POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO EM CONSONÂNCIA COM A POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS – LGDP

Sócio Administrador

Título:	Política de Segurança Cibernética e da Informação em Consonância com a Política de Privacidade e Proteção de Dados Pessoais - LGPD
Versão:	E – 01
Sigla da Unidade Elaboradora:	CLO – Chief Legal Officer
Processo Vinculado:	Compliance
Distribuição:	Hyper Cash
Regulamentação Utilizada:	Lei 13.709, de 14 de agosto de 2018

Sócio Administrador

Apresentação

A HYPER CASH PAYMENTS LTDA, comumente conhecida como “HYPER CASH”, é uma pessoa jurídica de direito privado, devidamente registrada sob o CNPJ n.º 32.369.437/0001-93, e tem sua sede localizada na Rua Ministral, n.º 332, Edifício The Point, Sala 209-A, Bairro Despraiado, Cuiabá, Mato Grosso, CEP: 78.048-222. O representante legal da empresa, ISMAEL NAZARIO CARDOSO, brasileiro, solteiro, empresário, identificado pela Cédula de Identidade/RG n.º 7483484 SSP/SC e CPF n.º 120.382.979-59, atua neste ato em nome da HYPER CASH.

A HYPER CASH reafirma seu compromisso com a ética e a responsabilidade socioambiental, repudiando veementemente quaisquer formas de corrupção, suborno, discriminação, falsificação ideológica e documental, apropriação indébita ou usurpação, bem como qualquer tipo de trabalho infantil, forçado, escravo ou análogo a escravo. A empresa empenha-se em selecionar colaboradores e prestadores de serviços que estejam em conformidade com seus valores éticos.

Esta Política de Segurança Cibernética e da Informação em consonância com a Política de Privacidade e Proteção de Dados Pessoais - LGPD tem como objetivo orientar e estabelecer diretrizes claras para todos os membros, colaboradores, parceiros, terceiros e prestadores de serviços relevantes da HYPER CASH, com o intuito de promover a integridade e garantir o cumprimento das obrigações legais relacionadas à segurança cibernética e proteção de dados.

Todos os membros, colaboradores, parceiros, terceiros e prestadores de serviços relevantes da HYPER CASH são obrigados a aderir e seguir estritamente esta Política em todas as suas atividades. O desconhecimento desta Política não será considerado uma justificativa para o descumprimento da mesma. Qualquer dúvida, esclarecimento ou necessidade de orientação deve ser prontamente direcionada à Área de Compliance e Gestão de Riscos.

Esta Política estará disponível para consulta, tanto impressa e encadernada na área de Compliance, quanto na rede interna da empresa por meio da intranet. É responsabilidade de todos os membros, colaboradores, parceiros, terceiros e prestadores de serviços relevantes reportar imediatamente à Área de Compliance e Gestão de Riscos qualquer atividade suspeita, ilícita ou que viole os princípios estabelecidos nesta Política e na legislação aplicável relacionada à segurança cibernética e proteção de dados.

Cuiabá, Mato Grosso, 3 de junho de 2024

Ismael Nazario Cardoso
Sócio Administrador

Sócio Administrador

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO EM CONSONÂNCIA COM A POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS - LGPD

Este documento estabelece A Política de Segurança Cibernética e da Informação, que se desenvolve em estrita observância à legislação vigente, em especial à Lei Geral de Proteção de Dados Pessoais (LGPD), com o propósito de garantir a proteção, integridade e confidencialidade dos dados pessoais sob nossa responsabilidade. O compromisso com a segurança cibernética e da informação é fundamental para preservar a confiança de nossos usuários, colaboradores e demais partes interessadas. Por meio desta política, buscamos estabelecer diretrizes claras e medidas robustas para mitigar riscos e assegurar o cumprimento das normas de privacidade e proteção de dados.

DO OBJETIVO:

Esta política tem como principal objetivo garantir a proteção, integridade e confidencialidade dos dados pessoais sob a responsabilidade da HYPER CASH, em conformidade com as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD).

