POLÍTICA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

LOWCOST

Sumário

Política de privacidade e segurança da informação

1. OBJETIVO

Esta política visa estabelecer os requisitos específicos de proteção e privacidade de dados de pessoas físicas utilizados pela Lowcost, frente à principal regulamentação brasileira sobre o tema, a Lei 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD), com o apoio de outras leis que também mencionam o respeito a privacidade de dados, como a Lei 10.406 de 10 janeiro de 2002 – Código Civil Brasileiro.

O compromisso da Lowcost é evidenciar de forma clara, quais os tipos de dados pessoais são coletados, para quais finalidades, como são tratados, com quem são compartilhados e quais os direitos que os TITULARES DE DADOS possuem sobre seus dados, além do tempo de armazenamento desses dados.

A Lowcost também busca demonstrar o alinhamento com as boas práticas de controles de medidas técnicas e organizacionais de segurança dos dados, definidas em nossa Política de Segurança da Informação e com o nosso Código de Ética e Conduta.

2. ABRANGENCIA

Esta Política de Proteção de Privacidade de Dados se aplica a todas as partes interessadas da Lowcost. Todos os parceiros devem se familiarizar com as regras aqui estabelecidas.

Entende-se por colaborador todos aqueles que executam serviços para a Lowcost, em regime celetista ou estatutário, em qualquer nível hierárquico, tais como conselheiros, diretores, gerentes, supervisores e toda a cadeia produtiva interna.

Por “parceiro” entendem-se todas as pessoas físicas ou jurídicas que, não estando compreendidas na definição de “colaboradores”, prestam algum tipo de serviço, fornecimento ou mantém algum tipo de relação contratual com a Lowcost, incluindo clientes.

Por candidatos à colaborador entende-se toda pessoa física que se submetem a processo de seleção para composição do quadro de colaboradores da Lowcost.

3. TERMOS E DEFINIÇÕES

Definições que serão utilizadas conforme Lei 13.709:2018.

- Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
- 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;
- Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- Encarregado ou DPO (Data Protection Officer): 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);

4. DIRETRIZES

4.1. SOBRE A LOWCOST

A LowCost atua no mercado de soluções tecnológicas e locação de equipamentos para empresas, com liderança e pioneirismo guia o mercado de locação de Notebooks, Smartphones e Impressoras com excelência e qualidade. Já são mais de 1000 empresas que escolheram o aluguel de equipamentos como a melhor solução para a gestão de ativos de TI. Situada em dois endereços:

- Escritório administrativo comercial: Rua Manoel da Nobrega, 891, 4˚ andar – Itaim Bibi – São Paulo – SP, CEP 04001-003
- Operação logística: Av. Tamboré, 1440 , Alphavile – Barueri – SP, CEP 06460-000

Lowcost mantem seus esforços no atendimento dos requisitos regulatórios aplicáveis ao negócio , assim como aos requisitos de produto e serviço.

5. MISSÃO, VISÃO, VALORES

5.1.1. Missão

Oferecer soluções e locação de equipamentos de TI para empresas de todos os segmentos e portes a fim de otimizar o investimento de nossos clientes e impulsionar seus negócios.

5.1.2. Visão

Entregar soluções diferenciadas e inovadoras somadas a um atendimento de excelência para o nosso cliente.

5.1.3. Valores

Temos como prioridade a satisfação de nossos clientes e a busca constante pela excelência no atendimento e serviços prestados. Prezamos as relações baseadas no respeito e comprometimento com ética e transparência.

6. LGPD – Lei 13709:2018

Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Entende-se como 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.

