POLÍTICA DE SEGURANÇA DA INFORMAÇÃOE CYBER SECURITY

1. Introdução

A Goon Data Assessoria de Crédito Ltda. ("GOON DATA"), distribuidora autorizada dos produtos da Quod, valoriza a segurança da informação e a proteção de dados pessoais. Em conformidade com a Lei nº 13.709, de 14 de agosto de 2019 - Lei Geral de Proteção de Dados Pessoais ("LGPD"), esta Política de Segurança da Informação estabelece diretrizes para garantir a integridade, confidencialidade e disponibilidade das informações e dos dados pessoais tratados pela empresa.

2. Objetivo

O objetivo desta Política é definir os princípios e as práticas de segurança da informação e cyber security a serem adotados pela GOON DATA para proteger seus ativos de informação contra ameaças internas e externas, assegurando o cumprimento da LGPD e demais legislações aplicáveis.

3. Âmbito de Aplicação

A Política de Segurança da Informação e Cyber Security da GOON DATA é um documento fundamental que estabelece diretrizes e controles para proteger os ativos de informação da organização. Esta política tem como objetivo garantir a confidencialidade, integridade e disponibilidade das informações, além de mitigar riscos relacionados a ameaças cibernéticas. O âmbito de aplicação desta política é abrangente e inclui todos os indivíduos e entidades que, de alguma forma, interagem com as informações da GOON DATA.

Especificamente, esta política se aplica aos seguintes grupos:

- Colaboradores: Todos os funcionários da GOON DATA, independentemente de sua posição, função ou nível hierárquico.
- Terceiros: Profissionais ou empresas contratadas para fornecer serviços temporários ou especializados, que necessitam acessar os sistemas ou dados da GOON DATA.
- Prestadores de Serviços: Empresas ou indivíduos que fornecem serviços contínuos ou de suporte à GOON DATA, implicando acesso a informações corporativas.
- Parceiros: Organizações ou indivíduos que colaboram com a GOON DATA em projetos, negócios ou outras atividades que envolvam o compartilhamento de informações.

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

- Quaisquer Outras Partes: Entidades ou indivíduos que, não se enquadrando nas categorias acima, necessitam de acesso às informações da GOON DATA para cumprir responsabilidades contratuais, regulamentares ou operacionais.

Em resumo, a Política de Segurança da Informação e Cyber Security da GOON DATA aplica-se a todos os que interagem com os ativos de informação da organização. Esta abordagem abrangente assegura que todas as partes estejam cientes de suas responsabilidades e do compromisso da GOON DATA com a proteção das informações, promovendo um ambiente seguro e confiável para todos.

4. Definições

O tópico "Definições" tem como objetivo esclarecer e padronizar o entendimento dos termos e conceitos utilizados ao longo desta política. A correta compreensão desses termos é essencial para a aplicação efetiva das diretrizes e medidas de segurança estabelecidas. Para os fins desta Política de Segurança da Informação e Cyber Security da GOON DATA, consideram-se as seguintes definições:

- Segurança da Informação: Conjunto de ações voltadas para proteger a informação contra acessos não autorizados, alterações indevidas e indisponibilidade. A segurança da informação abrange práticas e políticas que visam garantir que os dados da organização sejam acessíveis apenas por pessoas autorizadas, que permaneçam inalterados salvo por indivíduos ou processos autorizados e que estejam disponíveis quando necessários. Exemplos incluem criptografia de dados, controles de acesso e backups regulares.

- Cyber Security: Medidas e controles para proteger sistemas, redes e programas contra ataques cibernéticos. Cyber Security foca na proteção de infraestruturas tecnológicas contra ameaças como malware, phishing, ataques de negação de serviço (DDoS), e invasões de rede. Exemplos de medidas incluem firewalls, sistemas de detecção de intrusões (IDS), e práticas de desenvolvimento seguro de software.

- Dados Pessoais: Informações relacionadas a pessoa natural identificada ou identificável. Dados pessoais são aqueles que podem identificar diretamente uma pessoa, como nome, endereço, número de telefone, ou que podem tornar alguém identificável quando combinados com outras informações, como data de

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

nascimento ou localização. Esses dados devem ser tratados com cuidado para proteger a privacidade dos indivíduos.

- Dados Sensíveis: Dados pessoais 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. Dados sensíveis requerem um nível mais alto de proteção devido à sua natureza delicada e ao potencial de causar discriminação ou danos aos indivíduos. Exemplos incluem informações médicas, dados biométricos como impressões digitais, ou afiliações religiosas e políticas.