Através desta política, buscamos estabelecer diretrizes claras e medidas robustas para mitigar riscos relacionados à segurança cibernética e à proteção da informação, assegurando o cumprimento das normas de privacidade e proteção de dados estabelecidas pela legislação vigente.

Além disso, a política visa promover uma cultura organizacional voltada para a conscientização e a responsabilidade no tratamento de dados, tanto por parte dos colaboradores quanto de parceiros, terceiros e prestadores de serviços relevantes da HYPER CASH.

Dessa forma, nosso objetivo é assegurar não apenas a conformidade legal, mas também a confiança de nossos clientes, colaboradores e demais partes interessadas, reafirmando o compromisso da HYPER CASH com a ética, transparência e responsabilidade no uso e proteção dos dados pessoais.

DAS DEFINIÇÕES

Para uma análise precisa dos procedimentos de segurança cibernética e proteção de dados, é essencial compreender as definições a seguir, as quais estabelecem a base conceitual necessária para uma aplicação eficiente. Essas definições esclarecem os termos e conceitos essenciais relacionados à segurança cibernética e proteção da informação, garantindo uma interpretação consistente e abrangente dos procedimentos estabelecidos. Ao detalhar e aprofundar tais definições, asseguramos que os envolvidos compreendam plenamente suas responsabilidades e obrigações na adesão aos princípios estabelecidos. Esta abordagem simplifica a implementação dos procedimentos delineados na política de segurança cibernética e da informação, promovendo uma cultura organizacional de integridade e conformidade com as leis e regulamentos pertinentes, incluindo a LGPD.

RECURSOS: Esses são todos os ativos, tangíveis ou intangíveis, que pertencem, estão

Sócio Administrador

a serviço ou sob a responsabilidade da HYPER CASH e que possuem valor para a empresa. Isso inclui uma variedade de elementos, como pessoas, ambientes físicos, tecnologias, serviços contratados (incluindo serviços em nuvem), sistemas e processos. Todos esses recursos desempenham um papel fundamental no suporte às operações e na consecução dos objetivos da organização.

AMEAÇA: Uma ameaça é qualquer causa potencial de um incidente indesejado que pode resultar em impacto nos objetivos do negócio. As ameaças podem surgir de fontes internas ou externas e podem ser intencionais (como ataques cibernéticos) ou não intencionais (como falhas de hardware). É crucial identificar e avaliar as ameaças para implementar medidas adequadas de mitigação de riscos.

CONTROLE: Um controle é qualquer recurso ou medida que assegura formas de tratamento de riscos, incluindo a redução, eliminação ou transferência dos mesmos. Os controles podem assumir diversas formas, tais como políticas, processos, estruturas organizacionais, técnicas padrões, software, hardware e outros. A implantação e manutenção adequada de controles são essenciais para garantir a segurança das informações e dos recursos da organização.

GESTOR: Um gestor é um colaborador que exerce um cargo de liderança na organização, como Diretor Presidente, Coordenador ou Supervisores de seção. São responsáveis por orientar e supervisionar as atividades relacionadas à segurança cibernética e da informação, além de promover uma cultura de segurança dentro da empresa.

INFORMAÇÃO: Informação é qualquer conjunto organizado de dados que possui algum propósito e valor para o sistema da HYPER CASH, seus clientes, parceiros e colaboradores. Pode incluir informações de propriedade da empresa, bem como aquelas sob sua custódia ou de terceiros, como as informações armazenadas em nuvem. Proteger a informação é fundamental para garantir a confidencialidade, integridade, disponibilidade e conformidade dos dados.

PRINCÍPIOS DE "LEAST PRIVILEGE" E "NEED TO KNOW": Esses princípios orientam a autorização de acesso a sistemas e informações, garantindo que apenas as pessoas que realmente precisam de acesso recebam permissão para fazê-lo. De acordo com esses princípios, o acesso concedido deve ser o mínimo necessário para que os colaboradores possam desempenhar suas funções de forma eficaz e segura.

