Política de Segurança da Informação ProBrain

Versão: julho/2022

SUMÁRIO

1. Introdução

1.1. A "Informação" é um dos principais ativos para a empresa e, por este motivo, a sua segurança é uma das maiores preocupações da ProBrain.

1.2. A Informação é intangível, mas pode se materializar por diversos meios, como escrito, falado, armazenado eletrônica ou fisicamente, transmitido, entre outros.

1.3. A Política de Segurança da Informação (a "Política") consiste em uma série de normas internas padronizadas pela empresa que devem ser seguidas à risca por todos os colaboradores, parceiros, prestadores de serviço e demais pessoas que tenham acesso à empresa, minimizando ao máximo o risco de possíveis ameaças à segurança da informação.

1.4. O presente documento é fundado principalmente nas normas NBR ISO/IEC 27.002/2005 e na lei nº 13.709/18 ("Lei Geral de Proteção de Dados" ou "LGPD"), além das demais leis, normas e práticas em vigência aplicáveis ao tema, das políticas e códigos da ProBrain.

2. Objetivo

2.1. Essa Política tem como objetivo estabelecer regras à Segurança da Informação, determinar as medidas de segurança, técnicas e administrativas, para proteger todas as informações envolvidas no negócio da empresa, principalmente contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, a fim de garantir o sigilo e a integridade destes dados.

3. Abrangência

3.1. Esta Política se aplica a todas as pessoas físicas ou jurídicas, incluindo colaboradores, prestadores de serviço, parceiros, clientes e demais pessoas que tem autorização e acesso às informações e recursos da empresa.

3.2. Todos os colaboradores que tiverem acesso ao sistema da ProBrain e às informações retratadas na Política são denominados de Usuários (os "Usuários").

4. Responsabilidades

4.1. Importante esclarecer que é DEVER de todos os atingidos por esta Política considerar as informações envolvidas no negócio como um ativo essencial e de grande valor para a ProBrain, devendo ser sempre tratada com as melhores práticas de confidencialidade, integridade e profissionalismo.

4.2. A segurança da informação apenas estará garantida com o comprometimento de todos. Portanto, são responsabilidades essenciais a serem observadas:

a) Cumprir fielmente a Política e todos os demais documentos aplicáveis;

b) Proteger as informações contra acessos, modificações, destruições ou divulgações não autorizadas, não provocando ou auxiliando terceiros a invadirem computadores ou a rede de dados, conforme artigo 154-A do Código Penal Brasileiro;

c) Buscar autorização prévia e escrita da Gestora de Tecnologia da Informação quando, para execução dos serviços, for necessário utilizar equipamentos pessoais de armazenamento de dados ou que possam comprometer a parte lógica do sistema operacional;

d) Assegurar que os recursos tecnológicos, as informações e os sistemas à sua disposição sejam utilizados apenas para atividades lícitas, seguras e que seja possível garantir a integridade do ambiente;

e) Cumprir as leis e as normas que regulamentam a propriedade intelectual e a confidencialidade;

f) Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (tais como meios de transporte, restaurantes, eventos etc.), incluindo a emissão de comentários e opiniões em sites e redes sociais;

g) Assegurar que pessoas não autorizadas não acessem a máquina ou o ambiente da ProBrain em caso de ausência do local de trabalho;

h) Não compartilhar informações confidenciais de qualquer tipo;

i) Propor ações de aperfeiçoamento à segurança da informação;

j) Relatar imediatamente à Gestora de Tecnologia da Informação qualquer descumprimento ou violação dessa Política e/ou das Normas e Procedimentos da empresa voltados ao tema, para que sejam tomadas todas as providências cabíveis;

k) Responder pelo uso exclusivo e intransferível de suas senhas de acesso, sendo proibido o fornecimento ou divulgação a qualquer pessoa, colaborador ou prestador de serviço por qualquer razão. Em caso de suspeita ou confirmação de comprometimento da senha, deverá ser notificado ao Time de Segurança da Informação, conforme determinado na Gestão de Incidentes, e cadastrada nova senha diferente da anterior;

l) Disponibilizar em pasta específica do drive e própria para essa finalidade, os dados de login e senha dos sistemas, com acesso restrito aos responsáveis da área da segurança da informação e os Sócios;

m) O Usuário deverá criar senhas seguras e fortes (letras maiúsculas e minúsculas, dígitos, símbolos) para acesso à máquina e ao sistema, para evitar ataques hackers de força bruta

n) Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, confidencialidade, integridade, fragilidade, mau funcionamento, presença de vírus etc.;

o) É proibido ao Usuário realizar intervenções ilegais ou indevidas em hardwares de alocação de dados;

p) O Usuário pode realizar instalação, desinstalação ou configuração de softwares na máquina utilizada, desde que garanta a segurança da operação e relate previamente à Gestora de Tecnologia da Informação sobre o procedimento;

q) É proibida a intervenção do Usuário na transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros (pirataria);

r) O desrespeito a essa Política poderá gerar um incidente de segurança da informação, o que não será tolerado pela ProBrain, podendo ser aplicada a penalidade cabível, nos termos da lei e normas aplicáveis ao evento, e de acordo com as políticas e códigos da ProBrain.

4.3. O uso de equipamentos periféricos, como fones de ouvido, mouse e teclado, independentemente de autorização prévia da Gestora de Tecnologia da Informação, podem ser utilizados pelos Usuários.

4.4. O Usuário poderá acessar páginas como Instagram, Facebook, Youtube, Spotify, páginas de jogos interativos ou outras plataformas ou softwares, desde que se responsabilize pela segurança do ambiente e pela licitude das atividades desenvolvidas.

5. Classificação da Informação e de Dado Pessoal

5.1. Todas as informações produzidas, recebidas e/ou tratadas nas atividades da empresa serão classificadas de acordo com os níveis de confidencialidade abaixo:

a) CONFIDENCIAL: Informação sigilosa que demanda o mais alto nível de segurança. Sua divulgação não autorizada gera grande impacto financeiro e reputacional à empresa. Será mantida em confidencialidade e manuseada apenas pelo grupo restrito composto pelos sócios fundadores e pelas gestoras administrativa e de tecnologia da informação.

b) RESTRITA: Informação de médio nível de confidencialidade, cujo acesso e manuseio são apenas por pessoas autorizadas (Sócios, Gestora administrativa, Gestora de Tecnologia da Informação e Gestor De Aplicações). Sua revelação não autorizada compromete a estratégia da empresa.

c) INTERNA: Informação acessada por prestadores de serviços, colaboradores e parceiros autorizados que contribuem para o negócio da empresa. Sua divulgação não autorizada pode comprometer o negócio da empresa.

d) PÚBLICA: Informação que pode ser de conhecimento público e não possui restrições de divulgação.

5.1. Os Dados Pessoais são todas as informações que identificam uma pessoa natural, como nome, CPF, número de RG, ou que podem identificá-la, mediante combinação de outras informações e dados, como o primeiro nome com a idade.

5.1.1. Existem os Dados Pessoais Sensíveis, relacionados à saúde, como por exemplo o tipo sanguíneo e os resultados de exames de sangue ou de radiografias, dados biométricos ou genética, como a digital e religião, orientação sexual e política, raça e etnia.

6. Descarte de Mídias e Dados

6.1. A informação será descartada de acordo com os prazos legais ou regulatórios, decisões judiciais ou administrativas, levando em consideração também a sua necessidade para a empresa. O descarte, será feito através de práticas que impossibilitem a sua reconstrução, seja no meio físico, seja no meio digital.

6.2. Mídias com informações do negócio da ProBrain, como SSD, Cartão de Memória, HD e Pen Drive (USB), além da Memória RAM, deverão ser destruídas antes do descarte, em caso de impossibilidade de serem reutilizadas. Por isso, o descarte será realizado após análise da Gestora De Tecnologia Da Informação.

6.3. Os dados armazenados nos Data Centers serão descartados por pessoa autorizada.

6.4. Os dados armazenados nas pastas de trabalho nos Data Center com informações confidenciais, restritas e internas serão descartados através da pasta “Lixeira”, local de acesso restrito à Gestora de Tecnologia da Informação, à Gestora Administrativa e aos Sócios. A análise e descarte final serão realizados a cada 1 (um) ano.

6.5. As mídias físicas, como papéis, livros e impressões que contenham informações da ProBrain ou Dados Pessoais, deverão ser destruídas, a fim de garantir a impossibilidade de reconstrução da informação, e somente após descartadas. Cada Usuário que esteja em posse dos documentos deverá, após autorização, realizar o descarte.