- Controlador: Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais. O controlador é responsável por definir como e por que os dados pessoais serão processados. Na GOON DATA, o controlador pode ser a própria organização ou um indivíduo dentro dela que tem autoridade sobre as políticas de tratamento de dados, como o Diretor de Privacidade ou o Departamento de TI.

- Operador: Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador. O operador é a entidade ou pessoa que efetivamente manipula os dados pessoais conforme as instruções do controlador. Isso pode incluir funcionários da GOON DATA, prestadores de serviços terceirizados que processam dados em nome da organização, ou empresas de hospedagem de dados.

Com essas definições claras, todos os envolvidos na GOON DATA podem entender melhor suas responsabilidades e a importância da proteção da informação, contribuindo para um ambiente de trabalho seguro e em conformidade com as normas de segurança da informação e cyber security.

5. Princípios da Segurança da Informação

Os princípios da segurança da informação são fundamentos essenciais que orientam as práticas e políticas para proteger os dados da organização contra ameaças e garantir a confiabilidade das informações. Esses princípios são aplicados de forma a proteger os ativos de informação da GOON DATA, promovendo um ambiente seguro e em conformidade com regulamentações. A GOON DATA adota os seguintes princípios para a segurança da informação:

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

- Confidencialidade: Garantir que a informação seja acessível somente a pessoas autorizadas. A confidencialidade visa proteger os dados contra acessos não autorizados, garantindo que apenas indivíduos com permissões específicas possam visualizar ou manipular informações sensíveis. Isso envolve o uso de medidas como controle de acesso, criptografia, e políticas de privacidade.

- Integridade: Assegurar que a informação seja mantida em seu estado original, sem alterações indevidas. A integridade garante que os dados não sejam alterados de maneira imprópria, seja intencionalmente ou acidentalmente. Isso inclui a implementação de mecanismos que detectem e impeçam alterações não autorizadas.

- Disponibilidade: Garantir que a informação esteja disponível para uso sempre que necessário. A disponibilidade assegura que os sistemas de informação e dados estejam acessíveis quando forem necessários, prevenindo interrupções que possam impactar a operação da organização.

- Autenticidade: Verificar a identidade dos usuários que acessam as informações. A autenticidade garante que a identidade dos usuários e dispositivos que acessam os sistemas e dados seja verificada, prevenindo fraudes e acessos não autorizados.

- Legalidade: Cumprir todas as legislações e regulamentações aplicáveis à segurança da informação e proteção de dados. A legalidade implica que todas as ações e políticas relacionadas à segurança da informação estão em conformidade com as leis e regulamentos aplicáveis. Isso envolve entender e implementar requisitos legais para proteção de dados pessoais e sensíveis, além de garantir que práticas de segurança sejam auditáveis.

Ao adotar e implementar esses princípios, a GOON DATA fortalece sua postura de segurança, protegendo suas informações críticas e assegurando a confiança de seus clientes, parceiros e colaboradores.

6. Responsabilidades

O tópico "Responsabilidades" descreve as funções e deveres de todos os indivíduos e grupos dentro da organização com relação à segurança da informação. É essencial que cada pessoa compreenda e cumpra suas responsabilidades para garantir a proteção adequada dos dados e a efetividade das políticas de segurança. Todos os colaboradores e terceiros que tenham

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

acesso às informações da GOON DATA são responsáveis por seguir esta Política de Segurança da Informação e Cyber Security e garantir a proteção dos dados. As responsabilidades específicas são detalhadas a seguir:

- Alta Administração: Aprovar e apoiar a implementação da Política de Segurança da Informação. A Alta Administração tem um papel crucial na definição do tom e da cultura de segurança da informação dentro da organização. Eles devem garantir que a política seja formalmente aprovada, alocar os recursos necessários para sua implementação e manutenção, e demonstrar um compromisso visível com as práticas de segurança.

- Gestores de Áreas: Garantir que suas equipes cumpram as diretrizes estabelecidas nesta Política. Os gestores de áreas têm a responsabilidade de assegurar que todos os membros de suas equipes estejam cientes das políticas de segurança da informação e que sigam as práticas recomendadas. Eles devem promover uma cultura de segurança dentro de suas áreas e monitorar o cumprimento das políticas.

- Equipe de TI e Segurança da Informação: Implementação, monitoramento e manutenção das medidas de segurança da informação e cyber security. A equipe de TI e Segurança da Informação é responsável por desenvolver e aplicar as soluções técnicas que protegem os ativos de informação. Eles monitoram a rede e os sistemas em busca de ameaças, realizam testes de segurança e garantem que as políticas sejam atualizadas conforme necessário.

- Colaboradores e Terceiros: Seguir as práticas de segurança da informação e relatar qualquer incidente ou suspeita de violação de segurança. Todos os colaboradores e terceiros que têm acesso às informações da Goon Data devem aderir às políticas e práticas de segurança estabelecidas. Eles também têm a responsabilidade de estar vigilantes e reportar quaisquer incidentes de segurança ou comportamentos suspeitos que possam comprometer os dados.

A segurança da informação é uma responsabilidade compartilhada que requer o comprometimento de todos os níveis da organização. A Alta Administração deve liderar com o exemplo, fornecendo apoio e recursos; os Gestores de Áreas devem garantir o cumprimento das políticas dentro de suas equipes; a Equipe de TI e Segurança da Informação deve implementar e manter as defesas técnicas; e todos os Colaboradores e Terceiros devem aderir

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

às práticas de segurança e estar vigilantes contra ameaças. Ao seguir essas responsabilidades, a GOON DATA pode proteger melhor seus ativos de informação e manter a confiança de seus clientes, parceiros e colaboradores.

7. Diretrizes de Segurança da Informação

As diretrizes de segurança da informação são um conjunto de instruções detalhadas e orientações práticas destinadas a proteger os ativos de informação da organização contra ameaças e vulnerabilidades. Estas diretrizes proporcionam um quadro operacional que ajuda a garantir que todos os aspectos da segurança da informação sejam geridos de maneira consistente e eficaz. Elas abrangem práticas, processos e tecnologias necessárias para proteger os dados contra acessos não autorizados, alterações indevidas e indisponibilidade, além de garantir a conformidade com regulamentações e normas aplicáveis. A GOON DATA adota as seguintes diretrizes de segurança da informação:

7.1 Classificação da Informação

A classificação da informação é um processo essencial para a gestão eficaz dos dados dentro da organização. Ela envolve a categorização das informações de acordo com seu nível de sensibilidade e criticidade, estabelecendo os critérios para seu manuseio, armazenamento e compartilhamento. Este processo garante que as informações recebam o nível adequado de proteção, alinhado com seu valor e sensibilidade, minimizando riscos de acesso não autorizado e perda de dados. As informações da GOON DATA são classificadas nas seguintes categorias:

- Pública: Informações que podem ser divulgadas sem restrições e cujo acesso não prejudica a organização ou seus stakeholders. Exemplos: Materiais de marketing, comunicados de imprensa, informações publicadas no site corporativo. Não requerem controles especiais de acesso ou proteção. No entanto, deve-se garantir a precisão e a integridade dos dados públicos.

- Interna: Informações de uso interno da GOON DATA, destinadas aos colaboradores e partes interessadas dentro da organização. Exemplos: Políticas internas, diretórios de colaboradores, comunicações internas. Acesso restrito aos colaboradores e partes autorizadas. Devem ser protegidas contra acesso externo não autorizado, usando medidas como autenticação básica e firewalls.

- Confidencial: Informações que requerem proteção contra divulgação não autorizada devido ao potencial impacto negativo para a organização se expostas.

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

Exemplos: Planos de negócios, dados financeiros internos, informações de clientes e parceiros. Acesso restrito aos colaboradores que precisam das informações para suas funções. Devem ser armazenadas em sistemas seguros, com criptografia de dados em repouso e em trânsito, além de controles de acesso rigorosos.

- Restrita: Informações altamente sensíveis que, se divulgadas, poderiam causar danos significativos à organização, seus clientes ou parceiros. Exemplos: Segredos comerciais, informações de saúde sensíveis, dados pessoais altamente confidenciais. Acesso estritamente limitado a indivíduos autorizados. Requer o mais alto nível de proteção, incluindo criptografia robusta, autenticação multifator, e monitoramento contínuo de acessos e atividades.

A classificação da informação é um componente vital da Política de Segurança da Informação e Cyber Security da GOON DATA. Ao categorizar as informações de acordo com seu nível de sensibilidade e criticidade, a organização pode implementar medidas de proteção apropriadas, garantindo que os dados estejam seguros e acessíveis apenas a indivíduos autorizados. Este processo não só protege os ativos de informação da organização, mas também reforça a confiança de clientes, parceiros e colaboradores na capacidade da GOON DATA de gerenciar e proteger suas informações de maneira eficaz e segura.