Link da Lei na íntegra:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

6.1. Do Controlador e do Operador

O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

É esperado, que para atendimento da Lei, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

6.2. Da Responsabilidade e do Ressarcimento de Danos

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do Controlador, hipótese em que o operador se equipara ao Controlador, salvo nos casos de exclusão previstos no art. 43 da Lei;

Os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 da Lei.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

Dessa maneira é esperado que medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

6.3. Canal LGPD

O canal LGPD configura-se na mais importante fonte de informação para a esclarecimentos de dúvidas com relação a LGPD, conduta e ética. O uso deve ser feito sob o princípio da boa-fé, ou seja, não se tolera o uso do canal para fazer intrigas, calúnias, relatar mentiras propositadamente ou

retaliação de qualquer natureza. A Lowcost, por sua vez, criará todas as demais condições para a credibilidade dessa ferramenta e a sua efetiva utilização.

A credibilidade do canal e do tratamento das manifestações é fundamental para se alcançar o sucesso desejado. Assim, a Lowcost compromete-se com:

- Confidencialidade da fonte, exceto na extensão necessária para avançar em uma investigação.
- Garantia do anonimato, se o manifestante assim o desejar.
- Proibição de retaliação de qualquer natureza, para quem usa o canal, para quem apura as denúncias e para quem decide sobre as medidas disciplinares cabíveis, quando for o caso.
- Apuração de todas as manifestações e jamais apagar e/ou deletar qualquer registro e aplicação das medidas disciplinares pertinentes e previstas em lei.

O acesso será possível por: lgpd@lowcost.com.br, aos cuidados da Flávio Santos – DPO (Data Protection Officer) ou doravante denominada Encarregada ou DPO.

Como ação de um reporte, haverá uma investigação, observada a legislação brasileira.

Caso seja constatado o desrespeito às condutas aqui apresentadas, ao infrator serão aplicadas as sanções previstas pela Consolidação das Leis do Trabalhos, além da legislação aplicável a cada caso.

6.4. Canais de coleta de dados pessoais

Os dados pessoais que a Lowcost coleta são principalmente, provenientes dos seguintes canais:

- pela equipe de RH, dados de colaboradores são coletados para cumprimento do processo de contratação;
- pela equipe de RH, CVs de candidatos são coletados para seleção de recurso humano no preenchimento de vagas internas;
- processos: Comercial e Marketing, NDC, Operações e Financeiro. Onde são coletados dados pessoais para cadastro para notificações, entrega/retirada de produto, prestar assistência técnica e emitir boletos;
- pelos parceiros das atividades jurídicas, contabilidade com atividades de DP-Departamento Pessoal dos colaboradores da Lowcost, seguro de vida, seguro saúde e vale alimentação.

O detalhamento sobre quais dados são coletados e suas respectivas finalidades estão descritas na tabela 1 – Anexo A desta política.

6.5. Requisitos para coletar e tratar os dados pessoais

Todos os dados solicitados, tratados e coletados pela Lowcost, estão alinhados com as diretrizes apresentadas na LGPD:

- mediante o consentimento do TITULAR DOS DADOS, que o faz ao inserir de forma voluntária seus dados no site na assinatura do contrato de contratação ou de rescisão dos serviços da Lowcost;
- para cumprimento de obrigação legal e procedimentos internos para comprovação de formação e capacitação, a equipe de Recursos Humanos solicita e utiliza os dados pessoais do TITULAR DOS DADOS no seu processo de contratação pela Lowcost.
- quando solicitado pelo TITULAR DOS DADOS para participação de seus dependentes em planos de saúde e seguro de vida contratados pela Lowcost, conforme exigências da lei, a Lowcost coleta dados pessoais destes dependentes (nome completo, sexo, data de nascimento, naturalidade,

nacionalidade, estado civil, filiação e nome do cônjuge, RG, CPF, endereço completo, número de telefone e ocupação profissional).

6.6. Coleta de dados pessoais sensíveis

A Lowcost trata apenas um tipo de dado pessoal sensível, sendo este relacionado à saúde:

- laudo pericial médico para licença médica pelo INSS e encaminhado para a Lowcost a pedido do TITULAR DOS DADOS; e
- laudo pericial médico que ateste algum tipo de deficiência física, para fins de contratação de colaborador para preenchimento de cotas de PCD, conforme exigência do Ministério do Trabalho, encaminhado para a Lowcost pelo TITULAR DOS DADOS.

Outros eventuais dados relacionados à saúde dos TITULARES DOS DADOS ou seus dependentes são tratados diretamente entre o Titular e a operadora do Plano de Saúde, sem intermediação da Lowcost.

6.7. Coleta de dados pessoais de menores e adolescentes

A Lowcost faz a coleta de dados de menores e adolescentes conforme mencionado na LGPD no Art.14, § 1º, mediante à solicitação do TITULAR DOS DADOS, para inclusão em plano de saúde e seguro de vida, conforme descrito no item 6.5 deste documento, na existência de dependentes menores e adolescentes.

Outra situação em que dados pessoais de menores são coletados é na contratação de estagiário menor de idade e menor aprendiz, sendo o processo o mesmo para os demais colaboradores. Além disso, a Lowcost utiliza entidades específicas para contratação de estagiários e menores aprendizes.

6.8. Coleta e tratamento de dados pessoais pela Área de Recursos Humanos

A área de RH da Lowcost coleta dados pessoais através do recebimento de currículos, enviados pelos TITULARES DOS DADOS. Estes dados são compartilhados com as áreas internas responsáveis pelas vagas, em eventual processo seletivo.

O RH também coleta dados pessoais para preenchimento do contrato de trabalho, os quais são fornecidos pelo TITULAR DOS DADOS.

6.9. Direitos dos Titulares de dados pessoais

De acordo com a LGPD, os direitos do TITULAR DOS DADOS em relação ao acesso facilitado das suas informações e como elas são tratadas pelo Controlador são:

- direito de ser informado: o TITULAR DOS DADOS deve ser informado sobre a coleta e tratamento dos seus dados;
- direito de retificação: o TITULAR DOS DADOS pode corrigir e atualizar os seus dados que acredita estarem incorretos ou incompletos;
- direito de apagar: o TITULAR DOS DADOS pode solicitar o direito de ser esquecido (apagar seus dados) desde que observados as exceções mencionadas na LGPD, como o cumprimento de obrigação legal por parte da Lowcost (Controlador) e o seu legítimo interesse.

Solicitações e dúvidas podem ser direcionadas para o e-mail: lgpd@lowcost.com.br

6.10. Compartilhamento de dados pessoais

A Lowcost compartilha dados pessoais dos TITULARES DE DADOS nas seguintes situações:

com seus parceiros de soluções tecnológicas e serviços, que apoiam a Lowcost em suas atividades junto aos seus colaboradores, sempre observando contratos de confidencialidade e os controles de medidas técnicas de segurança entre ambas as partes. Os dados compartilhados são estritamente necessários para que os serviços ou benefícios oferecidos pela Lowcost aos seus colaboradores, terceiros e clientes possam ser realizados. A saber:

- empresa contratada para atividades de folha de pagamento, fiscal entre outras;
- empresa contratada para exames médicos periódicos, consultas médicas, exames admissionais e demissionais;
- empresa contratada para seguro de vida do grupo;
- empresa contratada para administração do Plano de Saúde;
- empresa contratada para suporte e manutenção de TI;
- empresa contratada para suporte e manutenção do sistema de gestão;
- empresa contratada para suporte e manutenção do sistema de informações gerenciais;
- Com empresas para composição de parceria para submissão conjunta de propostas e, caso venham a ser aprovadas para execução dos serviços contratados. Esta composição sempre observa contratos de confidencialidade e controles de medidas técnicas de segurança entre ambas as partes.

Maiores informações no anexo A.

7. Retenção de dados pessoais

Os dados pessoais coletados pela Lowcost possuem um período de retenção na base de dados que é definido da seguinte forma:

- dados de Colaboradores da Lowcost: permanecem nas bases de dados enquanto estiverem ativos;
- dados de ex-Colaboradores (após fim de vínculo contratual): permanecem na base de dados ativa por no mínimo cinco anos a partir do encerramento do contrato (prazo esse que pode ser ampliado pela autoridade competente) para cumprimento de obrigações legais com o Ministério do Trabalho e Previdência Social (ver se existe prazo obrigatório previsto em lei);
- dados de currículos enviados para a área de Recursos Humanos por candidatos a vagas: permanecem por 30 dias em nossa base de dados, sendo excluídos em sua totalidade após esse prazo;
- dados pessoais dos clientes não mantidos para prestação dos serviços conforme consentimento obtido em assinatura de contrato; ou declaração de remessa e/ou coleta e
- Para realização de serviço de assistência técnica dos equipamentos locados.

Dados pessoais	Objetivo	Armazenagem	Período
Nome completo e CPF	Para análise de crédito	GED (pasta de contratos)	Até o encerramento das nossas atividades com o cliente
Nome completo, endereço, CPF, email, nr° de telefone.	Elaboração de orçamento	ERP e e-mail	Até o encerramento das nossas atividades com o cliente
Nome completo, CPF endereço, nr° de telefone celular e e-mail particular	Preenchimento da declaração de remessa e para envio ou coleta de equipamentos e documentos. Para contato referente a coleta e entrega de equipamentos e pedidos de determinados clientes	ERP e e-mail	Até o encerramento das nossas atividades com o cliente
E-mail particular.	Cadastro de chamados, Assistência Técnica	HELPDESK	Até o encerramento das nossas atividades com o cliente.
CPF, RG, CTPS, comprovante endereço, reservista, filiação, nome dos filhos, estado civil, grau de escolaridade, escolaridade, data nascimento, naturalidade, nacionalidade, PIS, título eleitor, habilitação, certidão nascimento, certidão casamento, dados bancários, e-mail pessoal, nome completo.	Emissão do contrato admissional – CLT Atendimento à legislação trabalhista. (Normas regulamentadoras e E-social)	ERP e e-mail	Cinco anos após o desligamento dos colaboradores

PIS RG, CPF e nome completo	Cadastro no ponto digital.	(Ponto mais)	
Nome completo, cargo, CPF e endereço.	Termo de entrega e devolução de notebook.	ERP e e-mail	
CPF, RG, CTPS, comprovante endereço, reservista, filiação, nome dos filhos, estado civil, grau de escolaridade, escolaridade, data nascimento, naturalidade, nacionalidade, PIS, título eleitor, habilitação, certidão nascimento, certidão casamento, dados bancários, e-mail pessoal, nome completo.	Cadastro dos colaboradores no ERP	ERP e e-mail	
Fotos e vídeos	Preenchimento do formulário F.7.1D - Autorização de imagem – Uso do Marketing e RH em Ações sociais, imagens e vídeos eventos comemorativos.	GED e e-mail	
CPF, RG, CTPS, comprovante endereço, reservista, filiação, nome dos filhos, estado civil, grau de escolaridade, escolaridade, data nascimento, naturalidade, nacionalidade, PIS, título eleitor, habilitação, certidão nascimento, certidão casamento, dados bancários, e-mail pessoal, nome completo.	Plataforma para homologação dos colaboradores Camara Arbitral. Ambiente para registro do processo de homologação	Camara Arbitral	
Nome completo, foto e gravações	Preenchimento de lista de presença ou registro de participação em reuniões/capacitação		

	direto dos aplicativos de reunião.		
CPF, RG, CTPS, comprovante endereço, reservista, filiação, nome dos filhos, estado civil, grau de escolaridade, escolaridade, data nascimento, naturalidade, nacionalidade, PIS, título eleitor, habilitação, certidão nascimento, certidão casamento, dados bancários, e-mail pessoal, nome completo. APENAS PARA COLABORADOR QUE ESTEJA TRABANHANDO PARA O PROJETO GERDAU.	Cadastro dos colaboradores no Banco DOC. _ pois a Low cost tem funcionários trabalhando no ambiente CLT.	Banco DOC – Gerdau.	
Nome completo e RG	Cadastro portaria do prédio – emissão de crachá de acesso.	E-mail e Portaria do prédio	
E-mail pessoal e nome completo	Processo admissional e demissional.	ERP e e-mail	

8. Uso de comunicados e informativos

Os comunicados podem ser enviados para os Parceiro de Negócio os contatos externos classificados como parceiros da Lowcost e contatos da imprensa, recebem em seus e-mails as informações e comunicados da organização, que possuem conteúdos que visam informá-los sobre as notícias das áreas de negócio e dos serviços.

Caso os Parceiros de Negócio ou contatos externos não desejarem mais receber os comunicados, eles podem se descadastrar clicando na opção “Cancele o recebimento” no final do comunicado, lembrando que:

- essa opção serve apenas para que o parceiro ou contato externo não receba mais os comunicados e informativos; e
- isso não remove o seu dado pessoal da base de dados, apenas não permite mais o uso de um dado específico (e-mail) para disparo de comunicados e informativos.

Solicitações e dúvidas podem ser direcionadas para o e-mail: lgpd@lowcost.com.br

9. Violação da privacidade de dados pessoais

Nos casos de suspeita de violação da privacidade de dados, ela deve ser relatada imediatamente através do nosso canal de contato LGPD: lgpd@lowcost.com.br

Consultas relacionadas a esta política ou à Lei de Proteção de Dados em geral ou a qualquer outro tema sobre Privacidade de Dados, consulte a área de privacidade de Dados no site institucional:

https://www.lowcost.com.br

Em caso de dúvidas relativas a tratamento de dados e solicitações sobre os direitos dos TITULARES DOS DADOS, entre em contato:

Encarregado de dados (DPO) – Flavio Santos

Email: lgpd@lowcost.com.br

Telefone: +55 11 2178-1010 Ramal: 105

10. Controles técnicos

10.1. Login e senhas

Limitar o acesso à informação e aos recursos de processamento da informação. Os usuários devem somente receber acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.

Um processo formal de provisionamento de acesso do usuário deve ser implementado para conceder ou revogar os direitos de acesso para todos os tipos de usuários em todos os tipos de sistemas e serviços.

A concessão e uso de direitos de acesso privilegiado devem ser restritos e controlados são formalizadas pelo DPO.

Onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações devem ser controlados por um procedimento seguro de entrada no sistema (log-on) e gerenciamento de senhas devem ser interativos e devem assegurar senhas de qualidade. Conforme estabelecido no procedimento de Utilização de recursos computacionais.

11. Dispositivos móveis e trabalho remoto.

A segurança das informações no trabalho remoto e no uso de dispositivos móveis devem ser asseguradas pela organização e usuário. Medidas que apoiam a segurança da informação, de acordo com os riscos decorrentes, medidas foram implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.

Conforme estabelecido no procedimento de Utilização de recursos computacionais.

12. Gestão de ativos

Os ativos associados com informação e com os recursos e processamento da informação foram identificados e inventariados.

A área de Logística é a responsável por manter atualizado o inventário dos ativos.

O processo de RH deve comunicar as áreas da TI e Logística para comunicar as contratações demissões para que os ativos necessários sejam providenciados a entrega e/ou devolução.

Conforme estabelecido no procedimento de Utilização de recursos computacionais.

13. Tratamento de mídias

13.1. Mídias removíeis

Estabelecer a sistemática de controle para prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.

Procedimentos devem ser implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização. Mídias contendo informações devem ser protegidas contra acesso não autorizado, uso impróprio ou corrompida, durante o transporte

As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, conforme estabelecido no procedimento de Utilização de recursos computacionais.

Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sob regravados com segurança.

14. Equipamentos

Estabelecer os controles para:

- falta de energia, impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das operações da organização.
- O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos.
- Os equipamentos devem ter uma manutenção correta para assegurar a sua continua integridade e disponibilidade.
- informações ou software não devem ser retirados do local sem autorização prévia.
- Devem ser tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.
- Assegurar que os equipamentos não monitorados tenham proteção adequada.

14.1. Criptografia (Bitlocker)

A sistemática, de acordo com a classificação da informação, o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação, utilizada pela Lowcost é o Bitlocker.

Os critérios sobre o uso, proteção e tempo de vida das chaves criptográficas deve ser desenvolvida e implementada ao longo de todo o seu ciclo de vida, conforme estabelecido no procedimento de Utilização de recursos computacionais.

14.2. Transferência de informação

Políticas, procedimentos e controles de transferências formais foram estabelecidos para proteger a transferência de informações por meio do uso de todos os tipos de recursos de comunicação inclusive entre a organização e partes externas.

As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas. Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação devem ser identificados, analisados criticamente e documentados.

Dados pessoas podem ser recebidos por e-mail pelo TITULAR DO DADO, demais informações são mantidas apenas no sistema de gestão.

14.3. Cookies

Cookies são arquivos instalados no seu navegador para aprimorar sua experiência e personalizar suas preferências ao visitar nossas plataformas e sites. Utilizamos os cookies do Google Analytics e do Facebook. Acesse o Aviso de Privacidade do Google e do Facebook para obter mais informações sobre o tratamento dos dados:

Google – https://policies.google.com/privacy?hl=pt#about

Facebook – https://www.facebook.com/policy.php

O uso dos cookies é previamente comunicado ao usuário quando de seu acesso às plataformas e sites. As autorizações podem ser revisadas e modificadas pelo usuário, a qualquer momento, pelo seu próprio navegador, contudo, esclarecemos que o bloqueio dos cookies pode interferir no acesso a algumas funções das plataformas e sites.

14.4. Proteção contra malware e Gerenciamento da segurança em redes

A Lowcost implementou o Windons Defender que tem como principais funcionalidades, de antivírus e antipyware que trabalha na detecção, prevenção e recuperação de arquivos, combinados com um adequado programa de conscientização do usuário.

As informações estão majoritariamente armazenadas em em ambientes remotos (nuvens) , onde o nível de segurança é maior em relação aos servidores locais.

Mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede foram identificados e incluídos no acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.

14.5. Registros e monitoramento

Registros de eventos (log) das atividades do usuário (administradores e operadores), exceções, falhas e eventos de segurança da informação devem ser produzidos, mantidos e analisados criticamente, a intervalos regulares. Os recursos devem ser protegidos contra acesso não autorizado e adulteração.

14.6. Controle de software operacional

Procedimentos para controlar a instalação de software em sistemas operacionais devem ser implementados.

Conforme estabelecido no procedimento de Utilização de recursos computacionais.

14.7. Gestão de vulnerabilidades técnicas

Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas em tempo hábil; a exposição da organização a estas vulnerabilidades devem ser avaliada e devem ser tomadas as medidas apropriadas para lidar com os riscos associados.

14.8. Gestão de incidentes de segurança da informação

Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação

Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.

Os eventos de segurança da informação devem ser relatados por meio dos canais de gestão, o mais rapidamente possível. Os funcionários e partes externas que usam os sistemas de informação e serviços da organização devem ser instruídos a notificar e registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços.

A organização deve determinar seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.

A organização deve estabelecer, documentar, implementar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa.

Os recursos de processamento da informação devem ser implementados com redundância suficiente para atender aos requisitos de disponibilidade

Conforme procedimento de Plano de resposta a Incidentes na tecnologia da Informação.

14.9. Vigência e validade

Essa política inicia a sua vigência após aprovação e de sua publicação, com prazo indeterminado de validade, ficando revogadas as disposições em contrário.