6.6. O Usuário que realizar a exclusão de informação ou dado disponível de sua máquina deverá se certificar de que, em sendo o caso, o arquivo também foi excluído do serviço de armazenamento em nuvem utilizado pela ProBrain.

7. Política de Uso de E-mail

7.1. O correio eletrônico fornecido pela ProBrain é um instrumento de comunicação interna e externa para a realização dos negócios da empresa.

7.2. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da empresa, não podem ser contrárias à legislação vigente, à moral, aos bons costumes, à ordem pública e nem aos princípios éticos estabelecidos no “Código de Conduta de Ética” da empresa.

7.3. O Usuário deverá se certificar de que utiliza o ambiente da ProBrain logado na conta do seu e-mail profissional.

8. Política de Uso da Internet

8.1. O uso indevido do acesso à Internet é de inteira responsabilidade do Usuário, que poderá ser responsabilizado legalmente pelos danos causados.

8.1.1. É lícito que o Usuário utilize plataformas interativas de jogos ou de músicas, desde que não interfira diretamente nos seus serviços e que se assegure, antes do acesso, que o ambiente é seguro e que as informações estão protegidas.

8.1.2. A ProBrain não se responsabiliza pelo pagamento de mensalidades ou planos para utilização das plataformas ou outros sites utilizados pelo Usuário.

8.2. A auditoria dos acessos à Internet leva ao conhecimento dos responsáveis hierárquicos relatórios com nomes dos Usuários, páginas consultadas, tempo de consulta e o conteúdo navegado.

8.2.1. Em qualquer dos casos, os Dados Pessoais do Usuário disponíveis na auditoria serão tratados com o devido respeito, proteção e privacidade, nos termos que a LGPD determina.

8.3. Os Usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

8.4. É proibido o acesso a sites cujas atividades sejam ilegais e indevidas, isso é, contrárias à legislação e aos bons costumes, incluindo acesso e divulgação de conteúdo pornográfico, uso de bate-papo ("salas" de conversação), que não tenham relação com os serviços ou atividades profissionais relacionados à ProBrain.

9. Política de Instalação de Aplicativos e Softwares

9.1. Os softwares homologados e instalados nos computadores são de propriedade da ProBrain, sendo proibidas as cópias integrais, ou mesmo as parciais, bem como a instalação de softwares piratas.

9.2. É proibida a instalação de softwares não autorizados ("Pirataria"). Pirataria é crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, a qual estabelece ao infrator pena de detenção e multa, além de causar prejuízos materiais, funcionais e reputacionais à empresa.

9.3. Em caso de necessidade de alteração, formatação e aprimoramento dos equipamentos de propriedade da ProBrain que tenham sido entregues aos colaboradores e aos prestadores de serviço, incluindo, mas não se limitando a notebooks, pendrives e

HD externos, deverá ser solicitada autorização prévia e escrita à Gestora De Tecnologia Da Informação.

Em nenhuma hipótese, por questões de segurança e privacidade, o Usuário estará autorizado a realizar acesso remoto a máquinas de clientes ProBrain.

10. Controle e Restrição de Uso de Mídias Removíveis/Portas USB

10.1. É possível o uso de mídias removíveis e Porta USB desde que realizado de forma responsável. O dessas mídias é controlado e poderá ser restringido ou bloqueado a qualquer momento, via acesso remoto, se identificado que houve uso indevido.

10.2. Em caso de bloqueio, será solicitado à Gestora de Tecnologia da Informação e aos Sócios a aprovação do uso da mídia e a liberação temporária do recurso para o Usuário específico.

10.3. Nenhum dispositivo removível será utilizado sem antes ter sido realizada varredura pelo Antivírus utilizado pela ProBrain.

11. Armazenamento de Arquivos

11.1. Todos os arquivos contidos no Drive da ProBrain e nos equipamentos de propriedade da Probrain (notebooks, pendrives, HD externos) devem ser exclusivamente de interesse da empresa.

11.2. É proibido o armazenamento de documentos pessoais nestes ambientes.

12. Política de Uso de Antivírus

12.1. A ProBrain utiliza software corporativo de antivírus instalado em todas as máquinas dos colaboradores e prestadores de serviços, mantendo-se ativo durante o uso do equipamento, varrendo mídias e emitindo alertas caso detectada qualquer ameaça.

12.2. A Gestora de Tecnologia da Informação é a responsável por decidir quais programas de antivírus são os adequados para cada máquina. Atualmente o programa padrão de antivírus utilizado na ProBrain é o Kaspersky.