7.2 Controle de Acesso

O controle de acesso é um princípio fundamental da segurança da informação, assegurando que apenas indivíduos autorizados possam acessar dados e sistemas. Este processo é baseado no princípio da "necessidade de conhecimento" (need-to-know), que garante que os usuários só tenham acesso às informações necessárias para desempenhar suas funções. Implementar controles de acesso eficazes minimiza o risco de acesso não autorizado e protege os ativos de informação da organização. A GOON DATA assegura que o controle de acesso seja rigorosamente aplicado através das seguintes diretrizes:

- Acesso Concedido Apenas a Indivíduos Autorizados: Somente indivíduos que tenham uma necessidade legítima e autorizada de acessar determinadas informações poderão fazê-lo.

- Gestão e Proteção de Credenciais de Acesso: As credenciais de acesso (como senhas, tokens e cartões de acesso) devem ser gerenciadas e protegidas contra comprometimentos.

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

- Revogação Imediata de Acesso: O acesso deve ser imediatamente revogado em caso de desligamento do colaborador ou mudança de função que elimine a necessidade de acesso às informações previamente autorizadas.

O controle de acesso é vital para proteger os ativos de informação da GOON DATA. Ao garantir que apenas indivíduos autorizados tenham acesso às informações necessárias para suas funções e ao gerenciar e proteger as credenciais de acesso de forma rigorosa, a GOON DATA minimiza os riscos de acesso não autorizado e mantém a integridade e a confidencialidade de seus dados. A revogação imediata de acessos em caso de desligamento ou mudança de função é igualmente crucial para prevenir acessos indevidos e proteger as informações da organização.

7.3 Segurança Física e Ambiental

A segurança física e ambiental é crucial para a proteção das instalações e dos ativos de informação da GOON DATA. As medidas de segurança física garantem que os dados e os sistemas sejam protegidos contra acesso não autorizado, danos e interrupções causadas por ameaças físicas. A GOON DATA implementa uma série de medidas rigorosas para assegurar a integridade, a confidencialidade e a disponibilidade das informações, bem como a continuidade das operações em caso de incidentes.

Para proteger as instalações e os ativos de informação, a GOON DATA adota as seguintes medidas de segurança física e ambiental:

- Controle de Acesso Físico a Áreas Sensíveis: Implementação de sistemas de controle de acesso físico que restringem a entrada a áreas sensíveis e críticas, garantindo que somente pessoas autorizadas possam acessá-las.

- Monitoramento por Câmeras de Segurança: Instalação de câmeras de vigilância para monitorar e registrar atividades em áreas sensíveis e de acesso restrito, garantindo a capacidade de detectar e responder a incidentes de segurança.

- Sistema de Alarme e Detecção de Intrusão: Implementação de sistemas de alarme e detecção de intrusão para alertar sobre tentativas de acesso não autorizado e outras atividades suspeitas.

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

- Medidas de Proteção contra Desastres Naturais e Incêndios: Implementação de medidas para proteger as instalações e os ativos de informação contra desastres naturais e incêndios, garantindo a continuidade das operações.

As medidas de segurança física e ambiental são fundamentais para a proteção dos ativos de informação da GOON DATA. Implementando controles rigorosos de acesso físico, monitoramento por câmeras, sistemas de alarme e detecção de intrusão, e medidas de proteção contra desastres naturais e incêndios, a GOON DATA garante um ambiente seguro e protegido. Esses esforços não só protegem a integridade e a confidencialidade dos dados, mas também asseguram a continuidade das operações da empresa em caso de incidentes físicos ou ambientais.

7.4 Gestão de Riscos

A gestão de riscos é uma componente essencial da segurança da informação e cibersegurança na GOON DATA. O objetivo da gestão de riscos é identificar, avaliar e mitigar os riscos potenciais que podem comprometer a confidencialidade, integridade e disponibilidade das informações da organização. Um processo de gestão de riscos robusto permite antecipar ameaças e tomar medidas proativas para minimizar os impactos adversos, garantindo a segurança e a resiliência dos ativos de informação da empresa.

Para assegurar uma gestão eficaz dos riscos de segurança da informação, a GOON DATA adota as seguintes práticas:

- Avaliações de Riscos Periódicas: Realização de avaliações regulares para identificar e analisar os riscos de segurança da informação que a organização pode enfrentar.

- Desenvolvimento de Planos de Mitigação para Riscos Identificados: Criação e implementação de planos detalhados para mitigar os riscos identificados nas avaliações de risco.

- Monitoramento Contínuo da Eficácia das Medidas de Mitigação: Monitoramento constante das medidas de mitigação implementadas para garantir sua eficácia contínua e ajuste conforme necessário.

A gestão de riscos é um componente vital da Política de Segurança da Informação e Cyber Security da GOON DATA. Ao identificar, avaliar e mitigar riscos potenciais de maneira sistemática e contínua, garantimos a proteção de nossos ativos de informação e a

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

continuidade dos negócios. Através de avaliações de risco periódicas, desenvolvimento de planos de mitigação e monitoramento contínuo da eficácia das medidas de segurança, a GOON DATA está comprometida em manter um ambiente seguro e resiliente contra ameaças.

7.5 Gestão de Incidentes de Segurança

A Gestão de Incidentes de Segurança é uma parte essencial da abordagem da GOON DATA para proteger seus ativos de informação contra ameaças cibernéticas e outros incidentes de segurança. Estabelecemos processos robustos para detectar, responder e recuperar de incidentes, visando minimizar o impacto negativo e garantir a continuidade das operações. Nossa abordagem proativa e sistemática permite uma resposta rápida e eficaz a incidentes, mitigando danos potenciais e protegendo a integridade, confidencialidade e disponibilidade dos dados da empresa.

Para assegurar uma gestão eficaz de incidentes de segurança, a GOON DATA adota as seguintes práticas:

- Identificação e Reporte Prontos de Incidentes: Estabelecemos procedimentos para identificar e reportar prontamente qualquer incidente de segurança, independentemente de sua natureza ou gravidade.

- Plano de Respostas a Incidentes Documentado e Testado: Desenvolvimento e documentação de um plano de resposta a incidentes que detalha os procedimentos a serem seguidos em caso de incidentes de segurança.

- Análises Pós-Incidente para Evitar Recorrências: Realização de análises detalhadas de todos os incidentes de segurança para identificar suas causas raiz e implementar medidas preventivas para evitar recorrências.

A gestão de incidentes de segurança desempenha um papel crucial na proteção dos ativos de informação da GOON DATA contra ameaças cibernéticas e outros incidentes de segurança. Ao estabelecer processos para detectar, responder e recuperar de incidentes, garantimos uma resposta rápida e eficaz a qualquer violação de segurança, minimizando o impacto nos negócios e protegendo a confidencialidade, integridade e disponibilidade dos dados da empresa. Através de uma abordagem proativa e uma cultura de melhoria contínua, a GOON DATA está comprometida em manter um ambiente seguro e protegido contra ameaças cibernéticas.

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

7.6 Treinamento e Conscientização

Na GOON DATA, reconhecemos que a conscientização e o treinamento contínuo são fundamentais para fortalecer a segurança da informação e proteger os ativos da empresa contra ameaças cibernéticas. Por isso, promovemos iniciativas abrangentes para educar e capacitar nossos colaboradores, garantindo que todos estejam bem informados e preparados para enfrentar os desafios da segurança cibernética.

- Programas de Treinamentos Regulares: Realizamos programas de treinamento regulares para todos os colaboradores, abordando políticas e práticas de segurança da informação.

- Campanhas de Conscientização: Conduzimos campanhas de conscientização regulares para sensibilizar os colaboradores sobre ameaças cibernéticas, como phishing, engenharia social e outras táticas utilizadas por hackers.

- Avaliações de Conhecimentos e Simulações de Segurança: Conduzimos avaliações de conhecimento e simulações de segurança para avaliar o entendimento dos colaboradores sobre práticas de segurança da informação e sua capacidade de responder a incidentes.

A conscientização e o treinamento contínuo são elementos essenciais da Política de Segurança da Informação e Cyber Security da GOON DATA. Ao educar e capacitar nossos colaboradores, fortalecemos a postura de segurança da organização e reduzimos o risco de incidentes cibernéticos. Através de programas de treinamento regulares, campanhas de conscientização e avaliações de conhecimento, estamos comprometidos em manter uma cultura de segurança robusta e preparada para enfrentar os desafios de segurança da informação em constante evolução.

8. Cyber Security

Cyber Security, ou segurança cibernética, refere-se ao conjunto de práticas, tecnologias e processos projetados para proteger sistemas de computador, redes, dispositivos e dados contra ataques cibernéticos, roubo de dados e outras ameaças digitais. Em um mundo cada vez mais interconectado e dependente da tecnologia, a segurança cibernética desempenha um papel crucial na proteção da confidencialidade, integridade e disponibilidade das informações digitais.

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

8.1 Proteção de Redes e Sistema

Na GOON DATA, reconhecemos a importância crítica de proteger nossas redes e sistemas contra ameaças cibernéticas em constante evolução. Implementamos medidas proativas para garantir a segurança e integridade de nossa infraestrutura digital, minimizando os riscos de violações de segurança e mantendo a confidencialidade, integridade e disponibilidade dos dados da empresa.

Medidas Implementadas:

- Firewalls, Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS): Utilizamos firewalls e sistemas de IDS/IPS para monitorar e filtrar o tráfego de rede, identificando e bloqueando atividades suspeitas ou maliciosas. Essas medidas ajudam a proteger nossas redes contra ataques de malware, tentativas de acesso não autorizado e outras ameaças cibernéticas.

- Segmentação de Redes: Implementamos a segmentação de redes para isolar sistemas críticos e sensíveis, reduzindo a superfície de ataque e limitando o impacto de possíveis violações de segurança. Isso garante que, mesmo que uma parte da rede seja comprometida, o acesso a outros sistemas seja restrito.

- Atualização e Patching Regular: Realizamos atualizações e patching regular de sistemas operacionais, aplicativos e firmware para corrigir vulnerabilidades conhecidas e garantir que nossos sistemas estejam protegidos contra exploits e ataques baseados em falhas de segurança conhecidas.

Na GOON DATA, estamos comprometidos com a manutenção de práticas de segurança cibernética de alto nível para proteger nossos ativos digitais e garantir a confiança de nossos clientes e parceiros. Continuaremos a avaliar e fortalecer nossas medidas de proteção de redes e sistemas, mantendo-nos atualizados com as últimas ameaças e tendências em segurança da informação.

8.2 Gerenciamento de Vulnerabilidade

Na GOON DATA, reconhecemos a importância crítica do gerenciamento de vulnerabilidades para garantir a segurança e integridade de nossos sistemas e dados contra ameaças cibernéticas. Adotamos práticas proativas para identificar e corrigir fraquezas em nossa infraestrutura digital, garantindo que estejamos preparados para enfrentar os desafios do cenário de segurança da informação em constante evolução.

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

Medidas Implementadas:

- Varreduras Regulares de Vulnerabilidades: Realizamos varreduras regulares de vulnerabilidades em nossa infraestrutura de TI para identificar possíveis falhas de segurança, pontos de entrada não autorizados e outras vulnerabilidades que possam ser exploradas por atacantes. Essas varreduras nos permitem avaliar proativamente o estado de segurança de nossos sistemas e priorizar a correção de vulnerabilidades críticas.

- Testes de Penetração Periódicos: Conduzimos testes de penetração periódicos, também conhecidos como testes de ethical hacking, para avaliar a eficácia de nossas defesas de segurança e identificar possíveis pontos fracos em nossa infraestrutura. Esses testes simulam ataques cibernéticos reais e nos fornecem insights valiosos sobre como melhorar nossa postura de segurança e proteger nossos ativos digitais.

- Correção de Vulnerabilidades em Tempo Hábil: Agimos prontamente para corrigir as vulnerabilidades identificadas durante varreduras de vulnerabilidades e testes de penetração. Priorizamos a correção de vulnerabilidades críticas e de alto risco, garantindo que estejamos protegidos contra possíveis explorações antes que elas possam ser aproveitadas por atacantes.

O gerenciamento de vulnerabilidades é uma parte essencial de nossa Política de Segurança da Informação e Cyber Security na GOON DATA. Ao adotar práticas como varreduras regulares de vulnerabilidades, testes de penetração periódicos e correção oportuna de vulnerabilidades, estamos fortalecendo nossa postura de segurança e garantindo a proteção de nossos sistemas e dados contra ameaças cibernéticas. Com um compromisso contínuo com a segurança da informação, estamos preparados para enfrentar os desafios em constante evolução do cenário de ameaças cibernéticas.

8.3 Gestão de Identidade e Acesso

Na GOON DATA, reconhecemos que a gestão eficaz de identidade e acesso é essencial para proteger nossos sistemas e dados contra acesso não autorizado e garantir a segurança da informação. Implementamos soluções para garantir que apenas usuários autorizados tenham acesso aos recursos e informações necessárias para realizar suas funções, enquanto protegemos contra ameaças internas e externas.

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

Práticas Implementadas:

- Verificação de Identidades: Antes de conceder acesso a sistemas e dados, todas as identidades são rigorosamente verificadas para garantir que os usuários sejam quem dizem ser. Isso é alcançado por meio de processos de autenticação robustos, como senhas fortes, biometria e certificados digitais.

- Princípio do Privilégio Mínimo: Praticamos o princípio do privilégio mínimo, garantindo que os usuários tenham acesso apenas às informações e recursos necessários para realizar suas funções. Isso limita o potencial de danos causados por usuários mal-intencionados ou comprometidos.

A gestão de identidade e acesso desempenha um papel fundamental em nossa Política de Segurança da Informação e Cyber Security na GOON DATA. Ao implementar soluções e seguir práticas como verificação de identidades e princípio do privilégio mínimo estamos protegendo nossos sistemas e dados contra ameaças cibernéticas e garantindo a integridade e segurança de nossas operações. Com um compromisso contínuo com a segurança da informação, estamos preparados para enfrentar os desafios em constante evolução do cenário de ameaças digitais.

9. Conformidade com a LGPD

Na GOON DATA, reconhecemos a importância crítica de estar em conformidade com a Lei Geral de Proteção de Dados (LGPD) para garantir a privacidade e a proteção dos dados pessoais de nossos clientes, colaboradores e parceiros. Nossa política de segurança da informação e cyber security é projetada e implementada com base nos princípios e requisitos estabelecidos pela LGPD, assegurando que tratemos os dados pessoais com o mais alto nível de responsabilidade e conformidade legal.

Práticas Implementadas:

- Tratamento de Dados Pessoais: Garantimos que o tratamento de dados pessoais seja realizado com base em bases legais previstas na LGPD, como o consentimento do titular, o cumprimento de obrigações legais e contratuais, e a execução de políticas públicas.

- Proteção dos Direitos dos Titulares de Dados: Respeitamos e protegemos os direitos dos titulares de dados, incluindo o direito à privacidade, à transparência,

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

à informação, ao acesso, à correção, à exclusão e à portabilidade de seus dados pessoais. Garantimos que os titulares de dados possam exercer esses direitos de forma fácil e eficaz.

- Implementação de Medidas Técnicas e Organizacionais: Implementamos medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra acessos não autorizados, alterações indevidas, divulgação ou destruição acidental ou ilícita. Isso inclui a criptografia de dados, o controle de acesso, a anonimização, a pseudonimização, a avaliação de impacto à proteção de dados, entre outras medidas de segurança.

A conformidade com a LGPD é uma prioridade fundamental em nossa Política de Segurança da Informação e Cyber Security na GOON DATA. Ao garantir o tratamento adequado dos dados pessoais, a proteção dos direitos dos titulares de dados e a implementação de medidas técnicas e organizacionais para proteger os dados pessoais, estamos fortalecendo nossa postura de segurança e garantindo a privacidade e a integridade dos dados de nossos clientes e parceiros. Com um compromisso contínuo com a conformidade legal e a proteção de dados, estamos preparados para enfrentar os desafios em constante evolução do cenário de privacidade e segurança da informação.

10. Auditoria e Revisão

Na GOON DATA, reconhecemos a importância de realizar auditorias periódicas para avaliar a conformidade com nossa Política de Segurança da Informação e Cyber Security e garantir a eficácia das medidas de segurança implementadas. Nossa abordagem de auditoria e revisão é projetada para garantir que nossos sistemas e processos estejam alinhados com os mais altos padrões de segurança da informação e cibernética, garantindo a proteção de nossos ativos digitais e a confiança de nossos clientes e parceiros.

Práticas Implementadas:

- Auditorias Internas e Externas**:** Conduzimos auditorias internas e externas regularmente para avaliar a conformidade com nossa Política de Segurança da Informação e Cyber Security. As auditorias internas são realizadas por nossa equipe de segurança da informação, enquanto as auditorias externas podem ser conduzidas por auditores independentes ou agências reguladoras.

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

- Análise dos Resultados e Ações Corretivas: Os resultados das auditorias são cuidadosamente analisados para identificar quaisquer áreas de não conformidade ou oportunidades de melhoria. Quando são identificadas deficiências, são desenvolvidos planos de ação corretiva para abordar as questões identificadas e fortalecer nossos controles de segurança.

