Sistema de Gestão de Serviço - SGS

Política de Segurança da Informação

Versão 1.0

Autor: Escritório de Projetos e Processos da Amazon Informática
Data de Publicação: terça-feira, 12 de abril de 2022.
Última Atualização: terça-feira, 12 de abril de 2022.

Aprovações:

Jefferson Brasil de Araujo – CEO
Marcos Batista Silva – Diretor de Tecnologia
Estenes Luiz Santos – Diretor Administrativo
Márcio José Ferreira – Gerente de Projetos

Controle do Documento

Versão	Descrição	Data
1.0	Confecção do documento	12 de abril 2022

Documentação Relacionada

Versão	Descrição	Data
1.0	ABNT/NBR ISO/IEC 20000-1	12 de abril 2022
1.0	ABNT/NBR ISO/IEC 20000-2	12 de abril 2022
1.0	ABNT ISO/IEC TR 20000-5	12 de abril 2022

Índice

1. Propósito

A Amazon Informática reconhece a importância da Política de Segurança da Informação e está comprometida de forma responsável com o negócio e a conformidade com todos os requisitos legais e regulamentares em relação à Prestação de Serviços para as organizações a qual contrata nossos serviços.

2. Princípios e valores

Nesta política, a "segurança da informação" é definida como:

Preservar: Isso significa que a gestão, em tempo integral ou meio período, subcontratados, consultores de projetos e quaisquer partes externas têm, e serão informados de suas responsabilidades (que são definidas em suas descrições de trabalho ou contratos) para preservar a segurança da informação, relatar violações de segurança e agir de acordo com as exigências do SGS (Sistema de Gerenciamento de Serviços). As consequências das violações da política de segurança são descritas na política disciplinar. Todos receberão treinamento de conscientização sobre segurança da informação e mais especializados receberão treinamento especializado em segurança da informação.

Disponibilidade: Isso significa que as informações e os ativos associados devem ser acessíveis aos usuários autorizados quando necessário e, portanto, fisicamente seguros. A rede de computadores deve ser resiliente e deve ser capaz em detectar e responder rapidamente a incidentes (como vírus e outros malwares) que ameaçam a disponibilidade contínua de ativos, sistemas e informações. Deve haver planos adequados de continuidade de negócios.

Confidencialidade: Isso envolve garantir que as informações só são acessíveis àqueles autorizados a acessá-la e, portanto, evitar acesso deliberado e acidental não autorizado às informações e conhecimentos proprietários e seus sistemas incluindo suas redes(s), sites(s), extranet(s) e sistemas de comércio eletrônico.

Integridade: Isso envolve a salvaguarda da exatidão e completude dos métodos de informação e processamento e, portanto, requer a prevenção de modificações deliberadas ou acidentais, parciais ou completas, de ativos físicos ou eletrônicos. Deve haver contingência apropriada inclusive para sistemas de rede, sistema de comércio eletrônico(s), sites(s), extranet(s) e planos de backup de dados e relatórios de incidentes de segurança. devem cumprir todas as legislações relevantes relacionadas aos dados nas jurisdições em que opera.

3. Objetivos

A Amazon Informática está comprometida em preservar a confidencialidade, integridade e disponibilidade de todos os ativos de informação física e eletrônica ao longo de seus, a fim de preservar sua vantagem competitiva, fluxo de caixa, rentabilidade, legal, regulatória e contratual e de imagem comercial.

Os requisitos de segurança de informações e informações continuarão alinhados com as metas do Sistema de Gerenciamento de Serviços (SGS) e para permitir o mecanismo de compartilhamento de informações, operações eletrônicas, além de reduzir riscos relacionados a informações a níveis aceitáveis.

4. Política

São ativos de informação dados e outras informações de propriedade, usadas, armazenadas, processadas ou transmitidas pela Amazon Informática ou por seus fornecedores, parceiros comerciais ou outros terceiros que atuam em nome da Amazon Informática (coletivamente "Fornecedores"), bem como os sistemas e aplicativos utilizados pela empresa para criar, processar, modificar, armazenar e comunicar tais informações.

A Amazon Informática cumprirá qualquer lei, regulamento ou política corporativa aplicável sobre a confidencialidade, integridade e disponibilidade.

A Amazon Informática também protegerá a confidencialidade, integridade e disponibilidade de ativos de informação da empresa proporcionais à sensibilidade e importância desses Ativos para a organização e seus clientes, o risco de uso indevido ou comprometimento desses Ativos e as potenciais consequências legais, regulatórias e comerciais, bem como considerações aplicáveis de segurança nacional.

A Amazon Informática reserva-se o direito de inspecionar, registrar e monitorar os Ativos de Informação organização, incluindo o uso, o acesso e a divulgação do mesmo, conforme permitido pela lei aplicável.

Para atender a esses requisitos e objetivos, esta Política exige a organização desenvolva, mantenha e revise periodicamente instruções, normas, procedimentos e diretrizes, para implementar a confidencialidade, integridade e disponibilidade adequadas dos Ativos de Informação e usar essas instruções, normas, procedimentos e diretrizes no curso ordinário dos negócios, tudo sob a direção e orientação da Alta Gestão.

