitê de Segurança da Informação, deverá avaliar internamente a relevância do risco ou dano do incidente para determinar se deverá comunicar à ANPD e ao titular.

4.5 Administração desta Política

Incentivamos os clientes, colaboradores, fornecedores e parceiros comerciais a comunicarem supostas violações destas diretrizes no canal de ouvidoria do Grupo IAG Saúde que se encontra na página de formulários de contato, no site do Grupo IAG Saúde: grupoiagsaude.com.br/fale-conosco.

O Grupo IAG Saúde está comprometido em proteger de retaliação qualquer pessoa que, agindo de boa-fé, registre uma denúncia ou ajude em uma investigação, incluindo, mas não se limitando a: suspensão, assédio, ameaças, intimidação,

coação, perda de benefícios, demissão ou qualquer outra forma de discriminação ou punição.

A ação ou a conivência que impliquem em desobediência ou inobservância das diretrizes desta política são consideradas infrações. As penalidades a que os infratores estão sujeitos são:

- Advertência
- Suspensão
- Demissão por justa causa
- Rescisão contratual

Declaramos que este documento é a cópia fiel da Política, aprovada pela Alta Direção.

Quaisquer dúvidas sobre a aplicação desta Política deverão ser reportadas à área de Compliance, através do e-mail compliance@grupoiagsaude.com.br.

5. REGISTROS

REG IAG 323 – Relatório de Investigação e Tratamento de Incidentes

6. REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001:2022 – Versão Corrigida: 2023 Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação – Requisitos. ABNT, 2023.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002:2022 Segurança da Informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação. ABNT, 2022.

POLÍTICA INSTITUCIONAL – POI IAG 024

POLÍTICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 37301:2021 Sistema de gestão de compliance – Requisitos com orientações para uso. ABNT, 2021.

PRS IAG 061 – Incidentes de Segurança da Informação, incluindo Dados Pessoais e sua Avaliação para Comunicação.