1. Objetivos

Este documento declara as diretrizes iniciais para o processo de Governança em Privacidade de Dados na Vultus Cybersecurity Ecosystem em consonância com as boas práticas do mercado e arcabouço regulatório vigente Lei Geral de Proteção de Dados 13.709/18 (LGPD).

1.1. Os objetivos do processo de Governança da Privacidade de Dados são:

1.1.1. **Cumprir as disposições legais e regulamentares**;

1.1.2. **Definir controles** para o tratamento dos riscos identificados e acompanhar o plano de ação para mitigá-los;

1.1.3. **Estabelecer as responsabilidades e os limites** de atuação dos colaboradores, parceiros e fornecedores da Vultus Cybersecurity Ecosystem em relação à proteção dos Dados Pessoais, reforçando a cultura e priorizando as ações necessárias conforme o negócio;

1.1.4. **Formalizar o comprometimento** da Vultus Cybersecurity Ecosystem em adequar-se às leis aplicáveis, fortalecendo os negócios, as parcerias e as relações com os titulares de Dados Pessoais.

1.1.5. **Fornecer recursos** apropriados para execução do processo de Governança em Privacidade de Dados;

1.1.6. **Identificar oportunidades** de melhoria nos processos internos e implementar controles e indicadores para monitoramento e mitigação dos riscos de vazamento de dados pessoais;

2. Público Alvo

Esta Política se aplica aos clientes internos e externos “usuários” da plataforma Vultus One e demais intervenientes participantes do processo de desenvolvimento seguro.

3. Conceitos

Agente de Tratamento: o controlador e o operador;

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano à Vultus Cybersecurity Ecosystem;

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento para retirar a possibilidade de associação, direta ou indireta, do dado pessoal a um indivíduo;

Ativo Intangível: todo elemento que possui valor para Vultus Cybersecurity Ecosystem e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando a dados, reputação, imagem, marca e conhecimento;

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;

Autoridade Nacional de Proteção de Dados: órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da Lei de Proteção de Dados Pessoais aplicável;

Backup: salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de restauração ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada;

Banco de dados: conjunto estruturado de dados, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Ciclo de Vida do Dado Pessoal: fluxo do tratamento do dado pessoal, que envolve as ações de Coleta, Armazenamento, Uso, Compartilhamento e Eliminação do dado pessoal;

Compartilhamento de dados pessoais: comunicação, difusão, transferência nacional ou cional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos, entidades ou pessoais, e para uma ou mais modalidades de tratamento;

Confidencialidade: garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do

conhecimento dos não autorizados;

Consentimento: manifestação livre, informada e inequívoca pela qual o Titular dos dados pessoais concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Controlador: pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Criptografia: é um meio de aprimorar a segurança de uma mensagem ou arquivo codificando o conteúdo de modo que ele só possa ser lido por quem tenha a chave/ senha de criptografia correta para decodificá-lo;

Dado anonimizado: dado que não identifica de forma direta ou indireta um Titular dos dados pessoais, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

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 física;

Dado Pessoal: informação relacionada à pessoa física identificada ou identificável. Para os propósitos desta Política, os dados pessoais são classificados como Informação Confidencial, abrangendo dados pessoais de consumidores, parceiros, fornecedores e dirigentes, colaboradores ou terceiros;

Dados de Saúde: dados sensíveis que permitem inferir informações referentes à saúde do titular;

Disponibilidade: garantia de que as informações e os Recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso;

Encarregado da Proteção de Dados Pessoais: pessoa indicada pela Vultus Cybersecurity Ecosystem e que atua como canal de comunicação entre a Organização e os Titulares dos dados pessoais ou a Autoridade Nacional de Proteção de Dados;

Incidente de Segurança da Informação: é um evento adverso identificado que indica possível violação à política de segurança da informação ou documentos complementares, falha de controles ou situação previamente desconhecida e que possa ser relevante à segurança da informação;

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;

Integridade: garantia de que as informações estejam fidedignas em relação à última alteração desejada durante o seu ciclo de vida;

Operador ou Processador: pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Pseudonimização: é o tratamento por meio do qual um dado pessoal perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro;

Relatório de Impacto à Proteção de Dados Pessoais: documento que contém a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais dos Titulares dos dados pessoais, bem como medidas, salvaguardas e mecanismos de mitigação desses riscos;

Risco: combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos;

Segurança cibernética: é a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação contra 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 no espaço cibernético;

Sigilo profissional: trata da manutenção de segredo para informação valiosa, cujo domínio de divulgação deva ser fechado, ou seja, restrito a um cliente, a uma organização ou a um grupo, uma vez que a ele é confiada a manipulação da informação;

Solicitação de Titular dos dados pessoais: requisição do Titular dos dados pessoais acerca de seus direitos estabelecidos em lei e relativos ao tratamento dos seus dados pessoais;

Titular dos Dados Pessoais: pessoa física a quem se referem os dados pessoais que são objeto de tratamento;

Tratamento de Dados Pessoais: 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;

Violação de Dados Pessoais: destruição, perda, alteração, divulgação acidental ou ilegal, não autorizada ou acesso a dados pessoais transmitidos, armazenados ou de outra forma processados, resultante de incidente de segurança.

4. Responsabilidades

4.1. Diretoria(s) e Membro(s) do Board Interno

4.1.1. Analisar todo o conteúdo desta Política e aprová-la conforme determinação do regimento interno da Organização;

4.1.2. Zelar para que a Vultus Cybersecurity Ecosystem cumpra com os pré requisitos da Lei Geral de Proteção de Dados;

4.1.3. Instaurar, quando necessário, processo de investigação para apuração de responsabilidade dos envolvidos em violações as diretrizes declaradas nesta Política.

4.2. Encarregado pela Proteção de Dados Pessoais (DPO)

4.2.1. Elaborar e ou revisar os procedimentos internos relativos ao gerenciamento dos dados pessoais;

4.2.2. Organizar treinamentos internos / capacitação do conhecimento e disseminação da Cultuta de Proteção de Dados Pessoais;

4.2.3. Analisar e aprovar contratos entre as partes que envolvam tratamento de dados pessoais;

4.2.4. Avaliar e divulgar o relatório de Impacto à Proteção de Dados Pessoais;

4.2.5. Monitorar junto aos Heads da Vultus Cybersecurity Ecosystem, que os processos estejam atualizados e em consonância com os pré requsitos da Lei Geral de Proteção de Dados;

4.2.6. Acolher reclamações e questões relacionadas aos titulares da dados pessoais sobre a privacidade, bem como, atender aos órgãos reguladores e autoridade nacional de proteção de dados.

4.3. Fórum Vultus Cybersecurity Ecosystem – Segurança da Informação

4.3.1. Definir controles para mitigar a integridade, confidencialidade e disponibilidade dos dados pessoais, conforme determinado em texto da Lei Geral de Proteção de Dados "vigente";

4.3.2. Identificar e avaliar os riscos relacionados à Segurança da Informação e propor planos de ação para mitigá-los.

4.4. Área de Segurança da Informação

4.4.1. Cumprir e fazer cumprir todas as diretrizes declaradas nesta Política e nas demais que possam complementar a Governança de Dados Pessoais no ambiente tecnológica da Vultus Cybersecurity Ecosystem;

4.4.2. Assegurar tempestivamente que os processos, serviços, sistemas e equipamentos utilizados para o tratamento de dados pessoais estejam dentro de um padrão aceitavel de segurança da informação;

4.4.3. Monitorar o ambiente tecnológico que contenha armazenamento de dados pessoais e garantir que as medidas necessárias e apropriadas para manutenção da confidencialidade, integridade e disponibilidade dos dados pessoais estejam sendo tomadas;

4.4.4. Coletar e manter registros de toda atividade relacionada ao tratamento de dados pessoais, desde documentos que comprovem o consentimento dos Titulares dos dados pessoais (logs de consentimento, por exemplo) até registro de utilização, compartilhamento, exclusão e outros, pelo período legal exigido.

4.5. Área de Recursos Humanos

4.5.1. Promover, em conjunto com o Encarregado da Proteção de Dados Pessoais, a cultura de proteção de dados pessoais, realizando campanhas de capacitação e divulgação da proteção dos dados pessoais;

4.5.2. Estipular controles de Proteção de Dados Pessoais especificamente relacionados aos processos de contratação, desligamento (ou encerramento de prestação de serviços), modificação de atividades (incluindo a promoção) e afastamentos (incluindo férias e quaisquer licenças ou suspensões).

4.6. Heads Vultus Cybersecurity Ecosystem

4.6.1. Firmar Acordo de Confidencialidade com o parceiro de negócios;

4.6.2. Preparar e manter atualizada uma lista com todas as categorias de dados pessoais tratados sob a sua responsabilidade, e submeter essa lista ao Encarregado da Proteção de Dados Pessoais e a Segurança da Informação;

4.6.3. Ao identificar violações de dados pessoais ou qualquer ação duvidosa, comunicar prontamente a Área de Compliance | DPO e Segurança da Informação.

4.7. Colaboradores Vultus Cybersecurity Ecosystem

4.7.1. Tratar os dados pessoais sob responsabilidade somente para fins autorizados, de forma ética e legal, confomre o Código de Conduta Ética Profissional, sendo assim, respeitando os direitos do Titular dos dados pessoais;

4.7.2. Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e legalidade dos dados pessoais acessados ou manipulados, não utilizando, enviando, transmitindo ou compartilhando indevidamente estes dados pessoais, em qualquer local ou mídia, inclusive na Internet;

4.7.3. Reportar formalmente a Área de Compliance | DPO e de Segurança da Informação e ao Encarregado da Proteção de Dados Pessoais quaisquer eventos relativos à violação ou possibilidade de violação de dados pessoais ou atividades suspeitas de que tiver conhecimento;

5. Políticas

5.1. Princípios de Proteção de Dados Pessoais

5.1.1. A Vultus Cybersecurity Ecosystem no exercício de suas atividades operacionais através da plataforma Vultus One, deve observar o tratamento de dados pessoais regidos pelos seguintes princípios, a saber:

5.1.1.1. **Adequação:** Os Dados Pessoais devem ser processados de modo adequado e pertinente às suas finalidades de uso;

5.1.1.2. **Finalidade:** Os Dados Pessoais devem ser coletados apenas para as finalidades determinadas, explícitas, legítimas e informadas antes do tratamento, não podendo ser tratados posteriormente para finalidades incompatíveis;

5.1.1.3. **Licitude:** O tratamento dos Dados Pessoais deve ser realizado de modo lícito, justo e transparente com relação ao titular dos Dados Pessoais;

5.1.1.4. **Limitação de armazenamento:** Os Dados Pessoais e registros devem ser guardados apenas durante o período estritamente necessário de acordo com sua finalidade, padrões dispostos pela Autoridade Nacional de Proteção de dados (ANPD) e de acordo com a legislação aplicável.

5.1.1.5. **Livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus Dados Pessoais;

5.1.1.6. **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

5.1.1.7. **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de Dados Pessoais;

5.1.1.8. **Proporcionalidade e Necessidade:** A coleta dos Dados Pessoais deve ser proporcional aos objetivos do negócio. A menor quantidade e categoria de Dados Pessoais possível deve ser coletada, armazenada e usada;

5.1.1.9. **Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o

cumprimento da finalidade de seu tratamento;

5.1.1.10. **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas.

5.1.1.11. **Segurança:** O tratamento deve ser realizado de modo a garantir a proteção e segurança da informação dos Dados Pessoais, incluindo a proteção contra o tratamento não autorizado ou ilícito, perda, destruição ou dano acidental, devendo a Vultus Cybersecurity Ecosystem adotar medidas técnicas e organizacionais para salvaguardar a integridade, confidencialidade e disponibilidade dos Dados Pessoais.

5.1.1.12. **Subsidiariedade:** Deve-se sempre buscar formas alternativas (subsidiárias) de se atingir as mesmas finalidades por meios menos invasivos à privacidade do Titular dos Dados Pessoais.

5.1.1.13. **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

5.2. Diretrizes Operacionais

5.2.1. O Tratamento de Dados Pessoais

5.2.1.1. O tratamento de Dados Pessoais significa toda e qualquer operação realizada pela Vultus Cybersecurity Ecosystem com Dados Pessoais, a exemplo de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração entre outras operações possíveis;

5.2.1.2. A coleta do dado pessoal significa a entrada do dado pessoal no ecossistema da plataforma Vultus One, podendo ser feita por meio de sistemas da informação ligados a sites, aplicativos, recebimento de arquivos, acesso a base de dados e outras formas operacionais envolvidas durante o exercício de contrato;

5.2.2. O Ato do Consentimento

5.2.2.1. Quando o tratamento dos Dados Pessoais se basear no consentimento do titular, este deve ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular concorda com o tratamento de Dados Pessoais da forma declarada;

5.2.2.2. O consentimento pode ser dado de modo escrito, digital ou oral, sendo fundamental que a Vultus Cybersecurity Ecosystem consiga registrar e comprovar a coleta do consentimento;

5.2.2.3. O silêncio, opções pré-validadas, generalistas ou a omissão NÃO são consideradas manifestações de consentimento;

5.2.2.4. Se o consentimento do titular dos Dados Pessoais for dado no contexto de uma declaração escrita que diga também respeito a outras finalidades de tratamento, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente das demais finalidades de modo inteligível, destacado, de fácil acesso e em linguagem clara e simples;

5.2.2.5. O consentimento para tratamento de Dados Pessoais sensíveis deve ser coletado de forma específica e destacada, para finalidades específicas.

5.2.3. A Eliminação do Dado Pessoal

5.2.3.1. Os Dados Pessoais devem ser armazenados por período limitado, levando em consideração a finalidade específica do tratamento;

5.2.3.2. Após cumprida a finalidade do tratamento e findo o prazo de armazenamento determinado, os dados podem ser eliminados de modo seguro, sejam eles registrados em meios físicos ou digitais;

5.2.3.3. A eliminação dos Dados Pessoais poderá ser realizada também a pedido do titular do dado ou da Autoridade Nacional de Proteção de Dados Pessoais.

5.2.4. O Relatório de Impacto à Proteção de Dados Pessoais

5.2.4.1. O relatório de impacto à proteção de Dados Pessoais visa a descrição dos processos de tratamento de Dados Pessoais e as medidas e mecanismos empregados para mitigar esses riscos pela Vultus Cybersecurity Ecosystem;

5.2.4.2. Todo tratamento de Dados Pessoais tendo como base legal o legítimo interesse deve ser precedido de relatório de impacto à proteção de Dados Pessoais (LIA Levantamento de Legítimo Interesse).

5.2.5. Resposta à ANPD – Autoridade Nacional de Proteção de Dados Pessoais

5.2.5.1. Os Diretores e Membros do Board Interno, colaboradores ou terceiros têm o dever de notificar o Encarregado da Proteção de Dados Pessoais, sem demora injustificada, e antes de responder à Autoridade, sobre qualquer ordem ou requisição relativa à privacidade e proteção de dados pessoais recebida da Autoridade Nacional de Proteção de Dados;

5.2.5.2. Quando requisitado por meio de ordem judicial, caberá à área Jurídica fornecer quaisquer esclarecimentos e entregar as informações demandadas pela Autoridade, sem demora injustificada, podendo requisitar o apoio do Encarregado da Proteção de Dados Pessoais caso entenda como necessário;

5.2.5.3. Quando a Autoridade determinar a necessidade de prestação de esclarecimentos, caberá à Área Jurídica buscar o Encarregado da Proteção de Dados Pessoais, bem como dirigentes, colaboradores, terceiros ou Heads que tenham envolvimento no fluxo de dados pessoais a ser analisado, solicitando relatórios, fazendo entrevistas, e buscando compilar o máximo de informações pertinentes para estruturar uma resposta adequada e concisa.

5.2.6. O Tratamento de Dados Pessoais Sensíveis

5.2.6.1. O tratamento de Dados Pessoais sensíveis deve ser precedido de relatório de impacto à proteção de Dados Pessoais;

5.2.6.2. O tratamento de Dados Pessoais sensíveis poderá ocorrer com o

consentimento dado pelo titular, realizado de forma específica e destacada, para finalidades específicas;

5.2.6.3. O tratamento de Dados Pessoais sensíveis poderá ocorrer sem o consentimento do titular dos Dados Pessoais, quando for indispensável o tratamento, nas seguintes hipóteses:

5.2.6.3.1. Cumprimento de obrigação legal ou regulatória;

5.2.6.3.2. Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

5.2.6.3.3. Feita a anonimização, compartilhamento para realização de estudos por órgãos de pesquisa;

5.2.6.3.4. Garantia de prevenção à fraude e segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (hipótese de legitimação exclusiva da lei de proteção de Dados Pessoais brasileira, aplicável, portanto, somente no território nacional);

5.2.6.3.5. Proteção da vida ou da incolumidade física do titular ou terceiro;

5.2.6.3.6. Tratamento compartilhado de Dados Pessoais pela administração pública, necessários para execução de políticas públicas previstas em leis ou regulamentos;

5.2.6.3.7. Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

5.2.7. O Tratamento de Dados Pessoais Sensíveis

5.2.7.1. Dados de saúde poderão ser compartilhados entre controladores, levando em consideração o benefício dos interesses dos titulares e se for realizado, exclusivamente, para:

A. assistência à saúde;

B. assistência farmacêutica;

C. prestação de serviços de saúde;

D. serviços auxiliares de diagnose;

E. serviços de terapia;

5.2.8. Contratos Vultus Cybersecurity Ecosystem

5.2.8.1. **A Vultus Cybersecurity Ecosystem na figura de Controlador**, sempre que fizer uso de um Operador, deve estabelecer contrato tendo em vista as regulamentações relacionadas à privacidade e proteção de Dados Pessoais vigentes no país onde ocorrerá o tratamento dos Dados Pessoais;

5.2.8.2. **A Vultus Cybersecurity Ecosystem na figura de Controlador,** deve garantir que todos os Contratos que envolvam serviços e/ou sistemas nos quais haja tratamento e/ou armazenamento de Dados Pessoais por operador contenham, no mínimo, os seguintes itens:

5.2.8.2.1. Obrigatoriedade legal de atuar respeitando legislação vigente no local de tratamento e/ou armazenamento dos Dados Pessoais, em especial a Lei 13.709 ("Lei Geral de Proteção de Dados Pessoais");

5.2.8.2.2. Diretrizes de tratamento:

A. Assunto do tratamento;

B. Duração do tratamento;

C. Natureza e propósito do tratamento;

D. Tipos de Dados Pessoais envolvidos;

E. Categorias de Dados Pessoais envolvidos;

F. Forma de coleta dos Dados Pessoais;

G. Forma de armazenamento dos Dados Pessoais;

H. Qualquer tipo de tratamento fora do especificado acima será considerado descumprimento do contrato.

5.2.8.3. Procedimentos a serem tomados no caso de requisições de titulares dos Dados Pessoais;

5.2.8.4. Obrigatoriedade acerca de manutenção de confidencialidade dos Dados Pessoais;

5.2.8.5. Adoção de medidas de segurança técnicas e organizacionais para garantir a confidencialidade, integridade e disponibilidade dos Dados Pessoais que passem por tratamento;

5.2.8.6. Adoção de medidas de anonimização, pseudonimização (quando aplicável) e criptografia dos Dados Pessoais conforme a necessidade do

tratamento em questão;

5.2.8.7. Notificação à Vultus Cybersecurity Ecosystem em até 72 horas sobre:

A. qualquer não cumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais;

B. qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais;

C. qualquer violação de segurança na contratada ou dos demais operadores;

D. quaisquer exposições ou ameaças em relação à conformidade com a proteção de Dados Pessoais.

5.3. Das Disposições Finais

5.3.1. O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com os demais procedimentos aplicáveis pela Organização.

5.3.2. Qualquer dúvida relativa a esta Política deve ser encaminhada ao responsável pela Área de CRC – Área de Riscos e Compliance, conforme segue:

Canal Externo (dpo@vultuscyber.com.br);

Canal interno (compliance@vultuscyber.com.br);

Telefone (011) 9.5617-7032;

Acesse o DPO (gilson.batista@vultuscyber.com.br).

5.3.3. Esta política entra em vigor na data de sua publicação e sua vigência e de até 12 meses. Podendo ser revisitada de acordo com a necessidade da Alta Administração.

6. Documentos de Referência

Lei nº 13.709, de 14 de agosto de 2018, Lei de Proteção de Dados Pessoais;

Decreto nº 8.771, de 11 de maio de 2016, regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações;

Lei nº 12.965, de 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

Lei nº 12.527, de 18 de novembro de 2011, regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

6.1. Penalidades

As violações às diretrizes descritas nesta Política podem acarretar medidas disciplinares a serem avaliadas pela alta administração da Vultus Cybersecurity Ecosystem.

7. Registros de Revisão

Revisão	Data	Conteúdo Revisado
016.01_Cód.CRC	25/02/2022	Elaboração da Política Pública de Governança da Privacidade de Dados Pessoais.
016.02_Cód.CRC	24/10/2022	Revisão da versão 1.0 com a atualização do item “8. Aprovações” com responsável.
016.03_Cód.CRC	29/09/2023	Revisão da versão 1.0 com a atualização do item “8. Aprovações” com responsável.

016.04_Cód.CRC	09/10/2024	Revisão da logo marca, nome da organização, fonte, revisão e o item 10. Aprovações.

8. Aprovações

Responsável	Data	Assinatura
Diretoria Jurídica	10/10/2024	Alexandre Brum | Leonardo Muroya
DPO e Riscos Corporativos	10/10/2024	Gilson Batista