ESPECIFICAÇÕES TÉCNICAS

Segurança da Informação - Versão 2.0

1. Termos e Definições

Os termos utilizados neste documento seguem as definições estabelecidas abaixo, bem como nos Termos de Uso e Política de Privacidade da Clicksign, disponíveis em www.clicksign.com.

| Colaboradores

Empregado, estagiário, prestador de serviço, terceirizado, conveniado, credenciado, fornecedor, cliente, menor aprendiz, ou qualquer outro indivíduo ou organização que venham a ter relacionamento, direta ou indiretamente com a Clicksign para prestação de serviços dentro do escopo de um contrato específico.

| Dado Pessoal

Toda e qualquer informação relativa a uma pessoa natural, identificada ou identificável.

| Partes externas

Inclui clientes, fornecedores, prestadores de serviços, parceiros, investidores, governo, imprensa e sociedade em geral.

| Signatário

Pessoa que utiliza a Plataforma para assinar um Documento.

| Ativos

São elementos que manipulam os processos da informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada. Figuram como ativos, além da informação, pessoas, AWS, notebooks, impressoras, servidores, dispositivos de armazenamento de dados, sistemas de informática, dispositivos e meios de transmissão de dados ou quaisquer outros dispositivos que venham processar informação ou prover acesso aos recursos de informática.

| Proprietário do Ativo

Responsável por operar, classificar, proteger e permitir acesso ao ativo.

2. Diretrizes

2.1. Políticas de Segurança da Informação

A Clicksign possui um conjunto de Políticas de Segurança da Informação, aprovado pelo C-level, publicado e comunicado a todos os colaboradores e partes externas relevantes. Os documentos de Segurança da Informação são apoiados por procedimentos específicos, que exigem a implementação de controles estruturados, considerando as necessidades da Clicksign.

São exemplos de tópicos específicos contidos nos documentos internos da Clicksign:

A. Controle de acesso;
B. Classificação e tratamento da informação;
C. Desenvolvimento seguro;
D. Orientações aos usuários finais;
E. Uso aceitável dos ativos;
F. Transferência de informações;
G. Dispositivos móveis e trabalho remoto;
H. *Backup*;
I. Transferência da informação;
J. Proteção contra códigos maliciosos;
K. Gerenciamento de vulnerabilidades técnicas;
L. Controles criptográficos;
M. Segurança nas comunicações;
N. Privacidade;
O. Gestão de fornecedores.

2.2. Organização da Segurança da Informação

A Clicksign, em conformidade com as diretrizes internas, define:

- As responsabilidades pela proteção de cada ativo e pelo cumprimento de processos de segurança da informação específicos.
- Os deveres locais para a proteção dos ativos e para a realização de processos de segurança da informação específicos.
- As atividades de gerenciamento dos riscos de segurança da informação, bem como a aceitação dos riscos residuais.

Tais definições são complementadas, quando necessário, com orientações mais detalhadas para locais específicos e recursos de processamento da informação.

Controles Relacionados:

- **Segregação de funções**: Funções conflitantes e áreas de responsabilidade são segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da Clicksign.
- **Contato com autoridades**: Contatos apropriados com autoridades relevantes são mantidos.
- **Segurança da informação no gerenciamento de projetos**: A segurança da informação é considerada no gerenciamento de projetos, independentemente do tipo destes.
- **Dispositivos móveis e trabalho remoto**: Cuidados especiais são tomados para assegurar que as informações do negócio não sejam comprometidas. A política de trabalho remoto e utilização de equipamento pessoal fornece orientações e boas práticas para que os riscos do uso de tais dispositivos sejam mitigados.

2.3. Segurança em Recursos Humanos

Asseguramos que colaboradores e terceiros à Clicksign entendam suas responsabilidades e estejam em conformidade com os papéis para os quais foram designados.

Os controles relacionados são:

- **Seleção**: Verificação e comprovação do histórico profissional e acadêmico, aspectos comportamentais e fit cultural são realizadas para todos os candidatos a uma posição na Clicksign, respeitando-se a ética, regulamentações e leis relevantes, bem como a proporcionalidade aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.
- **Termos e condições de contratação**: As obrigações contratuais com colaboradores e partes externas prevêem as suas responsabilidades e as da Clicksign para a segurança da informação.
- **Durante a contratação**: Assegurar que os colaboradores e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.

