Política de Privacidade dos Dados e Segurança da Informação

POLÍTICA INSTITUCIONAL – PADRÃO: POI IAG 009

POLÍTICA DE PRIVACIDADE DOS DADOS E SEGURANÇA DA INFORMAÇÃO

Versão: 3

Aprovação: Alta Direção

1. OBJETIVO

Estabelecer as diretrizes de privacidade dos dados e segurança da informação, visando garantir os princípios básicos de integridade, confidencialidade, disponibilidade, autenticidade e legalidade das informações do Grupo IAG Saúde®.

2. ABRANGÊNCIA

Grupo IAG Saúde® e partes interessadas.

3. SIGLAS E DEFINIÇÕES

Autenticação: Procedimento utilizado na identificação de usuários, dispositivos ou processos, e que é um pré-requisito para acesso aos recursos do sistema.

Autorização: É o direito ou permissão de acesso a um recurso.

Ativos: Consiste em todo e qualquer bem tangível ou intangível pertencente, administrado, locado ou custodiado pelo Grupo IAG Saúde®, sejam informações, sistemas ou dispositivos fixos e móveis.

Confidencialidade: Consiste na propriedade da informação que determina que esta não esteja disponível ou não seja exposta a indivíduos, entidades e/ou processos que não tenham sido previamente autorizados pelo proprietário.

Comitê de Segurança da Informação: Grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação do Grupo IAG Saúde.

Criptografia: É a disciplina que trata dos princípios, meios e métodos para a transformação de dados, tornando os inteligíveis, de forma a prevenir o uso não autorizado da informação.

Disponibilidade: Consiste na propriedade da informação que garante que esta esteja disponível, sempre que necessário, para o uso legítimo, ou seja, por aqueles usuários autorizados pelo seu proprietário visando à continuidade do negócio.

Informação confidencial: Toda informação técnica, industrial, comercial e administrativa, bens, direitos de propriedade da empresa, atividade material e intelectual desenvolvidos pelo funcionário, aperfeiçoamentos técnicos, dentre outros, todos relacionados ao funcionamento e desenvolvimento da empresa e que seja transmitida ao funcionário de

forma gráfica, escrita ou de qualquer outra forma que possa ser lida por máquinas ou computadores; verbal, ou que for exibida com os dizeres "confidencial e/ou sigiloso", ou qualquer outra expressão similar. Exemplos: Informações de clientes e funcionários que devem ser protegidas por obrigatoriedade legal (Nome, CPF e etc); dados bancários, informações sobre produtos e serviços que revelem vantagem competitiva do Grupo IAG Saúde frente ao mercado; todo material estratégico do Grupo IAG Saúde (impresso ou eletrônico) que não devem ser divulgadas ao meio externo.

Integridade: Consiste na propriedade da informação que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo seu proprietário, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção, armazenamento e descarte).

Hash: Algoritmo que mapeia dados grandes e de tamanho variável para pequenos dados de tamanho fixo. As funções Hash são conhecidas por resumirem o dado. A principal aplicação dessas funções é a comparação de dados grandes ou secretos.

Privacidade dos dados: Consiste na preservação da privacidade de dados e de dados pessoais, sensíveis ou não, atendendo aos requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709, de 14 de agosto de 2018).

Segurança da Informação: Consiste na preservação da confidencialidade, da integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade e confiabilidade da informação.

4. DIRETRIZES

A informação é um dos principais patrimônios do mundo contemporâneo. Um fluxo de informação de qualidade é capaz de decidir o sucesso de uma organização. Mas esse poder, somado à crescente facilidade de acesso, faz desse ativo um alvo de constantes ameaças internas e externas.

Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos ao Grupo IAG Saúde®, seus clientes e todas as partes interessadas.

Atentos a isso, publicamos a Política de Segurança da Informação, o alicerce dos esforços de proteção à informação do Grupo IAG Saúde®.

Os princípios de Privacidade dos Dados e Segurança da Informação estabelecidos nesta política possuem total aderência da alta direção da organização. São observados por todos

na execução de suas funções, incluindo, mas não se limitando à, todos os empregados, estagiários, colaboradores, prestadores de serviços, terceiros, parceiros.

Diante disso, podemos colocar que a segurança da informação são esforços contínuos para a proteção dos ativos de informação, auxiliando o Grupo IAG Saúde® a cumprir sua missão. Para tanto, visa atingir os seguintes objetivos:

a) Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
b) Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;
c) Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las;

Com a intenção de aumentar a segurança da infraestrutura tecnológica, a presente política está baseada na norma ABNT NBR ISO/IEC 27001:2013, reconhecida mundialmente para a gestão da segurança da informação, bem como na Lei Geral de Proteção de Dados do nosso país (LGPD). De acordo com a LGPD se caracteriza como controlador quando gera os dados pessoais e operador quando opera os dados pessoais gerados pelos clientes (hospitais e operadoras).

O Grupo IAG Saúde no tratamento de dados de caracteriza como:

Controlador

Tratamento de Dados dos Colaboradores

Tratamento de Dados de Terceiros (Fornecedores e Parceiros)

Tratamento de Dados de Usuários que Acessam as Mídias do Grupo IAG Saúde

Operador

Tratamento de Dados dos Pacientes nas soluções DRG Brasil

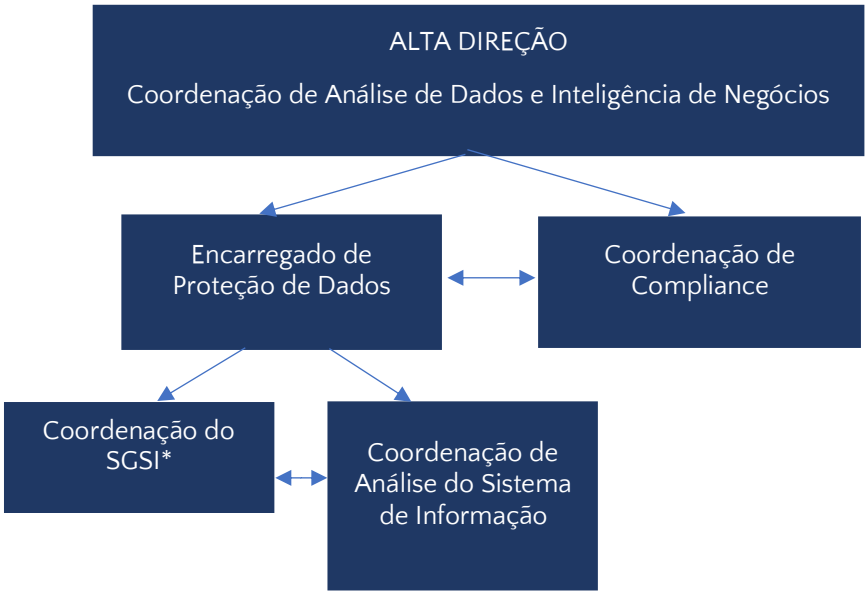
Tratamento de Dados dos Médicos nas soluções DRG Brasil

Tratamento de Dados dos Usuários nos softwares e apps do Grupo IAG Saúde

Para reafirmar o compromisso com a segurança, privacidade e a transparência no tratamento de dados pessoais, o Grupo IAG Saúde estabelece suas diretrizes por meio dos Termos de Uso e Políticas de Privacidade disponíveis em seus sites e softwares, que tem por finalidade prestar informações sobre a coleta, uso, armazenamento, proteção,

compartilhamento e direitos dos usuários em relação a seus dados pessoais (“Informações Pessoais”) quando da utilização das funcionalidades.

ORGANOGRAMA DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO – SGSI



*SGSI: Sistema de Gestão de Segurança da Informação

Alta Direção	Responsável pela análise de dados e inteligência de negócios, além da supervisão de uma série de funções relacionadas a dados que incluem o gerenciamento, a garantia da qualidade e o estabelecimento de estratégias que suportem a gestão e qualidade dos dados.
Encarregado de Proteção de Dados (DPO)	Conscientiza e aconselha a organização de suas obrigações de proteção de dados. Garante, de maneira independente, que a organização aplique as leis que protegem os dados pessoais dos indivíduos. Reporta diretamente à alta direção.
Coordenação de Compliance (CCO)	Responsável pela supervisão e gerenciamento do compliance da organização. Sua atribuição é a de garantir que todos os procedimentos realizados pelos funcionários estão de acordo com os regulamentos internos e com as leis externas à empresa. Cria e dissemina o programa de compliance, garantindo que todos os detalhes que compõem os processos de trabalho do dia a dia tenham sido previstos e orientados em um código de conduta. Reporta

	diretamente à alta direção.
Coordenação do Sistema de Gestão de Segurança da Informação (SGSI)	Responsável por estabelecer e manter a visão, estratégia e programa da empresa para garantir que os ativos e tecnologias da informação sejam adequadamente protegidos. Orienta a equipe na identificação, desenvolvimento, implementação e manutenção de processos em toda a empresa para reduzir os riscos de informações e tecnologia da informação.
Coordenação de Análise do Sistema de Informação	Responsável pelo estudo dos sistemas e procedimentos atuais da organização e por projetar soluções de sistemas de informação para ajudar a organização a operar com mais eficiência e eficácia. Reúne negócios e tecnologia da informação, entendendo as necessidades e limitações de ambos. Trabalha cooperativamente com a coordenação de SGSI.

4.1 Uso de Dispositivo Móvel

O Grupo IAG Saúde deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite o uso de dispositivos móveis. Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição como: notebooks e tablets

São diretrizes desta seção:

- É compromisso do colaborador, não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de sua função e permissão de acesso;
- É proibido o armazenamento de informações confidenciais do Grupo IAG Saúde;
- Utilize sempre telas de bloqueio automático com senhas para seu dispositivo móvel;
- Não conecte em redes de Wi-Fi desconhecidas, essas redes podem conter mecanismos de captura de dados;
- Desconfie de e-mails de origem desconhecida, não clique em links que venham nestes emails, não baixe anexos nem tão pouco informe dados pessoais.
- É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo Grupo IAG Saúde, notificar imediatamente a sua Gerência. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

4.2 Teletrabalho

A realização do Teletrabalho deverá ser realizada em local seguro, onde a privacidade das informações será garantida. São diretrizes desta seção:

- Não é permitido o trabalho em locais como aeroportos, transportes públicos, restaurantes, entre outros.
- É imprescindível o uso dos equipamentos cedidos pela empresa, como exemplo: computadores, notebooks e tablets.
- Todo acesso remoto a sistemas e ambientes de tecnologia que suportam informações corporativas do Grupo IAG Saúde é precedido, obrigatoriamente, por um processo de autenticação do usuário, pessoal e intransferível.
- As comunicações e transferências de dados ocorridas devem respeitar as premissas do Código de Ética e Conduta do Grupo IAG Saúde e operacionalizadas pelo e-mail corporativo.
- Para execução das atividades profissionais, deverá utilizar a rede de internet de sua própria residência ou do local previamente determinado para a execução das atividades, abstendo-se de utilizar redes públicas ou de terceiros, desconhecidas e que não ofereçam padrões mínimos de segurança e proteção.
- É responsabilidade do funcionário respeitar às diretrizes de segurança da informação, obrigando-se a comunicar imediatamente ao Encarregado de Proteção de Dados do Grupo IAG Saúde qualquer evento ou situação relacionada à suspeita ou ocorrência de vazamento de dados, perda ou extravio de mídias de armazenamento, documentos ou outros fatos que indiquem riscos à segurança e proteção de dados para que seja adotada as providências necessárias.

4.3 Controle de Acesso

Todo acesso à informação será dado através de mecanismos de controle de acesso. Qualquer mudança funcional implicará na revisão dos direitos de acesso à informação.

4.3.1 Sigilo de Informações Confidenciais e Dados de Acesso Internos

Na admissão o funcionário assina um contrato declarando a sua ciência e responsabilidade com as obrigações de privacidade e confidencialidade assumidas no contrato que irão prevalecer mesmo após o término ou rescisão do contrato de trabalho.

Todo funcionário, de acordo com suas funções, terá senha pessoal e intransferível para acesso ao e-mail corporativo, softwares, redes sociais, sites de compras, entre outros.

4.3.2 Acesso às redes e aos serviços de rede

Toda solicitação de acesso aos sistemas do Grupo IAG Saúde deverá ser autorizada pelo encarregado de proteção de dados. Os acessos serão concedidos após a sua aprovação respeitando as permissões especificadas no Mapeamento de Acessos.

4.3.3 Alteração de Perfis de Acesso

Quando houver mudança nas atribuições de um colaborador ou quando ocorrer o seu remanejamento para outra atividade, os perfis de acesso deverão ser readequados, através do preenchimento do Mapeamento de Acessos no SigQuali e aprovação do Encarregado de Proteção de Dados.

4.3.4 Revogação de Perfis de Acesso

No desligamento de funcionários a remoção dos acessos será solicitada pelo Departamento Pessoal através do preenchimento do Formulário - Check List Retirada dos Acessos com as informações (nome do funcionário e data para retirada dos acessos). O formulário deverá ser encaminhado via e-mail para áreas afins com cópia para a Gerência responsável. Após a conclusão do processo, os formulários serão publicados no SigQuali.

4.3.5 Auditoria dos Acessos

Anualmente são realizadas auditorias no banco de dados para verificação da conformidade dos perfis de acesso dos funcionários do Grupo IAG Saúde.

4.4 Controles Criptográficos

O Grupo IAG Saúde para a criptografia dos dados pessoais utiliza a solução KMS – Key Management Service da AWS (Amazon Web Services), que permite o controle centralizado das chaves de criptografia usadas para proteger os dados que estão sob o controle do grupo. É um serviço seguro e resiliente que usa módulos de segurança de hardware validados ou em processo de validação, para proteger as chaves criptográficas, garantindo uma maior escalabilidade para gerenciar as chaves de aplicativos e licenças de *softwares*, ou para efetuar verificações de consistência da criptografia dos dados.

O AWS KMS é integrado aos demais serviços da AWS, tornando mais fácil criptografar os dados armazenados nesses serviços e controlar o acesso às chaves que o descriptografam. É também integrado com o AWS CloudTrail, que oferece a habilidade de auditar quem usou quais chaves, em quais recursos e quando, fornecendo logs contendo toda a utilização das chaves para ajudar a cumprir requisitos normativos e de conformidade.

Ao usar o AWS KMS, é possível obter mais controle sobre o acesso aos dados que são criptografados, usando os recursos de criptografia e gerenciamento de chaves diretamente nos aplicativos ou por meio dos serviços da AWS integrados ao AWS KMS.

É um serviço gerenciado, que possibilita concentrar as necessidades de criptografia dos aplicativos enquanto a AWS lida com a disponibilidade, segurança física e manutenção de hardware da infraestrutura adjacente. Apresenta ainda:

- Gerenciamento de Chaves Centralizado – fornece um controle centralizado de chaves de criptografia.

- Integração com os serviços AWS – O Key Managemant Service tem total integração a vários outros serviços da AWS. Essa integração significa que é possível facilmente usar as chaves mestras do AWS KMS para criptografar os dados armazenados nesses serviços, trazendo assim maior segurança, funcionamento e facilidade para os serviços.
- Criptografia de envelopamento – a criptografia de envelope pode oferecer benefícios significativos de desempenho. Quando criptografa diretamente os dados com o KMS, eles precisam ser transferidos pela rede. A criptografia de envelope reduz a carga da rede para seu aplicativo ou serviço de nuvem da AWS. Apenas a solicitação de preenchimento da chave de dados pelo KMS precisa passar pela rede. Como a chave de dados é sempre armazenada de forma criptografada, é fácil e seguro distribuir a chave quando precisar, sem se preocupar com sua exposição. Chaves de dados criptografadas são enviadas para o AWS KMS e descriptografadas com chaves mestras para finalmente permitir que sejam descriptografados os dados. A chave de dados está disponível diretamente no aplicativo sem precisar enviar o pacote todo de dados para o AWS KMS e passar pela latência da rede, gerando assim uma maior segurança para a criptografia e descriptografia dos dados.

- Auditoria integrada – com o AWS CloudTrail é possível a gravação de logs do uso de cada uma das chaves armazenadas, armazenando automaticamente data, hora, chave utilizada e os dados do usuário que a manipulou. Assim cada utilização de uma chave armazenada no KMS é registrada em um arquivo de log, armazenado automaticamente no serviço do AWS CloudTrail.

- Seguro – KMS é projetado para que ninguém tenha acesso às suas chaves mestras. O serviço é criado em sistemas que protegem as chaves mestras com amplas técnicas de segurança.

- Conformidade – Para garantir a maior segurança e confiabilidade no uso e armazenamento de chaves de criptografia, a AWS KMS está em conformidade com os principais controles de qualidade e segurança, tais como ISO 9001 e ISO 27017.

A partir desse recurso, o Grupo IAG Saúde mantém um controle criptográfico de usuários e informações sensíveis, em todos os bancos de dados de suas aplicações, onde as tabelas responsáveis por armazenar tais informações, mantém todos os registros criptografados, garantindo a segurança e confiabilidade dos dados armazenados.

4.5 Gerenciamento de chaves centralizado

O AWS KMS fornece um controle centralizado de chaves de criptografia. Ele permite criar, importar, ou modificar facilmente as chaves de criptografia, além de definir políticas de uso, auditoria, utilização por meio de controle de gerenciamento da AWS usando o AWS SDK ou ainda a CLI.

As chaves mestras do KMS, sejam elas importadas ou criadas, são armazenadas em um local resiliente, com seu formato criptografado, para ajudar a garantir sua recuperação quando necessário. Pode ser configurado para que o KMS mude automaticamente as chaves criadas diretamente no KMS uma vez por ano sem a necessidade de criptografar novamente todos os dados que já estavam criptografados com a chave mestra. Não é preciso monitorar as versões anteriores da chave mestra, pois o próprio KMS as mantêm disponível para descriptografar dados anteriormente criptografados. Também existe a possibilidade de criar chaves mestras, e controlar quais usuários têm acesso a essas chaves e com quais serviços elas podem ser usadas, sempre que for necessário. Também é possível importar chaves de outras infraestruturas de gerenciamento de chaves e usá-las em outros serviços da AWS com o gerenciamento do AWS KMS.
Os principais recursos do gerenciamento de chaves do AWS KMS são:

- Criar chaves com alias e descrição exclusivas;
- Importação de chaves de infraestruturas externas à AWS;
- Definir quais usuários e funções do IAM (Identity and Access Management) podem gerenciar as chaves;
- Definir quais usuários do IAM (Identity and Access Management) podem usar a chave para criptografar e descriptografar dados;
- Possibilita a rotação automática de chaves anualmente;
- Desabilitação de chaves temporariamente para evitar uso indevido;
- Auditar o uso de chaves inspecionando os logs do AWS CloudTrail.

Com o KMS fica mais seguro implementar e manipular serviços e aplicativos na AWS, tendo uma infraestrutura escalável e confiável para a manipulação dos dados totalmente criptografados. O AWS KMS garante as conformidades e a total segurança da manipulação dos dados, e com a técnica de envelopamento torna os dados de suas aplicações mais seguros, ocasionando assim um maior conforto e proteção para os serviços e aplicações.

Nas APIs oferecidas pela plataforma DRG Brasil, temos o controle de chave individualizada por cliente, criada diretamente no AWS- Amazon pela API Gateway.

O API Gateway é uma ferramenta de gerenciamento de API que fica entre um cliente e uma coleção de serviços de back-end. Um API gateway atua como um proxy reverso para aceitar todas as chamadas de interface de programação de aplicativos (API), agregar os vários serviços necessários para atendê-las e retornar o resultado apropriado.

4.6 Mesa Limpa e Tela Limpa

Esta política se refere a práticas para assegurar que informações, tanto em formato digital quanto físico, e ativos (notebooks, tablets, etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo ou ao final do dia.

Uma vez que informações e ativos em uma área de trabalho estão em um de seus lugares mais vulneráveis (sujeitos a divulgação ou uso não autorizado), a adoção de uma política de mesa limpa e tela limpa é uma das principais estratégias a se utilizar na tentativa de reduzir os riscos de falhas de segurança.

No Grupo IAG Saúde, para reduzir riscos de acesso não autorizados, perda e dano da informação durante e fora da jornada de trabalho, algumas diretrizes foram estabelecidas, sendo elas:

- O armazenamento de quaisquer documentos físicos, sejam eles confidenciais, internos ou de uso pessoal devem, em situações de ausência temporária durante ou fora do expediente, ser armazenados em locais protegidos e seguros trancados à chave ou formas similares por seu responsável;
- O armazenamento de quaisquer documentos digitais, sejam eles confidenciais, internos ou de uso pessoal devem, em situações de ausência temporária durante ou fora do expediente, ser armazenados em locais protegidos e seguros, como aplicativos disponibilizados na Nuvem, por ex.: Google Drive, Nuvem da Microsoft (Office 365).
- Deve ser mantida diariamente a limpeza da área de trabalho, garantindo adequada organização dos arquivos.
- Todo documento que contenha dados, informação confidencial ou reservada deve ser eliminado através de destruição apropriada, impossibilitando a reconstrução.
- Quando se ausentar da estação de trabalho, e-mail/sistemas devem ser fechados e a tela do computador bloqueada;
- Ao final do dia os dispositivos devem ser desligados.

4.7 Cópias de Segurança das Informações

As informações do Grupo IAG Saúde são um ativo importante e, por isso, as cópias de segurança, devem ser realizadas periodicamente, certificando-se que elas sejam restauradas caso seja necessário.

Para armazenar os dados, o Grupo IAG Saúde, optou pelo armazenamento em Nuvem, por fornecer mais segurança e facilidade de acesso aos dados em comparação a outros meios e por ter um gerenciamento mais simples e rapidez no acesso aos arquivos, já que pode-se ter o acesso randômico.

Os dados do Grupo IAG Saúde estão armazenados em dois grandes repositórios em nuvem, de dois provedores diferentes, a saber:

1) Amazon Web Services (AWS)
2) Microsoft (Office 365)

Os dados hospedados na AWS estão relacionados às informações trafegadas nos seguintes sistemas/softwares: SigQuali®, DRG Brasil® e suas soluções, Siscorp®, Ambiente Virtual de Aprendizagem (Moodle), Mantis (sistema de abertura de chamados para os Analistas de Sistemas), sites.

Nesse ambiente, todos os backups são automatizados por sistemas de agendamento para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos softwares.

Diariamente, são disparados e-mails da confirmação da realização dos backups dos ambientes na AWS.

Com relação aos dados hospedados na Nuvem da Microsoft (Office 365) a política de backup seguida é da própria Microsoft. Com a abordagem da Microsoft, o acesso aos dados de clientes é rigidamente controlado e registrado, e auditorias de amostra são realizadas pela Microsoft e terceiros. Fornecem ainda recursos de controle de acesso e de gerenciamento de identidade. Incluem um armazenamento baseado na nuvem para os dados de diretório e um conjunto principal de serviços de identidade, incluindo processos de logon de usuário e serviços de autenticação.

4.8 Desenvolvimento Seguro

O Grupo IAG Saúde possui métodos que garantem a qualidade durante todas as etapas do desenvolvimento, além da realização de uma análise do processo de desenvolvimento de software.

Abaixo, estão relacionadas algumas boas práticas de segurança que são adotadas:

- Gerenciamento de código fonte – utilização de ferramenta para gerenciamento de código fonte que permite organizar a interação entre desenvolvedores, garantindo a integridade e possibilitando o gerenciamento de versões do código, evitando equívocos quanto a versão colocada em produção;
- Realização de testes – execução de testes desde pequenos trechos de código por vez (como os testes unitários) até práticas que buscam uma avaliação geral do software;

- Gerenciamento de correção de bugs – utilização de uma ferramenta de Bug Tracking (Mantis) permite manter registro das falhas encontradas nos sistemas e facilita a comunicação entre os envolvidos na identificação e correção de bugs;
- Utilização de processo de integração contínua – essa prática visa garantir a qualidade no software desenvolvido, automatizando verificações no processo de build da ferramenta, garantindo assim, que seja possível gerar um novo release com o mínimo possível de bugs;
- Documentação do software e da arquitetura que o suporta – uma documentação clara da arquitetura e código fonte ajuda a aumentar a qualidade do software desenvolvido. Uma documentação clara, objetiva e bem estruturada é de fundamental importância para que o software possa ser expandido de forma sustentável e segura;
- Utilização de padrões de código seguro e checklists – são utilizados padrões de códigos seguros e boas práticas de acordo com a linguagem adotada e ambiente definido. São usados checklists para verificar as principais ações durante o desenvolvimento e revisão de segurança do software.

O Grupo IAG Saúde possui ainda práticas de Desenvolvimento Seguro de Software que passa pelos seguintes temas e subtemas:

- ✓ Armazenamento de dados
  - Procedimentos e Meios para Armazenamento de Dados;
  - Permissões para Acesso a Informações em Bancos de Dados;
  - Gerenciamento e Distribuição de Senhas para Acesso a Dados.
- ✓ Gerenciamento de acessos e permissões de usuários;
  - Autorização e Autenticação de Usuários;
  - Autenticação em Sistemas Web.
- ✓ Comunicação Segura;
- ✓ Ataques a sistemas e suas defesas;
- ✓ Auditoria, Rastreamento e logs;

- ✓ Prevenção, Reação e mitigação de falhas de segurança
- ✓ Separação ambientes de desenvolvimento e ambientes de produção;

  Ambiente de desenvolvimento conta com acesso remoto pela Amazon WorksSpaces e acesso via VPN ao banco de dados, com rastreamento e controle de log. Nenhum dado é armazenado de forma local em nenhum dispositivo dos colaboradores/prestadores de serviço.
- ✓ Parametrização para proteção de dados
  - Criptografia e hash;
  - Gerenciamento de senhas;
- ✓ Ciclo de vida de software
  - Verificação dos requerimentos de software e sistema;
  - Análise de implementação das políticas e rotinas de segurança de software;
  - Análise e criação da estrutura do software;
  - Desenvolvimento do código do programa;
  - Teste, depuração e busca por erros;
  - Instalação, suporte e manutenção de todos os sistemas interligados ao software.

Para tornar os sistemas desenvolvidos mais seguros, são realizados alguns procedimentos, como:

- Na etapa de classificação de requisitos e formação da equipe de desenvolvimento, é identificada a necessidade de utilização de métodos de criptografia, segurança de usuários, treinamento e, em alguns casos, questões legais envolvendo licenciamento e manipulação de dados;
- Quando a arquitetura do software é projetada, é considerado o nível de segurança da arquitetura e da linguagem escolhida, as possíveis vulnerabilidades que o sistema pode apresentar e quando e como os métodos de autenticação e envio de dados seguro serão utilizados;
- É elaborada uma documentação com todos os requerimentos de segurança listados para a equipe. O time trabalha de acordo com as definições de segurança do projeto, usando as ferramentas da arquitetura e buscando vulnerabilidades da maneira correta;
- Antes de disponibilizar os sistemas para os clientes, são executados testes nos métodos de segurança para garantir a segurança dos sistemas. Nessa etapa, é importante garantir que todos os blocos de código que envolvem informações sensíveis não tenham brechas que possam comprometer a segurança do usuário;

- Após as versões de sistemas estarem disponíveis para os clientes, monitoramento em busca de falhas de segurança continuam sendo executadas.

4.9 Segurança da Informação no Relacionamento com os Fornecedores

Todos os fornecedores do Grupo IAG Saúde se obrigam a cumprir todos os requisitos da legislação vigente sobre o Acesso e Proteção de Dados Pessoais, as normas do Conselho Federal de Medicina – CFM, da Agência Nacional de Saúde Suplementar – ANS, bem como outras normas específicas e aplicáveis, brasileiras ou internacionais.

Todas as informações, documentos e comunicações por meio físico ou eletrônico utilizadas para o cumprimento de contrato são de caráter sigiloso, vedado à divulgação para terceiros, sem a prévia autorização por escrito do Grupo IAG Saúde.

Os termos de confidencialidade e deveres referentes à proteção de dados permanecerão vigentes mesmo após o encerramento do contrato com o Grupo IAG Saúde.

5. REGISTROS

- Mapeamento de Acessos
- Check List Retirada dos Acessos
- Backups
- Contratos assinados

6. REFERÊNCIAS

BRASIL. Lei nº 13709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível: em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 de Agosto de 2018.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT, 2013.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27701 – Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. ABNT, 2019.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 29151 – Tecnologia da informação – Técnicas de segurança – Código de prática para proteção de dados pessoais– Diretrizes. ABNT, 2020.

KMS – Key Management Service – Disponível em: https://aws.amazon.com/pt/kms/ Acesso em: 05 de Dezembro de 2020.

Microsoft – Disponível em: https://legal.office.com/pt-BR/docid24 Acesso em: 05 de Dezembro de 2020.