12.3. O antivírus é atualizado na estação de trabalho do Usuário sempre que uma nova versão for disponibilizada pelo fabricante.

12.4. A varredura rápida será realizada mensalmente para as máquinas da área de aplicações e trimestralmente nas máquinas das demais áreas. A varredura completa das máquinas será realizada a cada 06 (seis) meses através do antivírus.

12.5. O procedimento de varredura das máquinas pelo antivírus será pré programado pela Auditoria.

12.6. Caso o uso de determinado website ou funcionalidade do sistema exija a desabilitação do antivírus, de forma parcial ou total, o Usuário poderá realizá-lo, independentemente de autorização prévia, desde que entenda minimamente da operação e saiba como reativar o antivírus.

12.6.1. O procedimento ocorrerá por responsabilidade do Usuário.

12.6.2. Caso o Usuário tenha dificuldade ou dúvida em relação ao procedimento, deverá buscar apoio e maiores informações da área de TI.

13. Segurança dos Sistemas

13.1. Os sistemas desenvolvidos pela ProBrain possuem controle de segurança realizado pela plataforma 1P da ElvenWorks, realizando registros e emitindo alertas em caso de falha de funcionamento, acessos indevidos aos bancos de dados dos sistemas e demais incidentes no modelo 24/7.

13.2. Todos os registros geram dados estatísticos e relatórios que podem ser extraídos a qualquer momento.

14. Política de Acessos

14.1. A cada 06 (seis) meses os Usuários cadastrados nos sistemas da ProBrain serão revisados, com a finalidade de verificar as autorizações de acesso. As permissões serão mantidas, concedidas ou revogadas, de acordo com as definições da empresa.

14.2. Além da revisão periódica, este procedimento será realizado sempre que necessário para ajuste das permissões conforme a responsabilidade e a função de cada colaborador.

14.3. Este procedimento será integramente registrado, de modo que se identifiquem as alterações realizadas, os perfis alterados, data, hora e quais permissões foram concedidas ou revogadas.

15. Arquivos de Trabalho

15.1. Os arquivos de trabalho, considerados dados essenciais ao desenvolvimento do negócio, são mantidos nos servidores da ProBrain. São exemplos de arquivos de trabalho: Planilha de faturamento, Notas fiscais, Propostas comerciais, Relatórios de Análise Técnica, dentre outros.

16. Acesso Remoto Ao Data Center

16.1. Hoje a ProBrain está localizada no Brasil e a hospedagem dos dados é realizada em data centers das empresas Amazon Web Services (AWS) e Hostinger, cujos datacenters estão localizados nos Estados Unidos e na Europa.

16.2. O acesso aos servidores é realizado de forma remota a partir das máquinas dos Sócios, colaboradores e prestadores de serviços, por meio de login e senha individual com diferentes permissões (consulta, download, alteração etc.) de acordo com a função exercida na empresa.

16.3. Todos os acessos e ações geram um registro, podendo ser emitido, a qualquer momento, um relatório com os registros através da própria plataforma da empresa. A ProBrain utiliza um software proprietário para possibilidade de monitoramento remoto durante 24 (vinte e quatro) horas por dia das atividades realizadas nas máquinas.

16.4. Os Dados Pessoais de Usuários que venham a ser obtidos através dos relatórios serão tratados na medida determinada em lei, com a privacidade e proteção exigida.

17. Política de Backup

17.1. A política de Backup dos Datas Centers utilizados pela ProBrain contempla a realização diária e de hora em hora de backup completo, sendo criptografados e armazenados no mesmo servidor.

17.2. O Usuário deverá garantir que o backup automático esteja sincronizado em sua máquina.

17.3. Os testes de recuperação de backup dos Data Centers são realizados de 7 (sete) em 7 (sete) dias.

17.4. A exclusão de Dados Pessoais, ou outro Dado do Banco de Dados, será realizada de acordo com as normas vigentes, a solicitação do titular, ordens judiciais e os termos

desta Política, sendo apagados de qualquer backup, servidor de rede, storage de ambiente paralelo e/ou das estações de trabalho dos Usuários.

17.5. A ProBrain realizará controle das versões de aplicações realizadas pelos Usuários de TI. Todas as modificações a códigos que eventualmente forem realizadas nos sistemas deverão ser salvas automaticamente.