- **Conscientização, educação e treinamento em segurança da informação**: Todos os colaboradores da Clicksign e, quando pertinente, partes externas recebem treinamento, educação e conscientização apropriados, bem como as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

3. Gestão de Ativos

Identificamos os ativos da Clicksign e definimos as responsabilidades apropriadas para a sua proteção.

Inventário dos ativos: Os ativos associados com informação e com os recursos de processamento da informação são identificados e inventariados.

Proprietário dos ativos: As pessoas e outras entidades que tenham responsabilidades aprovadas pela direção para qualificar o ciclo de vida do ativo são designadas como proprietárias deste ativo.

Uso aceitável dos ativos: As regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação são identificadas, documentadas e implementadas.

Classificação da informação: A Clicksign assegura que a informação receba um nível adequado de proteção, de acordo com a sua importância para a empresa.

Tratamento de mídias: Há prevenção de divulgação não autorizada, bem como da modificação, remoção ou destruição da informação armazenada nas mídias.

4. Controle de Acesso

Procedimentos de controle de acesso são estabelecidos, documentados e analisados criticamente, baseado nos requisitos de segurança da informação e dos negócios.

Acesso às redes e aos serviços de rede : Os usuários somente recebem acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.

Gerenciamento de acesso do usuário: Assegura acesso de usuário autorizado e previne acesso não autorizado a sistemas e serviços.

Registro e cancelamento de usuário : Um processo formal de registro e cancelamento de usuário é implementado para permitir os direitos de acesso.

Provisionamento para acesso de usuário: Um processo formal de provisionamento de acesso é implementado para conceder ou revogar os direitos de acesso para todos os tipos de usuários em todos os tipos de sistemas e serviços.

Gerenciamento de direitos de acesso privilegiado: A concessão e uso de direitos de acesso privilegiado são restritos e controlados.

Gerenciamento da informação de autenticação secreta de usuários: A concessão de informação de autenticação secreta é controlada por meio de um processo de gerenciamento formal.

Análise crítica dos direitos de acesso de usuário: Os proprietários de ativos analisam criticamente os direitos de acesso dos usuários, a intervalos regulares.

Retirada ou ajuste de direitos de acesso: Os direitos de acesso de todos os colaboradores e partes externas às informações e aos recursos de processamento da informação são retirados logo após o encerramento de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades.

Responsabilidades dos usuários: Tornamos os usuários responsáveis pela proteção das suas informações de autenticação.

Controle de acesso ao código-fonte de programas: Os acessos ao código-fonte de programas e de itens associados (como desenhos, especificações, planos de verificação e de validação) são estritamente controlados, com a finalidade de prevenir a introdução de funcionalidade não autorizada,evitar mudanças não intencionais e manter a confidencialidade de propriedade intelectual valiosa.

5. Processamento e Retenção de Dados

Localização dos servidores: A Clicksign armazena e processa informações em servidores da AWS localizados em São Paulo e na Virgínia do Norte, nos Estados Unidos. Para mais detalhes a respeito da transferência de Dados Pessoais, consulte a Política de Privacidade.

Download de Documentos: Nos casos de contratação de plano específico e durante a vigência do contrato de prestação de serviços, a Clicksign adota procedimentos para permitir que o Cliente efetue o download de seus Documentos na forma de arquivo PDF e Zip via interface gráfica ou API.

Mover um Documento para a "lixeira": Depois que um Documento for movido para a "lixeira" por um Cliente, o administrador da conta Clicksign - a ser indicado pelo Cliente -

poderá restaurá-lo a qualquer momento durante a vigência do contrato de prestação de serviços, a menos que o Documento seja excluído definitivamente, ocasião em que seguirá o item "Exclusão" abaixo.

Exclusão: A exclusão definitiva de documentos, ocorrerá, após o cancelamento da conta, em duas etapas: (i) no prazo de 72 (setenta e duas) horas, o Documento será excluído das bases da Plataforma; (ii) ultrapassado o prazo referido, o Documento será excluído dos nossos *backups* após 30 (trinta) dias.

Retenção: Apenas na medida do necessário, a Clicksign retém Informações para (i) prestação dos serviços aos Usuários; (ii) cumprimento de obrigação legal ou regulatória e (iii) defesa em processos administrativos, judiciais ou arbitrais.

6. Criptografia

Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

Gerenciamento de chaves: Foi desenvolvida e implementada uma política sobre o uso, proteção e ciclo de vida das chaves criptográficas.

Criptografia de arquivos: São adotados procedimentos para criptografar as informações armazenadas no S3 da Amazon com algoritmo de cifra AES-256. As bases de dados da Clicksign são criptografadas e a criptografia é programada para ocorrer no S3, antes das Informações serem salvas.

Criptografia de transmissões: A Clicksign utiliza o *Transport Layer Security* (TLS) e criptografia de 256 bits para aumentar a proteção de informações durante a transmissão por redes públicas.

Cartão de crédito: A Clicksign não processa nem armazena informações de cartão de crédito. Tais procedimentos são realizados por prestadores de solução de pagamento com certificação PCI contratados pela Clicksign.

7. Segurança Física e do Ambiente

Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da Clicksign.

Segurança em escritórios, salas e instalações: A Clicksign atua integralmente no modelo *home office* e adota (i) política de BYOD; (ii) recomendações e assinatura de termos de responsabilidades; (iii) Políticas Institucionais e (iv) Código de Conduta.

Amazon Web Services: A Clicksign utiliza os serviços *Amazon Web Services* (AWS) para a sua infraestrutura, particularmente o EC2 (Amazon Elastic Compute Cloud), o RDS (*Amazon Relational Database Service*), o EKS (*Elastic Kubernetes Service*) e o S3 (*Amazon Simple Storage Service*) com criptografia de alta performance, controle de versionamento de arquivos e níveis de permissões diversos para restringir acessos indevidos às Informações.

8. Segurança nas Operações

Garantimos a operação segura e correta dos recursos de processamento da informação.

Documentação dos procedimentos de operação: Os procedimentos de operação são documentados e disponibilizados a todos os usuários que necessitem deles.

Gestão de mudanças: As mudanças na Clicksign, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação são controladas.

Gestão de capacidade: A utilização dos recursos é monitorada e ajustada e as projeções são feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema.

Separação dos ambientes de desenvolvimento, teste e produção: Ambientes de desenvolvimento, teste e produção são separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.

Proteção contra códigos maliciosos: As informações e os recursos de processamento da informação estão protegidos contra códigos maliciosos.

Cópias de segurança: Cópias de segurança das informações, *softwares* e imagens do sistema são efetuadas e testadas regularmente, conforme a política de geração de cópias de segurança definida.

Registros e monitoramento: Registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação são produzidos, mantidos e analisados criticamente, a intervalos regulares.

Proteção das informações dos registros de eventos (logs): As informações dos registros de eventos (log) e seus recursos são protegidas contra acesso não autorizado e adulteração.

Registros de eventos (log) de administrador e operador: As atividades dos administradores e operadores do sistema são registradas e os registros (logs) protegidos e analisados criticamente, a intervalos regulares.

Sincronização dos relógios: Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, são sincronizados com uma única fonte de tempo precisa.

Controle de software operacional: Procedimentos para controlar a instalação de software em sistemas operacionais são implementados.

Gestão de vulnerabilidades técnicas: Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso são obtidas em tempo hábil, permitindo a avaliação da exposição da organização a estas vulnerabilidades e a tomada de medidas apropriadas para lidar com os riscos associados.

9. Integridade

Hashing: A Clicksign adota procedimentos para utilizar o hashing – algoritmo SHA-256 – para proteção da integridade dos documentos. A verificação baseada em hashing assegura que um arquivo não foi alterado ao comparar o seu valor de hash com um valor previamente calculado. Se houver a tentativa de fazer hashing de um Documento com apenas uma pequena diferença do original, o resultado do Hash SHA-256 será totalmente diferente.

Número de documento e Log: Quando o Cliente faz upload de um Documento, a Clicksign adota procedimentos tanto para registrá-lo com um número único quanto para criar um Log registrando tal número. Dessa forma, o Documento e seu respectivo Log são logicamente associados. O Log é projetado para registrar assinaturas e outras informações relevantes, tais como hora, eventos e endereços de IP.

Marca d'água: Quando o Usuário faz upload de um Documento em alguns tipos de arquivos, como Microsoft Word ou PDF, a Clicksign adota procedimentos para inserir o número único de Documento. Essa marca d'água serve para ajudar a identificar a cópia impressa do Documento baixado da Clicksign.

Autenticação de Informações: A Clicksign adota procedimentos para assinar arquivos de Log com o certificado digital ICP-Brasil da Clicksign, de modo a atestar a proveniência do Documento.

10. Segurança nas Comunicações

Garantir a proteção das informações em redes e dos recursos de processamento da informação que os apoiam.

Controles de redes: As redes são gerenciadas e controladas para proteger as informações nos sistemas e aplicações.

Segurança dos serviços de rede: Mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede são identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente quanto para terceirizados.

Segregação de redes: Grupos de serviços de informação, usuários e sistemas de informação são segregados em redes.

***Firewalls* e VPN**: Os serviços da Clicksign hospedados na internet, tais como servidores de aplicação e outros servidores que operam com o EKS (*Elastic Kubernetes Services*), são protegidos por *Firewall* e WAF (*Web Application firewall)* nos data centers AWS. A Clicksign faz uso de rede particular virtual (VPN) para tornar segura a comunicação com nossos servidores. Os servidores de base de dados, apartados, não são expostos via internet.

11. Transferência de Informação

A segurança da informação transferida dentro da Clicksign e com quaisquer entidades externas.

Políticas e procedimentos para transferência de informações: Políticas, procedimentos e controles de transferências formais são estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.

Acordos para transferência de informações: São estabelecidos acordos para transferência segura de informações do negócio entre a Clicksign e partes externas.

Mensagens eletrônicas: As informações que trafegam em mensagens eletrônicas são adequadamente protegidas.

Acordos de confidencialidade e não divulgação: Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da Clicksign para a proteção da informação são identificados, analisados criticamente e documentados.

12. Aquisição, Desenvolvimento e Manutenção de Sistemas

A segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação na Clicksign. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas.

Análise e especificação dos requisitos de segurança da informação: Os requisitos relacionados com segurança da informação são incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.

Serviços de aplicação seguros em redes públicas: As informações envolvidas nos serviços de aplicação que transitam sobre redes públicas são protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.

Protegendo as transações nos aplicativos de serviços: Informações envolvidas em transações nos aplicativos de serviços são protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação da mensagem não autorizada.

Segurança em processos de desenvolvimento e de suporte: A segurança da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação.

Codificação: A Clicksign procura seguir as melhores práticas de mercado para desenvolvimento seguro de código (como o *OWASP Development Guide*) e realiza revisões e testes gerais antes de novos lançamentos. Os ambientes de desenvolvimento e teste são mantidos completamente separados do ambiente de produção.

Política de desenvolvimento seguro: Regras para o desenvolvimento de sistemas e *software* são estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.

Procedimentos para controle de mudanças de sistemas: As mudanças em sistemas no ciclo de vida de desenvolvimento são controladas utilizando procedimentos formais de controle de mudanças.

Análise crítica técnica das aplicações da Clicksign após mudanças nas plataformas operacionais: Quando plataformas operacionais forem modificadas, convém que as aplicações críticas de negócio sejam analisadas criticamente e testadas para assegurar que não ocorreu nenhum impacto adverso nas operações da Clicksign ou na segurança.

Restrições sobre mudanças em pacotes de *software*: Modificações em pacotes de software são desencorajadas, estão limitadas às mudanças necessárias e são estritamente controladas.

Princípios para projetar sistemas seguros: Princípios para projetar sistemas seguros são estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.

Ambiente seguro para desenvolvimento: A Clicksign estabelece e protege adequadamente ambientes de desenvolvimento seguros para os esforços de

desenvolvimento e integração de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistemas.

Teste de segurança do sistema: Os testes de funcionalidades de segurança são realizados durante o desenvolvimento de sistemas.

Proteção dos dados para teste: Os dados de teste são selecionados com cuidado, protegidos e controlados.

13. Relacionamento na Cadeia de Suprimento

Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores.

Política de segurança da informação no relacionamento com os fornecedores: Os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização são acordados com o fornecedor e documentados.

