

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 1 de 15
		Revisão: A

1. Controle de Revisões

27/08/2026	Primeira Versão
------------	-----------------

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 2 de 15
		Revisão: A

Sumário

1.	Controle de Revisões	1
2.	Finalidade	3
3.	Abrangência.....	3
4.	Responsabilidades	3
5.	Referências e fundamentos.....	4
6.	Princípios de Segurança da Informação	5
7.	Princípios de Proteção de Dados Pessoais.....	5
8.	Classificação das Informações (Rótulos)	5
9.	Controle de Acesso, Senhas e Autenticação.....	6
10.	Uso dos Recursos Tecnológicos	7
11.	Armazenamento e Compartilhamento de Informações	7
12.	E-mail e Comunicação Eletrônica	7
13.	Dispositivos, Trabalho Remoto e Uso de Equipamentos Pessoais.....	8
14.	Tratamento de Dados Pessoais	8
15.	Direitos dos Titulares	9
16.	Encarregado e Governança de Proteção de Dados	9
17.	Retenção, Arquivamento e Descarte	10
18.	Fornecedores, Parceiros e Terceiros.....	11
19.	Transferência Internacional de Dados	12
20.	Backup, Continuidade e Recuperação	12
21.	Gestão de Incidentes de Segurança	12
22.	Gestão de Riscos de Segurança da Informação e Proteção de Dados	13
23.	Conscientização e Treinamento.....	14
24.	Exceções	14
25.	Monitoramento e Conformidade	14
26.	Descumprimento.....	14
27.	Vigência, Aprovação e Revisão.....	15

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 3 de 15
		Revisão: A

2. Finalidade

Esta Política define os princípios e as responsabilidades adotados pela Jabarra Radioproteção para proteger as informações e os dados pessoais utilizados em suas atividades. Seu objetivo é garantir que esses dados sejam tratados de forma adequada, segura e compatível com sua finalidade, reduzindo riscos de acesso não autorizado, perda, alteração, indisponibilidade, fraude, vazamento ou uso indevido.

A segurança da informação deve estar presente nas atividades do dia a dia e ser considerada nas decisões que envolvam pessoas, processos e tecnologia. Isso inclui a contratação de fornecedores, a implantação ou alteração de sistemas, a criação de novos processos e o relacionamento com clientes, colaboradores, parceiros e demais partes interessadas.

3. Abrangência

Esta Política se aplica a diretores, colaboradores, estagiários, prestadores de serviços, fornecedores, parceiros e terceiros que, de forma permanente ou temporária, tenham acesso a informações, dados pessoais, documentos, sistemas, redes, contas ou equipamentos da Jabarra.

As regras abrangem informações em meio físico e digital, independentemente do local de armazenamento ou acesso. A obrigação de confidencialidade permanece após o encerramento do vínculo sempre que a natureza da informação assim exigir.

4. Responsabilidades

4.1. Usuários

Cumprir esta Política, proteger credenciais, utilizar os recursos de forma adequada, respeitar as permissões recebidas, preservar a confidencialidade das informações e comunicar incidentes ou situações de risco.

4.2. Gestores

Solicitar acessos coerentes com as funções das equipes, validar a necessidade de acesso às informações sob responsabilidade da área, apoiar revisões de permissões e garantir que os dados e documentos de seus processos sejam compartilhados somente quando necessário e de acordo com sua classificação.

4.3. Tecnologia / Segurança da Informação

O Gestor da área de Tecnologia e Projetos é responsável por garantir a administração dos controles técnicos, acessos, mecanismos de proteção, backup e recuperação, além de coordenar a resposta técnica aos incidentes de segurança. O Consultor Técnico da área de Tecnologia e Projetos atua como referência operacional nos temas de infraestrutura, segurança da informação e gestão técnica de acessos, por meio do canal ti@jabarra.com.br.

4.4. QSMS / Compliance

A área de QSMS/Compliance é responsável pela governança de Privacidade e Proteção de Dados e pela coordenação do acompanhamento desta Política. Compete à área orientar os setores quanto às

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 4 de 15
		Revisão: A

diretrizes de proteção de dados, acompanhar demandas de titulares e da ANPD, coordenar avaliações de conformidade e riscos, participar da análise de incidentes envolvendo dados pessoais e articular, quando necessário, a participação da Tecnologia, das áreas responsáveis pelos processos e da assessoria jurídica externa.

4.5. Recursos Humanos

O Recursos Humanos é responsável por comunicar à área de Tecnologia admissões, mudanças de função, afastamentos e desligamentos que afetem acessos; responde pelos dados trabalhistas e cadastrais de colaboradores com apoio da Tecnologia; e participa, em conjunto com QSMS/Compliance, dos processos de mobilização que envolvam dados pessoais.

4.6. Assessoria Jurídica Externa

A assessoria jurídica externa apoia a avaliação de obrigações legais e regulatórias, cláusulas contratuais relacionadas à confidencialidade e proteção de dados, situações de maior risco jurídico, demandas de titulares e eventuais comunicações à ANPD, quando acionada por QSMS/Compliance ou pelas áreas responsáveis.

4.7. Diretoria

Aprovar esta Política, deliberar sobre exceções e riscos relevantes, apoiar sua aplicação e assegurar que temas de Segurança da Informação e Proteção de Dados sejam considerados nas decisões da organização.

5. Referências e fundamentos

5.1. Referências

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Regulamentações e orientações aplicáveis da Autoridade Nacional de Proteção de Dados (ANPD), inclusive as relacionadas à comunicação de incidentes, atuação do encarregado e transferência internacional de dados;
- Normas ISO/IEC 27001 e ISO/IEC 27002, utilizadas como referência de boas práticas de segurança da informação;
- Obrigações legais, regulatórias, contratuais e normas internas aplicáveis à atividade da Jabarra.

Esta Política foi elaborada com base nas referências acima e nas boas práticas de mercado aplicáveis à segurança da informação e à proteção de dados pessoais.

5.2. Conceitos essenciais

Para fins desta Política, aplicam-se as seguintes definições:

- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;
- **Dado pessoal sensível:** dado pessoal que recebe proteção especial pela LGPD;
- **Titular:** pessoa natural a quem os dados pessoais se referem;
- **Controlador:** quem toma as decisões sobre o tratamento de dados pessoais;

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 5 de 15
		Revisão: A

- **Operador:** quem trata dados pessoais em nome do controlador;
- **Incidente de segurança:** evento que comprometa, ou possa comprometer, a confidencialidade, a integridade ou a disponibilidade de informações ou de dados pessoais.

6. Princípios de Segurança da Informação

A Segurança da Informação na Jabarra é fundamentada nos seguintes princípios:

- **Confidencialidade:** acesso às informações somente por pessoas autorizadas e para finalidade profissional legítima.
- **Integridade:** proteção contra alteração, exclusão ou modificação indevida.
- **Disponibilidade:** acesso às informações e recursos necessários dentro dos níveis de serviço definidos para a operação.
- **Rastreabilidade:** possibilidade de identificar, quando tecnicamente aplicável, acessos e ações relevantes realizados nos ambientes corporativos.
- **Menor privilégio:** concessão apenas dos acessos necessários à atividade desempenhada.
- **Responsabilidade:** atribuição clara de obrigações a cada usuário quanto ao uso adequado dos recursos, credenciais e informações a que tenha acesso.

7. Princípios de Proteção de Dados Pessoais

O tratamento de dados pessoais deve observar os princípios previstos na LGPD, especialmente finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Na prática, isso significa tratar apenas os dados necessários, para finalidade definida, com acesso compatível com a atividade e controles proporcionais ao risco envolvido.

8. Classificação das Informações (Rótulos)

A classificação orienta o nível de proteção esperado para cada informação. Na dúvida, deve-se adotar o nível mais restritivo até que o responsável pela informação defina o tratamento adequado.

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 6 de 15
		Revisão: A

Classificação	Definição	Exemplos	Tratamento esperado
Pública	Informação cuja divulgação externa foi autorizada.	Site, materiais institucionais e conteúdos publicados oficialmente.	Pode ser divulgada pelos canais aprovados.
Uso Interno	Informação utilizada na rotina da empresa e destinada ao ambiente corporativo.	Procedimentos, comunicações internas, documentos de trabalho e registros operacionais.	Compartilhamento limitado ao contexto profissional e às pessoas envolvidas.
Confidencial	Informação cuja exposição possa gerar risco à Jabarra, clientes, titulares ou terceiros.	Dados pessoais, contratos, propostas, informações financeiras, técnicas, estratégicas, credenciais e documentos de clientes.	Acesso limitado, compartilhamento controlado e armazenamento em ambientes autorizados.

A classificação pode ser complementada por critérios específicos definidos em contratos, projetos ou procedimentos internos.

9. Controle de Acesso, Senhas e Autenticação

Cada usuário deve utilizar conta individual e identificável, sendo vedado o compartilhamento de senhas, códigos de autenticação ou contas pessoais de acesso.

Os acessos devem corresponder às atividades efetivamente desempenhadas pelo usuário e podem ser solicitados por ele próprio ou pelo gestor responsável, mediante aprovação do gestor da área. A liberação técnica e a administração das permissões são conduzidas pela área de Tecnologia, por meio do canal ti@jabarra.com.br.

Nos serviços corporativos que disponibilizarem o recurso, a autenticação multifator (MFA) deve ser utilizada, salvo exceção formalmente aprovada.

Para manter esses controles atualizados, o Recursos Humanos deve comunicar à área de Tecnologia toda admissão, mudança de função, afastamento ou desligamento, permitindo o ajuste tempestivo dos acessos correspondentes.

Acessos administrativos, privilegiados ou de terceiros, por representarem maior risco, devem receber controle mais restritivo e revisão compatível com esse risco. De forma geral, as permissões de usuários e terceiros devem ser revistas periodicamente pela área de Tecnologia, com participação dos gestores das áreas envolvidas quando necessário.

Qualquer suspeita de comprometimento de conta deve ser comunicada imediatamente pelo canal ti@jabarra.com.br, sendo que a simples troca de senha não encerra o tratamento do incidente quando houver possibilidade de acesso indevido.

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 7 de 15
		Revisão: A

10. Uso dos Recursos Tecnológicos

Sistemas, contas, redes, equipamentos e serviços disponibilizados pela Jabarra destinam-se prioritariamente às atividades profissionais e devem ser utilizados de forma compatível com as regras internas e com a legislação aplicável.

A instalação de programas, extensões ou aplicativos com acesso a informações corporativas depende de autorização da área responsável por Tecnologia.

É vedada a tentativa de contornar controles de segurança, obter acesso não autorizado ou desabilitar mecanismos de proteção sem autorização.

Informações classificadas como Confidenciais, dados pessoais ou documentos de clientes não devem ser inseridos em ferramentas de inteligência artificial, armazenamento, comunicação ou produtividade não homologadas pela Jabarra.

Recursos corporativos não devem ser utilizados para práticas ilegais ou que exponham a empresa a risco de segurança, reputacional ou contratual.

11. Armazenamento e Compartilhamento de Informações

Sistemas, contas, redes, equipamentos e serviços disponibilizados pela Jabarra destinam-se prioritariamente às atividades profissionais e devem ser utilizados de forma compatível com as regras internas e com a legislação aplicável.

A instalação de programas, extensões ou aplicativos com acesso a informações corporativas depende de autorização da área responsável por Tecnologia.

É vedada a tentativa de contornar controles de segurança, obter acesso não autorizado ou desabilitar mecanismos de proteção sem autorização.

Informações classificadas como Confidenciais, dados pessoais ou documentos de clientes não devem ser inseridos em ferramentas de inteligência artificial, armazenamento, comunicação ou produtividade não homologadas pela Jabarra.

Recursos corporativos não devem ser utilizados para práticas ilegais ou que exponham a empresa a risco de segurança, reputacional ou contratual.

12. E-mail e Comunicação Eletrônica

O e-mail corporativo e os demais canais de comunicação devem ser utilizados com atenção à origem das mensagens, aos destinatários e ao conteúdo solicitado.

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 8 de 15
		Revisão: A

Solicitações atípicas envolvendo pagamentos, alteração de dados bancários, liberação de acessos, envio de documentos Confidenciais ou fornecimento de credenciais devem ser confirmadas por um segundo canal antes da execução.

Mensagens suspeitas, links inesperados, anexos de origem desconhecida e solicitações de senha ou código de autenticação não devem ser atendidos e devem ser encaminhados para avaliação da área responsável.

13. Dispositivos, Trabalho Remoto e Uso de Equipamentos Pessoais

Equipamentos utilizados para acessar recursos corporativos devem possuir proteção por senha ou mecanismo equivalente, bloqueio automático e atualizações de segurança compatíveis com sua utilização.

A tela deve ser bloqueada sempre que o usuário se afastar do equipamento.

Perda, furto ou comprometimento de equipamento com acesso a dados corporativos deve ser comunicado imediatamente.

O acesso a informações Confidenciais em redes públicas deve ser evitado quando não houver mecanismo seguro de conexão.

O uso de equipamento pessoal para atividade corporativa somente é permitido quando autorizado e deve observar as mesmas regras de proteção aplicáveis aos equipamentos da empresa.

Documentos físicos e telas contendo informação confidencial devem ser protegidos de visualização por pessoas não autorizadas, inclusive fora das instalações da empresa.

14. Tratamento de Dados Pessoais

Todo tratamento de dados pessoais realizado no âmbito das atividades da Jabarra Radioproteção deve estar vinculado a uma finalidade profissional definida e a uma hipótese legal aplicável. A avaliação deve considerar o tipo de dado tratado, os titulares envolvidos, a forma de utilização, eventual compartilhamento com clientes, fornecedores ou parceiros e o papel exercido pela Jabarra em cada operação de tratamento.

Nas atividades administrativas, comerciais, operacionais, de recursos humanos, treinamento, mobilização e prestação de serviços, devem ser tratados apenas os dados necessários à execução da atividade ou ao cumprimento das obrigações legais, contratuais e regulatórias aplicáveis.

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 9 de 15
		Revisão: A

Dados pessoais sensíveis, documentos pessoais e outras informações que possam representar maior risco aos titulares devem ter acesso restrito às pessoas que efetivamente necessitem dessas informações para o exercício de suas funções.

O acesso a um sistema, pasta ou documento não autoriza o usuário a utilizar os dados para finalidade diferente daquela relacionada à atividade que justificou sua permissão.

A implantação ou alteração de sistemas, criação de integrações, contratação de fornecedores que tratem dados pessoais, adoção de novas tecnologias ou criação de processos que impliquem novo uso ou compartilhamento de dados devem considerar os impactos à privacidade e à segurança antes de sua implementação.

Tratamentos que apresentem maior risco aos direitos e às liberdades dos titulares deverão ser submetidos a avaliação específica. Quando necessário ou recomendado em razão do risco identificado, poderá ser elaborado Relatório de Impacto à Proteção de Dados Pessoais — RIPD.

A Jabarra deverá manter registro das operações relevantes de tratamento de dados pessoais, contendo, conforme aplicável, a finalidade do tratamento, categorias de titulares e dados utilizados, sistemas envolvidos, compartilhamentos realizados, fornecedores participantes, hipótese legal adotada e medidas de proteção aplicáveis.

15. Direitos dos Titulares

A Jabarra deve permitir o exercício dos direitos previstos na LGPD, conforme aplicável ao tratamento realizado, incluindo confirmação da existência de tratamento, acesso, correção e demais solicitações previstas em lei.

As solicitações devem ser registradas, verificadas quanto à identidade do solicitante quando necessário e respondidas dentro dos prazos legais e regulatórios aplicáveis. Antes de fornecer dados, a empresa deve adotar medidas razoáveis para evitar entrega a pessoa não autorizada.

Canal institucional para assuntos relacionados à privacidade e à proteção de dados: ti@jabarra.com.br.

16. Encarregado e Governança de Proteção de Dados

A Jabarra centralizará as comunicações relacionadas à privacidade e à proteção de dados por meio do canal ti@jabarra.com.br, monitorado por mais de um integrante da área de Tecnologia. O endereço será utilizado para solicitações de titulares, comunicações relacionadas à LGPD, dúvidas sobre

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 10 de 15
		Revisão: A

tratamento de dados pessoais e reporte de situações que possam envolver uso, compartilhamento ou exposição indevida de informações.

A área de Tecnologia será responsável pelo recebimento, registro e direcionamento inicial das demandas encaminhadas pelo canal ti@jabarra.com.br. Adolfo Lira atuará como referência operacional para os temas de infraestrutura, acessos e segurança da informação. As demandas relacionadas à privacidade e à proteção de dados deverão ser encaminhadas à área de QSMS/Compliance, que coordenará sua análise e envolverá, conforme o caso, Recursos Humanos, Comercial, Operacional, Tecnologia e Projetos, Financeiro ou outras áreas responsáveis pelo processo.

Na estrutura atual da Jabarra, a governança de privacidade e proteção de dados é responsabilidade da área de QSMS/Compliance. Compete à área coordenar a aplicação das diretrizes desta Política, acompanhar solicitações de titulares e demandas da Autoridade Nacional de Proteção de Dados - ANPD, apoiar as áreas no tratamento adequado de dados pessoais e participar da avaliação de situações que possam representar risco à privacidade ou à conformidade da empresa.

A área de QSMS/Compliance deverá ser envolvida em situações que impliquem novo uso ou compartilhamento de dados pessoais, alterações relevantes de processos, contratação de fornecedores com acesso a dados pessoais ou outras mudanças que possam afetar a privacidade. A área de Tecnologia participará das avaliações quando houver sistemas, integrações, infraestrutura, acessos ou controles técnicos envolvidos, e a assessoria jurídica externa será acionada quando houver necessidade de avaliação legal ou regulatória.

As demandas recebidas deverão ser tratadas de forma rastreável, mantendo-se, quando aplicável, registro da solicitação, área envolvida, providências adotadas e conclusão.

Caso a legislação ou a estrutura de governança da Jabarra exija a designação formal de Encarregado pelo Tratamento de Dados Pessoais, a designação será conduzida no âmbito da governança de QSMS/Compliance, e sua identidade e suas informações de contato serão divulgadas de forma clara nos canais institucionais aplicáveis. O endereço ti@jabarra.com.br permanecerá como canal corporativo para recebimento e encaminhamento das comunicações relacionadas à proteção de dados.

17. Retenção, Arquivamento e Descarte

As informações e os dados pessoais tratados pela Jabarra deverão ser mantidos somente pelo período necessário ao atendimento da finalidade para a qual foram utilizados, ao cumprimento de obrigações legais, regulatórias ou contratuais e ao exercício regular de direitos da empresa ou de terceiros.

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 11 de 15
		Revisão: A

Os prazos de retenção deverão considerar a natureza de cada informação e o processo ao qual ela pertence. Documentos trabalhistas e cadastrais de colaboradores, registros de treinamentos, documentos de mobilização, contratos, propostas comerciais, documentos financeiros e fiscais, registros operacionais e informações relacionadas à prestação de serviços poderão, portanto, possuir períodos de guarda distintos.

As áreas responsáveis pelos processos deverão observar os prazos legais e contratuais aplicáveis e definir o período adequado de retenção das informações sob sua responsabilidade. Quando necessário, essa definição deverá contar com o apoio de QSMS/Compliance, Tecnologia e da assessoria jurídica externa.

Encerrado o período de guarda e inexistindo obrigação legal, regulatória, contratual ou necessidade legítima que justifique sua manutenção, os dados deverão ser eliminados ou, quando aplicável, anonimizados de forma segura.

O descarte deverá considerar o meio em que a informação está armazenada. Documentos físicos que contenham informações Confidenciais ou dados pessoais deverão ser destruídos de forma que impeça sua reconstrução. Arquivos digitais, mídias e equipamentos deverão ser descartados, reutilizados ou substituídos somente após a adoção de medidas que impeçam a recuperação indevida das informações neles armazenadas.

Os períodos de guarda deverão ser definidos de acordo com a natureza das informações, as obrigações legais, regulatórias e contratuais aplicáveis e as necessidades legítimas da Jabarra. Sempre que houver dúvida quanto à retenção ou ao descarte, a área responsável pelo processo deverá consultar QSMS/Compliance, Tecnologia e, quando necessário, a assessoria jurídica externa.

18. Fornecedores, Parceiros e Terceiros

O acesso de fornecedores, parceiros, consultorias, prestadores de serviços e demais terceiros às informações, sistemas e ambientes da Jabarra deve ser limitado ao necessário para a execução da atividade contratada e somente pelo período em que esse acesso for efetivamente necessário. Nas contratações que envolvam dados pessoais ou informações classificadas como Confidenciais, deverão ser previstas obrigações compatíveis de confidencialidade, proteção de dados e segurança da informação.

A área contratante, com apoio da área de Tecnologia, deverá avaliar de forma proporcional ao risco a capacidade do terceiro de proteger as informações às quais terá acesso.

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 12 de 15
		Revisão: A

Os dados e informações disponibilizados pela Jabarra deverão ser utilizados exclusivamente para a execução das atividades contratadas, sendo vedado o uso para finalidade própria, o compartilhamento não autorizado ou a utilização para finalidade diferente da originalmente estabelecida.

Subcontratações que envolvam tratamento de dados pessoais ou acesso a informações Confidenciais deverão observar as obrigações assumidas no contrato principal e os requisitos definidos pela Jabarra. Quando houver impacto contratual ou regulatório, a área contratante e a Tecnologia deverão contar com apoio da assessoria jurídica externa.

Encerrado o serviço, contrato ou qualquer outra necessidade que tenha justificado o acesso, as permissões deverão ser retiradas pela área de Tecnologia. As informações mantidas pelo terceiro deverão ser devolvidas, eliminadas ou conservadas somente quando houver obrigação legal, regulatória ou contratual que justifique sua retenção.

19. Transferência Internacional de Dados

Quando dados pessoais forem armazenados, acessados ou transferidos para outro país, a Jabarra deverá observar os requisitos da LGPD e da regulamentação vigente da Autoridade Nacional de Proteção de Dados sobre transferência internacional, incluindo a avaliação do mecanismo jurídico aplicável ao caso.

A utilização de serviços em nuvem ou fornecedores globais não afasta a responsabilidade de avaliar onde os dados são tratados e quais salvaguardas contratuais e técnicas são aplicáveis.

20. Backup, Continuidade e Recuperação

Informações necessárias à continuidade das operações devem estar contempladas nos mecanismos corporativos de backup e recuperação definidos para cada ambiente. Cópias mantidas apenas no computador do usuário não são consideradas backup corporativo.

A área de Tecnologia deverá manter controles de backup e recuperação proporcionais à criticidade dos ambientes e verificar periodicamente a capacidade de restauração das informações relevantes. A execução e o acompanhamento técnico desses controles ficarão sob responsabilidade da área de Tecnologia, com atuação operacional de Adolfo Lira nos temas de infraestrutura e segurança.

21. Gestão de Incidentes de Segurança

Devem ser comunicados sem demora eventos como acesso não autorizado, envio de informação ao destinatário errado, perda de equipamento, malware, phishing, fraude, vazamento, exclusão indevida de arquivos, comprometimento de conta ou qualquer situação que possa afetar a segurança das informações.

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 13 de 15
		Revisão: A

O usuário deve comunicar a ocorrência imediatamente pelo canal ti@jabarra.com.br e fornecer as informações disponíveis para avaliação pela área de Tecnologia.

Mensagens, arquivos, registros e demais evidências relacionadas ao evento não devem ser apagados ou alterados sem orientação da equipe responsável.

A área de Tecnologia será responsável por avaliar e classificar o incidente, coordenar as medidas iniciais de contenção e recuperação e definir o escalonamento necessário. Incidentes envolvendo dados pessoais deverão ser avaliados também quanto ao impacto e aos riscos para os titulares.

Quando houver possibilidade de comunicação à ANPD ou aos titulares afetados, a avaliação deverá envolver QSMS/Compliance, a área de Tecnologia e a assessoria jurídica externa. A Diretoria deverá ser informada nos casos de maior criticidade e participar da decisão quando aplicável.

Os incidentes, as avaliações realizadas, as decisões adotadas e as medidas implementadas deverão ser registrados pelo período legal ou regulatório aplicável, permitindo rastreabilidade e aprendizado.

O canal oficial de comunicação interna para incidentes de segurança é ti@jabarra.com.br.