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO: Esta política consiste em uma estrutura de documentos que inclui a política, normas e padrões de segurança cibernética e segurança da informação. Ela estabelece diretrizes e procedimentos para proteger os recursos e informações da organização contra ameaças cibernéticas e garantir o cumprimento das leis e regulamentos aplicáveis.

SEGURANÇA DA INFORMAÇÃO (SI): A segurança da informação refere-se à proteção das informações da organização, garantindo sua confidencialidade, integridade, disponibilidade e conformidade. Isso envolve a implementação de controles de segurança adequados para proteger as informações contra acesso não autorizado,

alteração indevida, indisponibilidade e garantir o cumprimento dos requisitos legais e regulamentares.

SEGURANÇA CIBERNÉTICA: A segurança cibernética engloba um conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados contra ataques cibernéticos, danos ou acesso não autorizado. Também conhecida como segurança de TI, seu foco está na proteção de ativos digitais e na prevenção de incidentes de segurança cibernética.

RECURSOS CRÍTICOS: Esses são os recursos essenciais para o funcionamento da operação do sistema da HYPER CASH, que possuem informações críticas ou sensíveis. São recursos cuja disponibilidade, integridade e confidencialidade são de extrema importância para a continuidade dos negócios e o cumprimento dos objetivos da organização. A proteção adequada desses recursos é vital para evitar impactos adversos nos negócios e na reputação da empresa.

DAS NORMAS DE REFERÊNCIA:

O HYPER CASH está comprometido em cumprir integralmente a legislação pertinente ao tema, incluindo a Lei Geral de Proteção de Dados (LGPD). Especificamente, destacam-se as seguintes normativas:

LEI 13.709, DE 14 DE AGOSTO DE 2018: Conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), é uma legislação brasileira que regula o tratamento de dados pessoais por parte de empresas e organizações.

DA BASE PROCEDIMENTAL:

A HYPER CASH reconhece a importância crítica da proteção da informação como um ativo essencial para os negócios da empresa. Nesse sentido, a segurança cibernética e da informação é fundamental para salvaguardar os dados contra uma variedade de ameaças, minimizando a exposição da empresa a riscos potenciais. A Política de Segurança Cibernética e da Informação da HYPER CASH é formulada com o objetivo de assegurar a preservação das características fundamentais da informação: confidencialidade, integridade, disponibilidade e conformidade. Para garantir a conformidade com os requisitos da LGPD e alinhar-se com os objetivos do negócio, a HYPER CASH estabelece as seguintes diretrizes:

PROTEÇÃO DE DADOS PESSOAIS: Todos os dados pessoais coletados, processados e armazenados pela HYPER CASH devem ser tratados com o mais alto grau de cuidado e proteção, em conformidade com os princípios e diretrizes estabelecidos pela LGPD.

CONSENTIMENTO E TRANSPARÊNCIA: É fundamental obter o consentimento explícito dos titulares dos dados antes de coletar ou processar qualquer informação pessoal. Além disso, a empresa deve fornecer transparência adequada sobre como os dados serão utilizados e protegidos.

MINIMIZAÇÃO DE DADOS: A coleta e o processamento de dados pessoais devem ser

limitados ao mínimo necessário para a realização das finalidades específicas para as quais foram coletados, em conformidade com o princípio da necessidade.

SEGURANÇA DA INFORMAÇÃO: Devem ser implementadas medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra acesso não autorizado, divulgação, alteração ou destruição não autorizada, levando em consideração as melhores práticas de segurança da informação.

ACESSO RESTRITO: O acesso aos dados pessoais deve ser restrito apenas a colaboradores autorizados que necessitem de acesso para desempenhar suas funções específicas. Esse acesso deve ser controlado e monitorado de forma a garantir a segurança e a confidencialidade dos dados.

TREINAMENTO E CONSCIENTIZAÇÃO: Todos os colaboradores da HYPER CASH devem receber treinamento adequado sobre as políticas e práticas de segurança da informação, bem como sobre as disposições da LGPD. A conscientização sobre a importância da proteção de dados pessoais deve ser promovida em todos os níveis da organização.

MONITORAMENTO E AUDITORIA: Devem ser estabelecidos mecanismos de monitoramento e auditoria para verificar o cumprimento das políticas de segurança da informação e identificar eventuais vulnerabilidades ou incidentes de segurança.

GERENCIAMENTO DE INCIDENTES: Deve ser implementado um processo de gerenciamento de incidentes de segurança da informação para detectar, investigar e responder rapidamente a quaisquer incidentes de segurança que possam afetar a proteção dos dados pessoais.

Ao seguir estas diretrizes, a HYPER CASH se compromete a proteger os dados pessoais de seus clientes, fornecedores e parceiros de negócios, cumprindo com as disposições da LGPD e garantindo a confiança e a privacidade dos titulares dos dados.

DA AMPLITUDE:

Os procedimentos de segurança cibernética e da informação em consonância com a Política de Privacidade e Proteção de Dados Pessoais - LGPD na HYPER CASH são aplicáveis a todas as etapas relacionadas à proteção e gerenciamento de dados. É responsabilidade de todas as áreas da empresa promover, cumprir e aprimorar as medidas de segurança cibernética e proteção de dados, garantindo uma abordagem integrada e abrangente na identificação e mitigação de potenciais riscos relacionados à segurança da informação.

Isso implica que todos os departamentos devem estar comprometidos em seguir as diretrizes estabelecidas nesta política, assegurando a conformidade regulatória e a integridade das operações da HYPER CASH. A colaboração de todos os setores é essencial para garantir a eficácia dos procedimentos de segurança cibernética e proteção de dados, prevenindo incidentes de segurança, violações de privacidade e o uso indevido de informações confidenciais.

Sócio Administrador

Ao seguir as diretrizes estabelecidas nesta política, a HYPER CASH reforça seu compromisso com a transparência, integridade e segurança em todas as suas operações relacionadas à proteção de dados e segurança cibernética.

DA APLICABILIDADE:

Os procedimentos de segurança cibernética e da informação em consonância com a Política de Privacidade e Proteção de Dados Pessoais - LGPD na HYPER CASH são aplicáveis a todos os órgãos e unidades operacionais da instituição, assim como a empresas terceirizadas, consultores, parceiros de negócios e quaisquer outras partes que mantenham relacionamento com a empresa. Isso significa que todas as entidades ou indivíduos que tenham vínculo ou realizem atividades em nome da HYPER CASH estão sujeitos aos princípios, diretrizes e procedimentos estabelecidos na política de segurança cibernética e da informação.

A abrangência destes procedimentos reflete o compromisso da HYPER CASH em garantir a conformidade e a integridade em todas as suas operações e relacionamentos comerciais, protegendo não apenas os dados pessoais dos clientes, colaboradores e parceiros, mas também assegurando a segurança cibernética de todos os sistemas e informações sob sua responsabilidade.

DA COMUNICAÇÃO E TREINAMENTO:

O HYPER CASH divulgará este conteúdo aos demais públicos relevantes de relacionamento, fornecendo diretrizes sobre a Política de Segurança Cibernética e da Informação em Consonância com a Política de Privacidade e Proteção de Dados Pessoais - LGPD, reiterando os princípios que orientam a relação com as partes interessadas.

Todos os funcionários devem receber treinamento regular sobre os procedimentos de segurança cibernética e da informação da HYPER CASH, assim como os procedimentos necessários para identificar e prevenir incidentes de segurança cibernética, violações de privacidade ou qualquer indício de irregularidades relacionadas à proteção de dados pessoais. Esse treinamento é fundamental para fortalecer a cultura organizacional de integridade e garantir o cumprimento das normas e regulamentações pertinentes ao setor bancário, especialmente a LGPD.