18. Auditoria

18.1. As auditorias serão realizadas e relatórios serão gerados a cada 6 (seis) meses, ou conforme solicitações, de acordo com os procedimentos da área de tecnologia da informação. Esse procedimento é de responsabilidade da Gestora da Área de Tecnologia da Informação e tem como objetivo verificar conformidades, levantar indicadores e promover melhorias nos procedimentos internos.

18.1.1. Na auditoria pré-programada, será realizada análise da conformidade da máquina e do Usuário com as regras da Política, verificando se estão habilitadas as atualizações do sistema, se o antivírus está com a varredura rápida realizada dentro do período determinado, se os backups estão ocorrendo, bem como se há alguma vulnerabilidade detectada.

18.1.2. O tempo de duração da auditoria pré-programada não ultrapassará 30 (trinta) minutos e se garantirá, sempre que possível, que o Usuário não seja prejudicado em suas atividades pelo procedimento.

18.1.3. Se verificado que há indícios ou fortes suspeitas de que há violação à Política, por ato do Usuário, nova auditoria, mais detalhada, poderá ser realizada pela ProBrain.

18.2. A auditoria de dados, mediante autorização dos sócios, seja de forma presencial, seja de forma remota, quando realizada nos equipamentos utilizados pelo colaborador e prestador de serviço para execução dos seus serviços, não caracterizará invasão. O relatório resultante deste procedimento poderá conter nome, acessos à internet, mensagens e outros dados permitidos legalmente.

18.3. Os resultados serão encaminhados aos sócios e armazenados pelo tempo necessário.

19. Contratos

19.1. Todos os contratos firmados com os colaboradores, parceiros, prestadores de serviço e demais pessoas que tenham acesso às informações, aos sistemas e/ou ao ambiente da ProBrain conterão cláusulas que assegurem o cumprimento das regras de segurança da informação e prevejam penalidades no caso de descumprimento.

20. Descumprimento

20.1. Não será tolerado pela ProBrain o não cumprimento das determinações deste documento, sujeitando-se o infrator às medidas disciplinares cabíveis e adequadas de natureza administrativa, cível e criminal.

21. Gestão de Incidentes

21.1. É responsabilidade de todos os atingidos por esta Política informar a ocorrência de qualquer desrespeito aos termos desta Política com o fim de registrar e avaliar a ocorrência imediatamente, assegurando que, em caso de configuração de incidente de segurança da informação, sejam tomadas todas as medidas cabíveis.

21.2. A comunicação deve ser realizada ao e-mail dpo@probrain.com.br para registro, avaliação e início do processo de investigação com a coleta das evidências do ocorrido, dentro dos limites legais.

21.3. Após, serão tomadas todas as medidas cabíveis, no menor tempo possível, com o fim de solucionar a ocorrência, reduzir e reparar os possíveis danos causados, como notificar todos os interessados em caso de suspeita ou confirmação da quebra de segurança, confidencialidade ou integridade das informações, além de agir na solução da origem do incidente.

21.4. Ademais, será promovida uma análise aprofundada de todos os procedimentos envolvidos na ocorrência com o fim de implementar melhorias.

21.5. A ProBrain irá cooperar e prestar toda a assistência necessária em relação a comunicações, notificações e reclamações recebidas caso haja incidente envolvendo dados de parceiros e consequências danosas.

21.6. As ocorrências envolvendo Dados Pessoais seguirão estas medidas além daquelas especificadas na Política de Privacidade e determinadas pela Autoridade Nacional de Proteção de Dados (a "ANPD").

21.7. Medidas judiciais e administrativas serão levadas aos Sócios para aprovação prévia sempre que necessário.

21.8. Se forem identificados indícios criminais, a questão será apresentada aos Sócios para a tomada das medidas cabíveis.

22. Vigência

22.1. O disposto no presente documento entrará em vigor na data da sua comunicação à pessoa atingida.

TERMO DE CIÊNCIA E COMPROMISSO

Eu declaro que recebi, li, compreendi e tenho plena ciência das disposições da Política de Segurança da Informação da ProBrain.

Eu me comprometo a cumprir e promover o cumprimento dos termos da Política de Segurança da Informação da ProBrain, sob pena de me sujeitar às penalidades de natureza administrativa, cível e criminal.

Assinatura: _____

Nome completo:

CPF:

Cargo:

Empresa:

Local e data: