Política de Privacidade dos Dados Pessoais e de Segurança da Informação

Introdução

As informações e os recursos de informação são ativos valiosos da Intergard do Brasil necessários para a realização de tarefas, tomada de decisão e desenvolvimento contínuo dos negócios e, por isso, devem ser adequadamente protegidos, controlados, adquiridos, utilizados, atualizados, administrados e descartados, de forma segura, independentemente do meio ou forma em que estejam armazenados.

Assim, criamos e revisamos nossa Política de Privacidade dos Dados Pessoais e de Segurança da Informação ("Política") à luz da Lei Geral de Proteção de Dados Pessoais (LGPD), lei n.º 13709/2018 e posteriores alterações e regulamentações.

A Segurança da Informação tem por objetivo proteger a Intergard do Brasil e, consequentemente, seus ativos das ameaças externas, a fim de assegurar a continuidade do seu negócio e preservar os direitos fundamentais de seus titulares. De tal modo, que a existência de uma Política de Segurança e Sigilo dos Dados apresenta à sociedade e, principalmente, aos nossos colaboradores que lidam com os processos em todas as áreas, a nossa adesão e conformidade com os princípios, fundamentos e as diretivas de Proteção dos Dados sob nossa custódia.

Desta forma, o primeiro passo para a implementação da privacidade dos dados pessoais e da segurança da informação é a adoção da Política de Segurança da Informação–criada pela Intergard do Brasil, cujo cumprimento depende, principalmente, das ações dos colaboradores e das demais pessoas envolvidas nas relações empresariais existentes entre a Intergard do Brasil e seus, clientes, parceiros, terceiros, em observância aos preceitos contidos na LGPD.

Para proteger seus ativos tangíveis e intangíveis, a Intergard do Brasil elaborou esta Política, pautada na legislação nacional vigente, nas melhores práticas do mercado e nos princípios da ética e da transparência, e que deve ser cumprida diariamente por todos.

A Diretoria da Intergard do Brasil está comprometida com a proteção dos ativos tangíveis e intangíveis e aprova, os princípios de Segurança da Informação contidos nesta Política para garantir a confidencialidade, integridade, disponibilidade e autenticidade desses ativos, e o seu uso em conformidade com a legislação pertinente, as necessidades de negócio e contratos estabelecidos.

A segurança das informações e dos recursos de informação da Intergard do Brasil é uma responsabilidade de todos os colaboradores e de todas as pessoas que se relacionam, direta ou indiretamente, com a Intergard do Brasil.

Objetivo

Esta Política tem por objetivo:

a) Definir os princípios de segurança das informações da Intergard do Brasil com o objetivo de proteger os seus ativos tangíveis e intangíveis;

b) Servir de fundamento para as diretrizes e processos relacionados à garantia da segurança das informações;

c) Estabelecer as responsabilidades e limites de atuação dos colaboradores da Intergard do Brasil e de terceiros em relação à segurança da informação, reforçando a cultura interna e priorizando as ações necessárias em conformidade com os objetivos do negócio e requisitos aplicáveis;

d) Orientar em relação à adoção de controles e processos para atendimento dos requisitos de segurança da informação e as legislações em relação à proteção dos dados pessoais;

e) Resguardar as informações da Intergard do Brasil, garantindo requisitos de confidencialidade, integridade e disponibilidade; e

f) Prevenir incidentes com segurança e tratamento de dados como o uso inadequado de bases de dados, tratamento de dados, vazamento de dados e responsabilização legal da Intergard do Brasil, nossos parceiros, usuários e colaboradores.

Abrangência

Esta Política é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir da sua publicação, aos colaboradores da Intergard do Brasil nos âmbitos administrativo (recursos de TIC), industrial (recursos de TA) e de internet das coisas (recursos de IoT).

Termos e Definições

Para os fins descritos na Política da Intergard do Brasil e segundo à legislação vigente considerar-se-ão os seguintes termos e definições:

a) Ameaça: Causa potencial de um incidente indesejado que pode resultar em dano à Intergard do Brasil, a seus colaboradores, parceiros, clientes e todas as pessoas que se relacionam, direta ou indiretamente, com a empresa.

b) Ativo: Qualquer coisa que tenha valor para a Intergard do Brasil e para as pessoas que com ela se relacionam e precisa ser adequadamente protegido.

c) Ativo Intangível: Todo elemento que possui valor para a Intergard do Brasil e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à reputação, imagem, marca e conhecimento.

d) Autenticidade: Garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.

e) Colaborador: Empregado, estagiário, menor aprendiz, terceiro, ou qualquer outro indivíduo que venha a ter relacionamento profissional, direta ou indiretamente, com a Intergard do Brasil.

f) Confidencialidade: Garantia de que as informações sejam acessadas e divulgadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio.

g) Conformidade: Garantia de que todas as informações sejam criadas e gerenciadas de acordo com os requisitos legais, regulatórios, organizacionais e contratuais.

h) Dado pessoal: Informação relacionada a pessoa natural (física) identificada ou identificável independente do meio em que estiver armazenada.

i) Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

j) Disponibilidade: Garantia de que as informações e os recursos de informação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

k) Informação: Conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

l) Integridade: Garantia de que as informações estejam completas e fidedignas em relação à última alteração desejada durante o seu ciclo de vida, além de protegida contra alteração ou destruição não autorizada.

m) Legalidade: Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.

n) Nível de Confidencialidade: identifica o nível de proteção necessário para as informações, de acordo com a sua natureza e o impacto estimado para a Intergard do Brasil, no caso de divulgação indevida:

• Informações públicas: são as informações que, por não apresentarem riscos, podem ser distribuídas livremente dentro e fora dos limites físicos e dos Recursos de TIC da Intergard do Brasil;

• Informações internas: são informações cuja divulgação a terceiros não autorizados poderia promover desvantagem comercial, questionamento de condições contratuais, ou a boa execução das atividades;

• Informações restritas: são informações cuja divulgação a pessoas não autorizadas poderia promover o comprometimento do sigilo de decisões gerenciais, cobertura em mídia local, o nível de segurança físico e lógico do ambiente corporativo, ou a divulgação indevida de dados pessoais;

• Informações confidenciais: são as informações cuja divulgação a pessoas não autorizadas poderia promover o comprometimento dos objetivos estratégicos da Intergard do Brasil, a perda de negócios, cobertura negativa em mídia nacional, afetar de forma negativa no faturamento da Intergard do Brasil, ou a divulgação indevida de dados pessoais sensíveis.

o) Risco: Efeito da incerteza sobre os objetivos, verificado pela combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos (consequências).

p) Recursos de Tecnologia da Informação e Comunicação (recursos de TIC): Hardwares, softwares, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.

q) Recursos de Tecnologias de Automação (recursos de TA): Conjunto de recursos de TIC aplicados especificamente nas atividades de operação, supervisão, automação controle, incluindo os sistemas de controle industrial.

r) Recursos de Internet das Coisas (recursos de IoT): Conjunto de recursos de TIC que formam uma rede de objetos que possuem tecnologia embarcada para identificar, comunicar e interagir com seu estado interno ou com o ambiente externo.

s) Recurso de Informação: É o conjunto de todos os recursos de TIC, TA e IoT.

t) Segurança da Informação: É a preservação da confidencialidade, integridade, disponibilidade, conformidade e autenticidade da informação. Visa proteger a informação e os recursos de informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação.

u) Tentativa de Burla: Fazer esforços para não respeitar ou tentar violar as diretrizes e os controles estabelecidos nos normativos da Intergard do Brasil.

v) Violação: Qualquer atividade que desrespeite as regras estabelecidas nos normativos da Intergard do Brasil.

w) Banco de dados: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

x) Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

y) Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

z) Encarregado: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

ç) Tratamento: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Princípios Gerais da Segurança da Informação

A Intergard do Brasil tem os seguintes princípios gerais de segurança da informação:

a) Preservar e proteger as informações e os recursos de informação da Intergard do Brasil, de seus colaboradores ou que estejam sob sua responsabilidade, dos diversos tipos de ameaça e em todo o seu ciclo de vida, contidas em qualquer suporte ou formato;

b) Prevenir, monitorar, identificar e responder aos incidentes de segurança da informação, reduzindo os seus impactos e assegurando a confidencialidade, integridade, disponibilidade, autenticidade das informações e a conformidade no uso dos recursos de informação no desenvolvimento das atividades profissionais;

c) Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados ao negócio no que diz respeito à segurança da informação e aos objetivos corporativos, morais e éticos da Intergard do Brasil.

Deste modo, as medidas de prevenção e controle adotadas pela Intergard do Brasil visam, em essência, gerenciar e manter os riscos em um nível adequado ao negócio.

Propriedade

As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os recursos de informação e demais ativos tangíveis e intangíveis disponibilizados, são de propriedade da Intergard do Brasil ou, quando de terceiros, estão sob sua guarda e sujeitos às determinações desta Política e das prescrições legais pertinentes.

Estratégia de Ação

A estratégia utilizada para o cumprimento dos princípios de segurança definidos nesta Política é a adoção de um Programa de Segurança da Informação que define os papéis, responsabilidades e as atividades de gestão e de melhoria contínua do nível de Segurança das Informações da Intergard do Brasil e a adoção de ações táticas de segurança que incluem a definição de diretrizes, padrões e a implementação de processos e controles para a adequada:

a) Gestão dos riscos relacionados à falta de segurança das informações e do uso dos Recursos de informação;

b) Proteção dos ativos tangíveis e intangíveis relacionados às informações e recursos de informação da Intergard do Brasil e de terceiros, de acordo com a sua importância para o negócio e nível de confidencialidade;

c) Garantia da legalidade e conformidade do uso das informações e recursos de informação;

d) Proteção da privacidade dos dados pessoais das pessoas que se relacionam com a Intergard do Brasil, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo seu tratamento autorizado nos termos da legislação de proteção de Dados Pessoais vigente;

e) Conscientização e treinamento dos colaboradores e terceiros para o adequado uso das informações e recursos de informação;

f) Identificação de ameaças, correção de vulnerabilidades e de problemas, e prevenção e resposta a incidentes de segurança da informação;

g) Gestão de projetos e de mudanças nos recursos de informação e nos processos que os utilizam;

h) Gestão das operações dos recursos de informação;

i) Gestão da continuidade das atividades de negócio;

j) Verificação e monitoramento do uso das informações e dos recursos informação;

k) Atuação em caso de violação dos princípios, dos controles estabelecidos e dos normativos da Intergard do Brasil;

Papeis e Responsabilidades

A Diretoria da Intergard do Brasil (Controlador) tem a responsabilidade de analisar, revisar e propor a aprovação de políticas e normas relacionadas à proteção dos dados pessoais, garantir a disponibilidade de recursos necessários para uma gestão efetiva do programa de proteção dos dados pessoais, garantir que a segurança dos dados estejam em conformidade com esta política e promover a divulgação da Política de Segurança da Informação e disseminar a cultura de proteção dos dados, uso legal e conceito de privacidade de dados.

Para o cumprimento desta Política, a Intergard do Brasil define a Diretoria que além das responsabilidades anteriormente mencionadas conjuntamente com a área de Tecnologia da Informação (TI) e Recursos Humanos (RH), são responsáveis por:

a) Manter esta Política atualizada e submetê-la para aprovação da Diretoria da Intergard do Brasil;

b) Definir e manter o Programa de Segurança da Informação da Intergard do Brasil;

c) Analisar e aprovar, ou não, os pedidos de exceções a esta Política, bem como, documentos normativos, modelos, padrões, processos, controles e recursos necessários para a Diretoria da Intergard do Brasil que é responsável pela adoção desta Política e por definir o responsável pela gestão da segurança da informação na empresa e quaisquer outras deliberações que forem apropriadas ao bom desenvolvimento desta política.

Os Gestores de departamentos da Intergard do Brasil (Operadores) são responsáveis por:

a) Garantir e gerenciar o cumprimento desta Política e demais documentos normativos pelos colaboradores e terceiros sob sua responsabilidade;

b) Identificar e medir as vulnerabilidades e ameaças nos processos e atividades de negócio sob sua responsabilidade, as quais devem ser tratadas diligentemente, de modo a reduzir o risco ao negócio;

c) Identificar incidentes de segurança da informação ou qualquer ação duvidosa praticada por colaboradores e terceiros sob sua responsabilidade e comunicar eventuais ocorrências à área responsável pela gestão de incidentes de segurança da informação da empresa.

Os colaboradores e os operadores de dados da Intergard do Brasil são responsáveis e por estarem cientes, cumprir e manterem-se atualizados com esta Política e demais documentos normativos que a complementem.

Exceções

As exceções que ocorram de forma exclusiva e excepcional a esta Política e aos demais documentos normativos complementares devem ser formalizados e fundamentados pelo Gestor responsável pela área, analisadas pelos

responsáveis pela área gestora dos recursos de informação e aprovadas pela Diretoria da Intergard do Brasil, que poderá a qualquer tempo as revogar.

Violações

As violações a esta Política ou tentativas de burlar as diretrizes e controles estabelecidos serão avaliadas e apuradas pelas áreas de Tecnologia da Informação (TI), Recursos Humanos (RH), Jurídico e pela Diretoria da Intergard do Brasil, que poderão decidir pela aplicação das penalidades cabíveis, mediante procedimento disciplinar, assegurando aos envolvidos a ampla defesa e contraditória.

Disposições Finais Gerais

A presente Política deve ser lida e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as Normas e Procedimentos aplicáveis pela Intergard do Brasil.

Esta Política, bem como os demais documentos que a complementam, se encontram disponíveis no *site* da Intergard Brasil ou, em caso de indisponibilidade, podem ser solicitadas às áreas responsáveis por Recursos Humanos (RH) e Tecnologia da Informação (TI) da Intergard do Brasil.

Periodicidade de Revisão desta Política

A revisão desta Política é realizada pela Diretoria, áreas de Tecnologia da Informação (TI) e de Recursos Humanos (RH), a cada dois anos, ou quando ocorrerem mudanças significativas na legislação pertinente, na estrutura organizacional, nos objetivos de negócio, nos processos internos, nos riscos à segurança das informações e nas Políticas internas da Intergard do Brasil.

Esta versão da Política de Privacidade dos Dados Pessoais e de Segurança da Informação entra em vigor na data de sua aprovação.

Aprovada em 10 de julho de 2024 pela Diretoria da Intergard do Brasil Ltda.

Avenida Capitão Casa,1485 Parque Espacial

09812-000 – São Bernardo do Campo - SP - Brasil

www. Intergard.com.br