DA DISTRIBUIÇÃO DE RESPONSABILIDADES

Na HYPER CASH, cada membro da equipe, independentemente de sua posição na hierarquia, possui responsabilidades específicas na gestão da Política de Segurança Cibernética e da Informação em Consonância com a Política de Privacidade e Proteção de Dados Pessoais - LGPD. A estrutura organizacional delineia de maneira clara as atribuições individuais de cada colaborador no cumprimento das normas e regulamentações relevantes para prevenir riscos e irregularidades relacionados à segurança cibernética e proteção de dados.

DA ALTA ADMINISTRAÇÃO: À Alta Administração cabe estabelecer as políticas e

Sócio Administrador

diretrizes gerais relacionadas à segurança cibernética e proteção de dados, garantindo sua conformidade com as leis e regulamentos aplicáveis. Além disso, é responsável por supervisionar e monitorar a eficácia dos procedimentos em toda a organização.

ÁREA DE COMPLIANCE E GESTÃO DE RISCOS: Compete à área de compliance e gestão de riscos desenvolver e implementar os procedimentos específicos de segurança cibernética e proteção de dados, incluindo a coleta e verificação de informações dos clientes, análise de riscos, monitoramento contínuo e treinamento de funcionários. Também é responsável por garantir que todos os procedimentos estejam em conformidade com as leis e regulamentos relevantes, incluindo a LGPD.

DEPARTAMENTO JURÍDICO: Sobre o departamento jurídico recai o dever de fornecer orientação legal sobre questões relacionadas à segurança cibernética e proteção de dados, garantindo que todos os procedimentos estejam em conformidade com as leis e regulamentos aplicáveis, incluindo a LGPD. Também é responsável por lidar com questões legais relacionadas à identificação e prevenção de atividades fraudulentas.

DEPARTAMENTO DE RECURSOS HUMANOS: Responsável por garantir que todos os funcionários recebam treinamento adequado sobre os procedimentos de segurança cibernética e proteção de dados e estejam cientes de suas responsabilidades individuais. Também é responsável por monitorar o cumprimento dos procedimentos pelos funcionários e tomar medidas corretivas, se necessário.

DEPARTAMENTOS DE NEGÓCIOS E ATENDIMENTO AO CLIENTE (CADASTRO DE CLIENTES): Responsáveis por implementar os procedimentos no dia-a-dia das operações, incluindo a coleta e verificação de informações dos clientes durante o processo de cadastro e credenciamento. Também são responsáveis por relatar quaisquer atividades suspeitas à Área de Compliance e Gestão de Riscos. Ainda incumbe a esses departamentos: a coleta de informações, a verificação de documentos, a análise de risco e o reporte de atividades suspeitas. Todos os colaboradores devem estar engajados em treinamentos regulares sobre os procedimentos, garantindo que estejam atualizados com as melhores práticas e regulamentações mais recentes, incluindo a LGPD.

Essa distribuição de responsabilidades garante uma abordagem integrada e abrangente na identificação e mitigação de potenciais riscos relacionados à segurança cibernética e proteção de dados, promovendo uma cultura organizacional de integridade e conformidade.

DAS BASES PARA O TRATAMENTO DAS INFORMAÇÕES

Para garantir a integridade e confidencialidade dos dados, é imprescindível que todas as informações, independentemente do meio de armazenamento, sejam regidas por regras claramente definidas pelo seu proprietário. Estas normas devem salvaguardar contra perdas, alterações e acessos não autorizados. Cada

Sócio Administrador

informação deve ser associada a usuários específicos, instituições ou áreas, estipulando-se os direitos de acesso para cada um.

A proteção contra acesso não autorizado é uma prioridade, sendo imperativo estabelecer procedimentos robustos para garantir a segurança dos dados em todos os níveis. Além disso, informações críticas para a continuidade das operações da HYPER CASH devem ser devidamente respaldadas por cópias de segurança, armazenadas em locais fisicamente segregados e seguros, assegurando sua rápida recuperação em caso de eventualidades.

Quando informações forem descartadas, seja em forma física ou digital, devem ser adequadamente destruídas ou armazenadas em ambientes protegidos contra o acesso não autorizado. Cada colaborador da HYPER CASH é responsável pela segurança das informações às quais tem acesso, reforçando a importância da vigilância contínua e do comprometimento com as políticas de segurança da informação.

Em casos de extravio de informações, é fundamental que sejam prontamente devolvidas à sua origem, minimizando potenciais riscos de segurança e preservando a integridade dos dados. Essas diretrizes visam não apenas proteger os interesses da empresa, mas também garantir a confiança e privacidade de todas as partes envolvidas.

DAS BOAS PRÁTICAS NO TRATAMENTO DAS INFORMAÇÕES

É fundamental que os colaboradores se abstenham de realizar tentativas de acesso a informações para as quais não possuam autorização explícita. Em vez disso, devem solicitar o acesso ao respectivo proprietário da informação, pasta ou arquivo, respeitando os protocolos estabelecidos para garantir a segurança e integridade dos dados.

A elaboração das normas e procedimentos de acesso deve ser conduzida com cuidado meticuloso, levando em consideração os potenciais riscos associados ao acesso e alteração não autorizados, à divulgação indevida e à indisponibilidade dos dados. Tais riscos podem acarretar consequências significativas, incluindo fraudes, problemas legais, perdas de negócios, danos à reputação e dificuldades na recuperação das informações afetadas.

Ao priorizar a proteção e segurança dos dados, a HYPER CASH reforça seu compromisso com a integridade, transparência e confiança, fundamentais para sustentar suas operações e relacionamentos comerciais. Essas recomendações visam garantir que a gestão da informação seja conduzida de maneira responsável e criteriosa, minimizando potenciais riscos e maximizando a eficiência operacional.

DOS PROPÓSITO E ORIENTAÇÕES PARA CLASSIFICAÇÃO DE DADOS

A classificação da informação tem como principal objetivo proporcionar aos usuários a capacidade de analisar e compreender suas informações de forma clara e eficaz, facilitando a definição do nível de acesso e as condições ideais de armazenamento. Este processo considera cuidadosamente os aspectos de confidencialidade, integridade e disponibilidade de cada conjunto de dados.

É imperativo que todas as informações sejam submetidas a um processo de classificação adequado. Até que

sua classificação seja estabelecida, todas as informações devem ser tratadas como sigilosas e de alto risco, garantindo uma postura proativa na proteção dos dados.

A proteção da informação, tanto em termos de acesso quanto de preservação, deve ser ajustada de acordo com sua classificação, assegurando que os recursos de segurança sejam proporcionais ao grau de sensibilidade dos dados. Em casos em que um mesmo meio físico contenha informações classificadas de forma diferente, a adoção da classificação mais restrita é essencial para garantir a segurança dos dados em conformidade com os requisitos de privacidade e segurança.

Quaisquer alterações significativas em sistemas informatizados ou nas características das informações devem ser comunicadas aos usuários com antecedência, seguidas por uma revisão da classificação para garantir que as medidas de proteção sejam devidamente atualizadas e alinhadas com os novos requisitos. Essas diretrizes visam promover uma gestão responsável e eficaz da informação, garantindo sua segurança e integridade em todos os momentos.

DOS CONCEITOS DE CONFIDENCIALIDADE E CLASSIFICAÇÃO DE INFORMAÇÕES

No ambiente corporativo, a gestão adequada da informação é crucial para a proteção dos interesses da organização, a preservação da confiança dos clientes e a conformidade com regulamentações pertinentes. Nesse contexto, a definição e classificação das informações desempenham um papel fundamental, especialmente no que diz respeito à confidencialidade dos dados.

Nesta abordagem, exploraremos os diferentes tipos de informações, desde aquelas consideradas altamente sigilosas até as de caráter público, delineando suas características distintivas e a importância de sua classificação apropriada para garantir a segurança e integridade dos dados corporativos. Vamos examinar cada categoria em detalhes, destacando suas peculiaridades e o impacto que cada uma possui na estratégia de proteção da informação da HYPER CASH.