Os ativos físicos de incluir, mas não se limitando a, hardware de computador, cabeamento de dados, sistemas telefônicos, sistemas de arquivamento e arquivos de dados físicos.

Uma VIOLAÇÃO DE SEGURANÇA é qualquer incidente ou atividade que cause, ou possa causar, uma quebra na disponibilidade, confidencialidade ou integridade dos ativos de informações físicas ou eletrônicas de Nome da organização.

Confidencialidade, integridade e disponibilidade apropriadas incluem, mas não se limita a, o seguinte:

- A adesão ao princípio do "menos privilégio", na maior medida prática, de tal forma que os direitos de acesso ou alteração de informações, e os direitos de exercer funções sensíveis ou críticas, são fornecidos apenas para satisfazer necessidades legítimas dos negócios.
- A inclusão de disposições para proteger os ativos de informação da organização condizente com esta Política em contratos com fornecedores.
- Uso de controles de segurança apropriados (por exemplo, físicos, eletrônicos ou processuais) para proteger os ativos de informação da Organização.
- Treinamento para o pessoal da Organização em medidas, processos e ferramentas para proteger os ativos de informação da Organização.
- Implementação de técnicas apropriadas (por exemplo, criptografia, marcação, mascaramento) para manter a confidencialidade e integridade dos dados quando armazenados, ou quando trocados entre sistemas ou em trânsito através de redes.
- Implementação e testes regulares de planos de continuidade de negócios e recuperação de desastres que incluem backup de informações, estratégias de recuperação e métodos alternativos de acesso e distribuição de informações.
- Integração da avaliação e análise de riscos, conscientização de segurança e engenharia de segurança como parte do desenvolvimento do ciclo de vida dos serviços.
- Auditorias periódicas e revisões de segurança para avaliar o cumprimento desta Política, incluindo suas instruções, procedimentos e normas de suporte.
- Um recurso de detecção e resposta de incidentes de segurança eficaz e regularmente testado.
- Trilhas de controle de acesso e auditoria para limitar o acesso, direitos de uso e outros privilégios para ativos de informação da Organização para os propósitos pretendidos.

A Amazon Informática atua com um plano estratégico de negócios e um quadro de gestão de riscos que fornece o contexto para identificar, avaliar, analisar e controlar riscos relacionados à informação através do estabelecimento e manutenção de um Sistema de Gerenciamento de Serviços (SGS).

O plano de avaliação de risco e tratamento de risco identificam riscos relacionados às informações e são controlados pelo responsável pela gestão e manutenção do plano de tratamento de risco.

Avaliações adicionais de risco podem, quando necessário, ser realizadas para determinar controles adequados para riscos específicos.

Em particular, planos de continuidade de negócios e contingência, procedimentos de backup de dados, prevenção de vírus e hackers, controle de acesso a sistemas e relatórios de incidentes de segurança da informação são fundamentais para essa política.

Os objetivos de controle para cada uma dessas áreas estão contidos por políticas e procedimentos documentados específicos.

Espera-se que os funcionários da Amazon Informática todas as partes externas identificadas no Sistema de Gerenciamento de Serviço cumpram essa política.

Todos, e certas partes externas incluindo os funcionários da Amazon Informática, receberão treinamento adequado.

O Sistema de Gerenciamento de Serviços (SGS) está sujeito a revisão e aperfeiçoamento contínuos e sistemáticos.

A Amazon Informática estabeleceu um grupo de gestão de alto nível, intitulado como Comitê Gestor de TI, presidido pelo Diretor Executivo (CEO) e incluindo o Gerente Responsável pela Segurança da Informação e outros Executivos / Especialista para apoiar o quadro e revisar periodicamente a política de segurança.

Esta política será revisada para responder a quaisquer mudanças no plano de avaliação de risco ou tratamento de risco e, pelo menos anualmente.

5. Aplicabilidade

Esta Política abrange a Amazon Informática, incluindo todos os funcionários, fornecedores e contratados quando estão envolvidos no fornecimento de serviços no âmbito do SGS.

O cumprimento da Política de Gestão de Serviços é obrigatório.

Todos os gestores são diretamente responsáveis pela implementação dessa política e pela garantia do cumprimento dos colegas dentro de suas funções.

Todos os funcionários da Organização são responsáveis pelo cumprimento desta Política. As violações desta Política devem ser relatadas imediatamente à Segurança Corporativa da Organização.

Os funcionários que contratam ou supervisionam o trabalho realizado pelos Fornecedores são responsáveis por comunicar os requisitos desta Política a esses Fornecedores e por supervisionar a conformidade dos Fornecedores.

6. Revisão

A política é revisada anualmente e/ou quando ocorrem mudanças significativas.

7. Proprietário de documentos e aprovação

O proprietário deste documento é responsável por garantir que este procedimento seja revisto.

Uma versão atual deste documento está disponível para todos os membros da equipe na intranet corporativa e publicada no endereço: http://aizon-doc/aizon/#/repository/home

Esse processo foi aprovado pela Diretoria Executiva da Amazon Informática e é emitido em uma base controlada por versão sob sua assinatura.