- Revisão e Atualização da Política: A Política de Segurança da Informação e Cyber Security é revisada e atualizada conforme necessário, com base nos resultados das auditorias, mudanças no cenário de ameaças cibernéticas e requisitos regulatórios. Essas revisões garantem que nossa política permaneça relevante e eficaz na proteção de nossos ativos digitais.

A auditoria e revisão são pilares essenciais de nossa Política de Segurança da Informação e Cyber Security na GOON DATA. Ao realizar auditorias internas e externas regularmente, analisar os resultados e implementar ações corretivas, estamos fortalecendo nossa postura de segurança e garantindo a conformidade com os requisitos regulatórios e as melhores práticas de segurança da informação. Com um compromisso contínuo com a auditoria e revisão, estamos preparados para enfrentar os desafios em constante evolução do cenário de ameaças cibernéticas e proteger nossos ativos digitais contra ameaças emergentes.

11. Auditoria e Revisão

Na GOON DATA, acreditamos na importância da transparência, responsabilidade e melhoria contínua em nossas práticas de segurança da informação e cyber security. Para garantir a eficácia de nossas medidas de segurança e o cumprimento de nossa Política de Segurança da Informação, realizamos auditorias periódicas que abrangem tanto auditorias internas quanto externas.

Práticas Implementadas:

- Auditorias Internas e Externas: Conduzimos auditorias internas e externas regularmente para avaliar a conformidade com nossa Política de Segurança da Informação e Cyber Security. As auditorias internas são realizadas por nossa equipe de segurança interna, enquanto as externas podem ser conduzidas por auditores independentes ou agências especializadas.

- Análise e Ações Corretivas: Os resultados das auditorias são minuciosamente analisados para identificar áreas de não conformidade ou possíveis melhorias em

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

nossos controles de segurança. Se forem identificadas deficiências, desenvolvemos e implementamos planos de ação corretiva para abordar essas questões e fortalecer nossos sistemas de segurança.

- Revisão e Atualização da Política: A Política de Segurança da Informação e Cyber Security é uma parte dinâmica de nossa estrutura organizacional. Revisamos e atualizamos regularmente nossa política com base nos resultados das auditorias, nas mudanças no cenário de ameaças cibernéticas e nas melhores práticas da indústria. Isso garante que nossa política permaneça relevante e eficaz na proteção de nossos ativos digitais.

A auditoria e revisão são pilares fundamentais de nossa abordagem de segurança da informação e cyber security na GOON DATA. Ao conduzir auditorias internas e externas regularmente, analisar os resultados e implementar ações corretivas, estamos fortalecendo nossa postura de segurança e garantindo a proteção de nossos ativos digitais e dados confidenciais. Com um compromisso contínuo com a auditoria e revisão, estamos preparados para enfrentar os desafios cada vez mais complexos do cenário de ameaças cibernéticas.

12. Conclusão

Nossa Política de Segurança da Informação e Cyber Security é mais do que um documento; é um compromisso inabalável com a segurança, privacidade e confiabilidade em todas as operações da GOON DATA. Ao adotar uma abordagem abrangente e proativa para a proteção de nossos ativos digitais e dados confidenciais, estamos construindo um ambiente seguro e confiável para nossos clientes, colaboradores e parceiros.

Com a implementação desta política, reforçamos nosso compromisso com a excelência em segurança da informação e reafirmamos nosso papel como líderes responsáveis no cenário digital em constante evolução. A segurança da informação é uma jornada contínua, e na GOON DATA, estamos prontos para enfrentar os desafios do futuro com confiança e determinação.

Este documento não apenas estabelece diretrizes e procedimentos, mas também reflete nossa cultura organizacional e nosso compromisso com a proteção de dados. Continuaremos a monitorar, revisar e atualizar nossa política para garantir que permaneça relevante e eficaz diante das mudanças no ambiente de segurança da informação.

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br

POLÍTICA DE SEGURANÇA DA INFORMAÇÃOE CYBER SECURITY

Juntos, fortaleceremos nossa postura de segurança e protegeremos o que mais importa: a confiança de nossos clientes, a integridade de nossos sistemas e a segurança de nossos dados. Na GOON DATA, a segurança da informação é mais do que uma prioridade; é parte integrante de quem somos e do que representamos.

Data de Vigência: Esta Política de Segurança da Informação e Cyber Security entra em vigor a partir de 12/06/2024.

GOON DATA ASSESSORIA DE CRÉDITO LTDA.

41-99995.7643
atendimento@goondata.com.br
www.goondata.com.br