Identificando a segurança da informação nos acordos com fornecedores: Os requisitos de segurança da informação relevantes são estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização.

Cadeia de suprimento na tecnologia da comunicação e informação: Acordos com fornecedores incluem requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia das comunicações e informação.

Gerenciamento da entrega do serviço do fornecedor: Mantemos um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

Monitoramento e análise crítica de serviços com fornecedores: A Clicksign monitora, analisa criticamente e audita a intervalos regulares a entrega dos serviços executados pelos fornecedores.

14. Gestão de Incidentes de Segurança da Informação

Asseguramos 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: São estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

Notificação de eventos de segurança da informação: Os eventos de segurança da informação são relatados através do e-mail seguranca@clicksign.com, o mais rapidamente possível.

Notificando fragilidades de segurança da informação: Os colaboradores e partes externas que usam os sistemas e serviços de informação da Clicksign são instruídos a registrar e notificar quaisquer fragilidades de segurança da informação, suspeita ou observada, nos sistemas ou serviços.

Avaliação e decisão dos eventos de segurança da informação: Os eventos de segurança da informação são avaliados e decididos se eles são classificados como incidentes de segurança da informação.

Resposta aos incidentes de segurança da informação: Incidentes de segurança da informação serão reportados de acordo com procedimentos documentados.

Aprendendo com os incidentes de segurança da informação: Os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação são usados para reduzir a probabilidade ou o impacto de incidentes futuros.

Coleta de evidências: A Clicksign define e aplica procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.

Segurança contra ataques: A Clicksign utiliza medidas técnicas apropriadas para efetuar o endurecimento do sistema operacional, aplicar patches de segurança, utilizar sistemas de detecção de intrusos e fazer testes de penetração. Nosso ambiente de produção é programado para ser monitorado 24 horas por dia, 7 dias por semana, 365 dias por ano.

Uptime: a Clicksign mantém informações sobre disponibilidade, eventos e manutenção acessíveis em https://status.clicksign.com, com taxas historicamente observadas acima de 99,99%.

15. Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio

A continuidade da segurança da informação é considerada nos sistemas de gestão da continuidade do negócio da Clicksign.

Planejando a continuidade da segurança da informação: A Clicksign determina 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.

Implementando a continuidade da segurança da informação: A Clicksign estabelece, documenta, implementa e mantém processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa.

Verificação, análise crítica e avaliação da continuidade da segurança da informação: A Clicksign verifica os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.

Disponibilidade dos recursos de processamento da informação: Os recursos de processamento da informação são implementados com redundância suficiente para atender aos requisitos de disponibilidade, a intervalos regulares, bem como para garantir que são válidos e eficazes em situações adversas.

16. Análise Crítica da Segurança da Informação

Asseguramos que a segurança da informação está implantada e operada de acordo com as políticas e procedimentos da organização.

Análise crítica independente da segurança da informação: A Clicksign gerencia a segurança da informação e a sua implementação (por exemplo: controles, objetivo dos controles, políticas, processos e procedimentos para a segurança da informação), além de analisá-la criticamente, de forma independente, a intervalos planejados ou quando ocorrerem mudanças significativas.

Testes de penetração: De acordo com as melhores práticas, com o objetivo de avaliar a efetividade de medidas de segurança, a Clicksign contrata periodicamente terceiros para realizar testes de penetração em sistemas internos e externos.

Conformidade com as políticas e procedimentos de segurança da informação: Os gestores analisam criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.

Análise crítica da conformidade técnica: Os sistemas de informação são analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.

17. Histórico de Revisão

Versão	Descrição de alteração
1.0	Versão inicial
2.0	Atualização técnica

18. Aprovação

Este documento foi criado, revisado e aprovado pelos Colaboradores abaixo listados:

Versão	Elaborado por:	Data de Elaboração	Revisado por:	Aprovado por:	Data da Aprovação
1.0	Sérgio Santos	30/06/2022	Louyse Breia	Adriano Pereira	30/06/2022
2.0	Sérgio Santos	13/09/2022	Miriam Stefanello	Adriano Pereira	20/10/2022

Para maiores informações, ou dirimir dúvidas sobre Segurança da Informação, entre em contato com a Clicksign através do e-mail seguranca@clicksign.com.