A área de Tecnologia coordenará a resposta, o escalonamento, a preservação de evidências, as comunicações internas e o acompanhamento do incidente até seu encerramento, envolvendo as demais áreas conforme a natureza e a criticidade da ocorrência.

22. Gestão de Riscos de Segurança da Informação e Proteção de Dados

A gestão dos riscos relacionados à Segurança da Informação e à Proteção de Dados será coordenada pela área de QSMS/Compliance, com participação da área de Tecnologia e das áreas responsáveis pelos processos avaliados. A análise deverá considerar mudanças em processos, sistemas, pessoas, fornecedores, integrações e tecnologias.

Os riscos identificados deverão ser avaliados considerando sua probabilidade de ocorrência, impacto potencial sobre a operação, clientes, titulares de dados e obrigações legais ou contratuais, bem como os controles existentes. Sempre que houver necessidade de tratamento, deverão ser definidas as medidas necessárias, o responsável por sua execução e, quando aplicável, prazo para implementação.

A avaliação dos riscos deverá ser revista anualmente e quando ocorrer incidente relevante, implantação ou alteração significativa de sistema, mudança de processo, contratação de fornecedor crítico, nova integração tecnológica ou outra situação capaz de alterar materialmente o nível de exposição da

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 14 de 15
		Revisão: A

Jabarra. Riscos relevantes ou que não possam ser adequadamente tratados pelas áreas responsáveis deverão ser submetidos à Diretoria.

23. Conscientização e Treinamento

Colaboradores e terceiros que tenham acesso a informações corporativas devem receber orientação compatível com suas responsabilidades. A área de Tecnologia, em conjunto com QSMS/Compliance, definirá os conteúdos e temas prioritários de conscientização em segurança da informação, privacidade e proteção de dados. O Recursos Humanos apoiará a convocação, o acompanhamento da participação e a manutenção dos registros das ações realizadas.

Áreas com acesso a informações de maior sensibilidade ou com responsabilidades específicas poderão receber capacitação adicional, incluindo temas como phishing, credenciais, compartilhamento de informações, uso de ferramentas tecnológicas, proteção de dados e resposta a incidentes.

24. Exceções

Exceções a esta Política devem ser justificadas, registradas e avaliadas previamente pelo gestor responsável e pelas áreas de Tecnologia e/ou QSMS/Compliance, conforme o tema. A aprovação final da exceção caberá à Diretoria. Sempre que possível, deverão ser definidos escopo, prazo e controles compensatórios.

25. Monitoramento e Conformidade

QSMS/Compliance, com apoio da área de Tecnologia e das áreas envolvidas, poderá coordenar revisões de acessos, verificações de configuração, avaliações de conformidade e outras atividades de monitoramento necessárias à proteção dos ambientes e informações da Jabarra, observados a finalidade, a proporcionalidade e os limites legais aplicáveis.

Não conformidades identificadas deverão ser comunicadas às áreas responsáveis e tratadas de acordo com sua criticidade. Situações de maior risco deverão ser acompanhadas por QSMS/Compliance e Tecnologia e, quando necessário, submetidas à Diretoria.

26. Descumprimento

O descumprimento desta Política será analisado conforme a natureza, a gravidade e o impacto da ocorrência e poderá resultar nas medidas administrativas, disciplinares, contratuais ou legais cabíveis, sem prejuízo das demais providências necessárias à proteção da empresa, dos titulares e de terceiros.

	Jabarra Radioproteção	
	POL-JAB-BRA-013 Política de Segurança da Informação e Proteção de Dados	Pág: 15 de 15
		Revisão: A

27. Vigência, Aprovação e Revisão

Esta Política entra em vigor após sua aprovação pela Diretoria da Jabarra Radioproteção e deve permanecer disponível aos públicos abrangidos por suas regras.

A área de QSMS/Compliance será responsável por coordenar a revisão desta Política, com participação da área de Tecnologia e das demais áreas envolvidas quando necessário. A revisão ordinária ocorrerá anualmente e deverá ser submetida à aprovação da Diretoria. Revisões extraordinárias poderão ocorrer antes desse prazo em razão de alteração legal ou regulatória relevante, incidente significativo, mudança tecnológica, alteração de processo ou identificação de risco que justifique a atualização das diretrizes.