POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

V 5.0 - dez. 2022

introdução

Introdução

A HealthBit Inteligência em Saúde, assumindo o dever de zelar pela preservação completa das informações recepcionadas e transmitidas em decorrência de sua atuação, considerando a necessidade de criar diretrizes de atuação para todos os seus colaboradores e fornecedores em geral, resolve publicar a presente Política de Segurança da Informação, nos termos abaixo especificados.

As normas que compõe o presente documento foram redigidas em respeito e observação às leis brasileiras aplicáveis ao tema, dentre as quais destacam-se:

- Constituição Federal
- Código Civil
- Marco Civil da Internet Lei nº 12 965 14
- Lei nº 9 610 98 Direitos Autorais
- Lei nº 9 609 98 Propriedade Intelectual
- Lei nº 12 846 13 Lei Anticorrupção
- Lei nº 13 709 18 Lei Geral de Proteção de Dados
- ABNT NBR ISO/IEC 27002 2013 Tecnologia da informação Técnicas de segurança Código de prática para controles de segurança da informação

objetivo

Objetivo

A publicação desta Política de Segurança da Informação se faz com o intuito de estabelecer publicamente o compromisso da HealthBit em proteger as informações por nós recebidas ou produzidas, a fim de criar orientações gerais contra eventuais modificações, divulgações indevidas ou destruição das mesmas.

Todos os nossos funcionários, executivos, prestadores de serviços, consultores, fornecedores em geral e parceiros devem seguir e respeitar as diretrizes de segurança ora publicadas, sem distinções ou exceções, nos moldes estipulados neste documento

compromissos da HealthBit

Aos colaboradores

Para viabilizar o cumprimento das normas aqui dispostas, a HealthBit se compromete a disponibilizar aos colaboradores treinamentos, processos e tecnologias voltados ao auxílio na execução das atividades e preservação das informações, atuando ativamente no desenvolvimento e implementação de controles de segurança.

Aos Clientes e à sociedade em geral

Assumimos o dever de atuar em um ambiente ético, seguro e controlado, com objetivo de garantir sigilo, confidencialidade, integridade e disponibilidade das informações por nós custodiadas ou de nossa propriedade, garantindo um ambiente com o nível adequado de segurança para a preservação da informação.

A HealthBit fomenta a conscientização sobre segurança da informação, influenciando todos os envolvidos em suas atividades, de forma direta ou indireta, para fins de contribuir com a criação de uma cultura de proteção contínua.

diretrizes de segurança

Respeito à Privacidade e Proteção de Dados Pessoais Lei nº 13.709/2018

Os processos e sistemas da HealthBit devem ser estruturados em conformidade com a Lei nº 13 709 2018 Lei Geral de Proteção de Dados, cumprindo ainda com os requisitos mínimos de segurança técnica e boas práticas de segurança corporativa, exigidos pela legislação.

Os contratos envolvendo tratamento de dados pessoais e dados pessoais sensíveis da HealthBit devem ter sua finalidade e resultados descritos, devendo também os clientes e parceiros moverem esforços para conformidade com a lei.

Serão observados os princípios da necessidade, adequação, qualidade dos dados, livre acesso ao titular, segurança, transparência, prevenção, finalidade e não discriminação, além da garantia à confidencialidade, integridade e disponibilidade dos dados.

O tratamento deve ser feito com a coleta mínima de dados, visando resultado compatível com a finalidade da coleta e utilizando de meios técnicos e administrativos para proteger os dados pessoais de acessos indevidos ou situações de tratamento inadequadas.

Identificação dos usuários

O acesso às informações produzidas ou recepcionadas pela HealthBit é concedido mediante identificação do usuário previamente autorizado, após a assinatura de um termo de acesso e confidencialidade pelo usuário, estabelecendo as responsabilidades deste.

A identificação é única, pessoal e intransferível, não devendo ser compartilhada com terceiros Os usuários recebem através de endereço eletrônico um login e senha para acesso aos sistemas/softwares da HealthBit, quando aplicável, com 10 caracteres ou mais, sendo devidamente instruídos a realizar a troca imediata da senha enviada.

A HealthBit faz diferenciações de acordo com o perfil do usuário, considerando as seguintes segmentações:

- Colaboradores
- Prestadores de serviço
- Estagiários
- Clientes

O usuário é o responsável pelas atividades realizadas com a utilização de sua identificação, devendo memorizar sua senha, não sendo permitido manter o registro em papel. Na hipótese de suspeita de quebra de sigilo, o usuário deve efetuar imediatamente a troca de sua senha, tomando as providências para comunicação de quaisquer incidentes à HealthBit.

Gestão e acesso às informações

O acesso às informações geradas ou recepcionadas pela HealthBit deve se limitar ao mínimo necessário para que cada colaborador realize suas atividades, devendo ser concedida por meio de identificação de acesso, única e intransferível para cada colaborador.

Para concessão do acesso, os colaboradores comprometem se a agir em conformidade com a presente Política de Segurança da Informação, submetendo se ainda ao Termo de Confidencialidade firmado junto à HealthBit. As concessões de acesso aos recursos e informações sob a guarda da HealthBit devem ser revisadas trimestralmente, a fim de evitar acessos não autorizados. Na hipótese de desligamento do funcionário da HealthBit, os acessos serão excluídos e desabilitados no prazo máximo de 72 (setenta e duas horas).

Nos casos de obtenção de informação de terceiros, a HealthBit providenciará a documentação formal relativa à cessão de direitos sobre as informações, antes de seu uso, garantindo o acesso apenas por pessoas autorizadas. No que toca aos sistemas disponibilizados à clientes, a HealthBit mantém a gestão dos acessos liberados e condiciona o mesmo à assinatura de termos de sigilo e cessão de acesso, com tratativa especial para acessos com informações de saúde. A HealthBit inspeciona, trimestralmente, os acessos ativos nos sistemas, para fins de conferência e gestão das cessões. Além disso, contratualmente é estabelecida a obrigação dos clientes da HealthBit comunicarem sobre o desligamento do funcionário cujo acesso foi solicitado no prazo de 48 (quarenta e oito) horas.

Treinamentos de segurança da informação

A HealthBit somente fornecerá acesso às informações sob sua responsabilidade para os usuários com a devida capacitação dos processos de negócio e da utilização dos recursos básicos para a realização de suas atividades.

Para tanto, o conhecimento em Segurança da Informação deve ser constantemente difundido, de forma a propiciar a conscientização de sua importância na atuação da HealthBit. Os usuários devem manter se informados sobre os requisitos adotados para minimizar os riscos à segurança das informações.

Além disso, os usuários devem estar cientes sobre as responsabilidades administrativas, legais e sanções decorrentes da má utilização dos recursos colocados à sua disposição.

Tratamento das informações

Toda informação criada, manuseada, armazenada, transportada ou descartada pelos colaboradores, no exercício de suas atividades, deve ser considerada como propriedade da HealthBit, seguindo as regras definidas neste documento e em normas de segurança correlatas.

Após recepcionadas, as informações sob a guarda da HealthBit devem ser tratadas conforme a classificação de sensibilidade e criticidade no manuseio, transporte, guarda e descarte, devendo ser preservado o sigilo das informações pelos usuários com acesso no exercício de suas funções.

No caso de não utilização e necessidade de manutenção, as informações devem ser armazenadas de forma segura, observando se padrões mínimos de segurança. Da mesma forma, sendo necessária a eliminação das informações, a HealthBit se compromete a adotar procedimento que impossibilite a recuperação total ou parcial das informações, declarando formalmente a exclusão.

Classificação das informações

A HealthBit deve adotar, para todas as informações sob sua guarda, a classificação quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita.

A informação que não possuir uma classificação explícita deve ser considerada de uso restrito às instalações da HealthBit.

Todos os colaboradores devem ser capazes de identificar a classificação de segurança atribuída a uma informação na HealthBit e tratá la conforme os mecanismos de proteção estabelecidos.

Segregação de função

As atividades da HealthBit devem ser executadas de maneira a proporcionar a segregação das funções, garantindo que o controle das tarefas de um processo seja sempre compartilhado. É vetado que apenas um único colaborador possua controle de um processo por inteiro, a fim de evitar a perda das informações ou condução inapropriada da atividade

As atividades de controle e execução da HealthBit devem ser realizadas por usuários distintos, de forma a garantir a verificação da integridade do processo O controle dos processos deve ser executado por uma liderança de equipe, visando garantir a rastreabilidade do processo e posterior auditoria pelos órgãos competentes.

Continuidade nos negócios

As informações de responsabilidade da HealthBit devem ser tratadas com a utilização de mecanismos que resguardem sua perda e destruição, intencional ou acidental, com o intuito de minimizar os riscos de vazamento dos dados.

Para tanto, a HealthBit realizará processos de auditoria, de forma a aferir o cumprimento da presente Política de Segurança da Informação, bem como seguirá um processo de gestão de continuidade dos negócios, mantido e trimestralmente testado, visando reduzir, a um nível aceitável, a possibilidade de interrupção dos serviços causada por desastres ou falhas nos recursos que suportam os processos críticos da HealthBit.

Além disso, a fim de garantir a segurança das informações, as lideranças de equipe da HealthBit são instruídas a assegurar que não haja um único colaborador com a operação exclusiva de um ou mais processos críticos, em conformidade com o princípio de segregação de funções acima exposto.

Gestão de rescursos

Os recursos da HealthBit são geridos e controlados através do setor de Desenvolvimento e Tecnologia da Informação, juntamente com a área administrativa, que mantém inventário atualizado sobre os equipamentos de propriedade da HealthBit e a disponibilização dos mesmos para os funcionários.

Os ativos tecnológicos são contabilizados trimestralmente, sendo feita a análise e conferência do uso dos equipamentos. Da mesma forma, a equipe de Desenvolvimento e Tecnologia da Informação procede com a verificação de atualizações necessárias, sistemas necessários e softwares instalados nos computadores e dispositivos de forma mensal, mantendo contato com os colaboradores para a melhor utilização dos recursos.

Utilização dos recursos

Os recursos da HealthBit são disponibilizados aos colaboradores para atender aos interesses da empresa em suas atividades profissionais. Todos os recursos computacionais, sejam estes hardware ou software, devem ser devidamente homologados pela Equipe de Desenvolvimento e Tecnologia da Informação para sua utilização pelo usuário.

Os colaboradores são responsáveis pelos recursos colocados à sua disposição, devendo preservá los em bom estado de uso, respondendo por qualquer dano causado por má utilização. Os ambientes onde se encontram instalados ou armazenados os recursos devem permanecer protegidos, inclusive na ausência do colaborador.

Equipamentos portáteis devem possuir controle de acesso e mecanismos de proteção física, sendo que eventuais alterações na configuração dos recursos só poderão ser feitas quando autorizadas.

Os recursos de propriedade da HealthBit só poderão ser removidos das instalações da empresa com autorização do líder da equipe do colaborador solicitante, e de modo excepcional. Além disso, toda transferência de recurso, interna ou externa, deve ser oficialmente comunicada à equipe competente.

A utilização de recursos no âmbito da HealthBit deve respeitar a legislação vigente, principalmente no que se refere a direitos autorais e patentes.

Instalação, Configuração e Manutenção de Sistemas Operacionais

A instalação, configuração, manutenção ou desinstalação do sistema operacional utilizado nos servidores de rede, estações de trabalho e notebooks de propriedade da HealthBit é de responsabilidade da Equipe de Desenvolvimento e Tecnologia da Informação, que deve também documentar e atualizar os procedimentos de instalação e configuração dos sistemas operacionais.

As atualizações dos servidores de rede devem ser precedidas de cópia de segurança da partição destinada ao sistema operacional. Além disto, os servidores de rede, estações de trabalho, notebook e equipamento de conectividade switch, router e afins) devem ser configurados de forma a:

- Manter a data e hora sincronizadas
- Desabilitar ou desinstalar os serviços desnecessários para sua utilização
- Emitir alertas nos casos de ocorrência de erro que provoquem sua indisponibilização total ou parcial
- Gravar logs das principais ocorrências

A equipe de Desenvolvimento e Tecnologia da Informação da HealthBit verificará a necessidade de atualização mensalmente.

Segurança física

A HealthBit realiza o controle de segurança física para acesso aos ambientes da empresa, de forma que apenas é permitido o acesso a pessoas previamente autorizadas e identificadas. No caso de terceiros com acesso autorizado ao ambiente físico da empresa, a visita e permanência é permitida tão somente mediante acompanhamento de funcionário.

Além disto, a HealthBit toma as pro vidências para proteção de suas instalações, com a presença dos devidos alarmes, trancas, monitoramento de segurança, extintores e demais equipamentos necessários para guarda do ambiente.

Ressalta se ainda que são contratados os seguros necessários ara a minimização dos riscos para as instalações físicas da empresa, com coberturas contratadas para todas as perdas e danos que eventualmente a HealthBit vier a sofrer.

Mesa e tela limpa

A HealthBit orienta seus funcionários à, quando se ausentarem de suas respectivas mesas, efetuarem o bloqueio da estação de trabalho com senha, aplicando se o mesmo para equipamentos portáteis.

Além disso, os usuários deverão manter suas mesas limpas, sem a presença de papéis ou conteúdos que contenham informações relacionadas à HealthBit, bem como, deverão manter telas abertas apenas quando necessário em seus computadores, a fim de evitar a visualização por terceiros

Desenvolvimento seguro

A Equipe de Desenvolvimento e Tecnologia da Informação da HealthBit somente utiliza computadores corporativos fornecidos para desenvolvimento, com a faculdade de utilizar Windows ou Linux como sistema operacional. Os códigos desenvolvidos são centralizados nos repositórios privados da Healthbit através do serviço GitHub, onde cada desenvolvedor tem sua chave de segurança cadastrada.

Os desenvolvedores são divididos em grupos, com diferentes acessos aos repositórios.

A HeathBit esclarece que o deploy dos sistemas é feito apenas pelos responsáveis por cada projeto, com o acesso aos servidores limitado por SSH com autenticação baseada em par de chaves de segurança. Os usuários com acesso ao servidor possuem, cada um, suas próprias chaves de segurança RSA 4096.

As chaves de segurança são alteradas pela HealthBit a cada seis meses.

A HealthBit assume seu compromisso com o desenvolvimento seguro e com as melhores técnicas utilizadas no mercado.

Licença de uso

A HealthBit veta a realização de cópia, distribuição ou alteração de softwares que necessitem de licença previamente legalizada. Para o uso autorizado de sistemas desta natureza deverão ser obtidas as respectivas licenças, a fim de proporcionar uma atuação em conformidade com as leis em vigor.

Os softwares considerados de uso público ou livre podem ser utilizados, uma vez que além de usar, contribuímos com o software livre, de acordo com as diretrizes inseridas na presente Política de Segurança da Informação.

Qualquer instalação de software em equipamentos da HealthBit, seja público ou por meio de licença, deve ser realizada de forma controlada, com uma análise de compatibilidade com as atividades dos colaboradores e/ou prestadores de serviço da HealthBit.

Gerenciamento de mudanças

A Equipe de Desenvolvimento e Tecnologia da Informação da HealthBit gerencia e controla as mudanças realizadas e todas as alterações feitas em ambiente produtivo.

Todas as mudanças são feitas apenas mediante a documentação e aprovação pelas partes interessadas

Os códigos desenvolvidos são centralizados nos repositórios privados da Healthbit através do serviço GitHub, onde cada desenvolvedor tem sua chave cadastrada. Os desenvolvedores são divididos em grupos, com diferentes acessos aos epositórios, conforme mencionado nesta Política.

propriedade intelectual

Propriedade intelectual

A HealthBit preza e resguarda a propriedade intelectual por ela produzida, bem como a de terceiros. Não é permitida a reprodução ou manutenção de cópias ilegais de propriedade intelectual de qualquer natureza pelos colaboradores ou prestadores de serviços nas dependências da empresa.

A HealthBit preserva os direitos autorais e de propriedade intelectual das informações e dos recursos por ela manuseados, mediante:

- Aquisição de produtos por meio de fontes conhecidas e com boa reputação
- Atualização e organização das evidências da aquisição ou cessão do direito de propriedade intelectual sobre uma informação ou produto
- Realização periódica de verificações quanto à utilização dos recursos e seus contratos de licenciamento, de forma a garantir que não esteja sendo utilizado o número de licença permitido contratualmente
- Informação constante aos colaboradores, prestadores de serviços e estagiários sobre as sanções que estes estarão sujeitos nos casos de violação dos direitos autorais e propriedade intelectual que venham a praticar

verificações de conformidade

Verificações de conformidade

As Lideranças de Equipe devem estabelecer, implementar e manter rotinas que garantam que os recursos sob sua responsabilidade se encontram em conformidade com as diretrizes de segurança da HealthBit.

Nos casos de identificação de não conformidade com a presente Política de Segurança da Informação, as Lideranças de Equipe devem providenciar as ações corretivas necessárias.

Os requisitos e atividades de auditoria que envolvam os recursos da HealthBit devem ser planejados e acordados previamente entre as áreas pertinentes a fim de minimizar a possibilidade de ocorrência de eventos que comprometam a disponibilidade dos serviços e/ou o processo de negócio.

Gestão de vunerabilidades

A HealthBit, com o objetivo de detectar e sanar eventuais falhas que podem ocasionar riscos de segurança, funcionalidade ou desempenho, organiza e executa plano de continuidade de negócios, visando também aumentar a eficiência dos sistemas e processos.

Para tanto, a HealthBit segue o seguinte fluxo, para cada processo executado no ambiente da empresa:

- Preparação e visualização de processos
- Designação de responsáveis
- Mapeamento de riscos
- Levantamentos, análises e priorização para resolução de problemas
- Tratamento técnico e organizacional de vulnerabilidades
- Treinamento de equipe
- Gestão e controle das vulnerabilidades encontradas e sanadas

responsabilidades

Da equipe de desenvolvimento e tecnologia da informação

A Equipe de Desenvolvimento e Tecnologia da Informação, juntamente com as demais Lideranças de Equipe da HealthBit, tem as seguintes atribuições:

- Elaborar, propor e buscar a aprovação, junto às demais lideranças, das diretrizes, normas e procedimentos de segurança da informação, planos de contingência e recuperação de desastres
- Coordenar as ações para implementação de políticas de segurança, padrões, ferramentas tecnológicas e demais providências necessárias para manutenção da disponibilidade, integridade e confidencialidade
- Promover a integração entre as medidas de segurança lógica e física, especialmente nas instalações de processamento e guarda de informações críticas do negócio
- Selecionar e implementar métodos para avaliação do nível de segurança
- Analisar incidentes de segurança da informação e implementar as ações corretivas correspondentes
- Promover e coordenar iniciativas para a conscientização e educação dos usuários quanto aos objetivos, métodos e benefícios da segurança da informação

Das demais lideranças de equipe da HealthBit

As Lideranças de Equipe da HealthBit devem:

- Assegurar que, dentro da sua área de competência, os colaboradores cumpram a Política, Normas e Procedimentos de segurança em vigor
- Realizar trimestralmente ações que visem identificar o grau de cumprimento da Política, Normas e Procedimentos de segurança em vigor e tomar as ações cabíveis nos casos nos quais for identificado o descumprimento por parte de seus colaboradores

Dos colaboradores e prestadores de serviço

Os Colaboradores e Prestadores de Serviço da HealthBit devem comprometer se a:

- Manter a segurança das informações da HealthBit e dos projetos de acordo com as diretrizes aqui implementadas
- Conhecer a Política de Segurança da Informação da HealthBit e demais Normas e procedimentos relativos à sua área
- Gerar e manter suas identificações pessoais com nível adequado de segurança, para mitigar os riscos às informações recebidas ou produzidas pela HealthBit
- Assinar o Termo de Confidencialidade e Sigilo, comprometendo se a não revelar informações obtidas em razão do vínculo junto à HealthBit. O termo de confidencialidade será provido pela empresa, onde devem constar as sanções aplicáveis em caso de quebra do sigilo
- Consultar o proprietário da informação, ou controlador de dados (conforme denominado na Lei nº 13 709 2018 Lei Geral de Proteção de Dados), sempre que pairar dúvidas quanto à utilização da informação e seu nível de segurança
- Notificar a Liderança responsável sempre que ocorrerem eventos suspeitos, ou que de alguma forma possam comprometer a segurança das informações sob a guarda da HealthBit

violação das normas e punibilidade

Violação das normas e punibilidade

Os incidentes que afetem a segurança das informações ou representem um descumprimento das regras descritas neste documento devem ser reportados à Equipe de Desenvolvimento e Tecnologia da Informação.

A HealthBit destaca que qualquer violação das regras de segurança aqui dispostas ensejará ação disciplinar, sem prejuízo das penalidades judicialmente cabíveis, observando se as normas aplicáveis descritas na introdução da presente Política de Segurança da Informação.

vigência e validade

Vigência e validade

A presente política passa a vigorar a partir da data de sua homologação e publicação, em dezembro de 2021 sendo válida por tempo indeterminado.

A HealthBit revisará semestralmente as disposições do presente documento, a fim de atualizar, sempre que necessário, as diretrizes de segurança da informação.

disposições finais

Disposições finais

A publicação da presente Política de Segurança da Informação presta se para firmar publicamente o compromisso da HealthBit em garantir a integridade, confidencialidade e disponibilidade das informações de nossa responsabilidade, devendo ser interpretada como diretriz básica para atuação da HealthBit.

HEALTHBIT

(19) 97812-7719

contato@healthbit.com.br