INFORMAÇÕES SIGILOSAS: Correspondem a dados altamente restritos, cuja divulgação é estritamente controlada devido ao seu valor estratégico e ao potencial de causar prejuízos significativos. O nível de proteção atribuído a essas informações deve ser o mais elevado possível.

INFORMAÇÕES CONFIDENCIAIS: Referem-se a dados de natureza setorial, destinados a um grupo restrito de indivíduos dentro de uma área específica ou setor de atividade.

INFORMAÇÕES INTERNAS: Englobam os dados utilizados internamente pela organização, abordando questões relevantes para os colaboradores e destinadas ao uso dentro do ambiente organizacional.

INFORMAÇÕES PÚBLICAS: São os dados que circulam livremente, tanto interna quanto externamente à HYPER CASH, sem restrições quanto à sua divulgação ou acesso, não sendo objeto de controle específico por parte da empresa.

DOS CONCEITOS DE INTEGRIDADE E DISPONIBILIDADE DE INFORMAÇÕES

No contexto da gestão da informação, a integridade e a disponibilidade são pilares essenciais para garantir a confiabilidade e a eficiência dos processos organizacionais. Compreender os diferentes níveis de risco associados às informações é fundamental para uma abordagem eficaz na proteção e na administração dos dados corporativos.

Nesta seção, exploraremos os conceitos de integridade e disponibilidade de informações, categorizando-as de acordo com seu potencial impacto nos negócios da HYPER CASH. Ao examinar os distintos níveis de risco e as medidas correspondentes de proteção e recuperação, será possível desenvolver uma estratégia abrangente para preservar a integridade dos dados e garantir sua disponibilidade quando necessário. Vamos analisar cada categoria em detalhes, identificando suas características distintivas e destacando a importância de sua gestão adequada para o sucesso contínuo das operações da empresa.

DE ALTO RISCO: Refere-se a informações cuja falta de disponibilidade ou integridade pode acarretar sérios prejuízos à continuidade das operações comerciais. A proteção e a recuperação dessas informações devem ser priorizadas devido ao seu impacto significativo nos negócios.

DE MÉDIO RISCO: Engloba informações que representam desafios em termos de disponibilidade e recuperação, porém, tanto o proprietário quanto os usuários estão cientes e aceitam as limitações de disponibilidade e o tempo necessário para a recuperação. Essas informações requerem uma atenção especial para garantir que os sistemas possam lidar com possíveis interrupções.

DE BAIXO RISCO: São informações que apresentam pouco ou nenhum risco para o negócio em termos de precisão e acessibilidade. Os usuários estão preparados para aceitar eventuais períodos de indisponibilidade e recuperação prolongada desses dados, dada a baixa criticidade associada a eles.

DA GESTÃO DE ACESSO DE USUÁRIOS: DIRETRIZES E PRÁTICAS

A administração eficaz do acesso aos sistemas é crucial para garantir a segurança e a integridade das operações da HYPER CASH Nesse sentido, a área responsável pelo controle de acesso deve estabelecer procedimentos formais abrangendo desde o registro inicial de novos usuários até a gestão de privilégios, senhas e revogação de autorizações.

Para prevenir acessos não autorizados, é essencial que a área de controle de acesso implemente medidas robustas de segurança. Cada usuário deve ser responsável pela gestão dos arquivos em sua pasta designada, assegurando a integridade e a confidencialidade dos dados sob sua responsabilidade.

É fundamental garantir que os usuários conectados à rede corporativa não comprometam a segurança dos sistemas operacionais ou produtos. Para isso, é necessário que cada estação de trabalho seja configurada com um servidor de controlador de domínio, impedindo alterações indevidas por parte dos usuários.

Ademais, a inserção de novas informações por meio de dispositivos removíveis deve ser estritamente controlada, exigindo autorização prévia do gerente ou gestor responsável, bem como a verificação da presença

e atualização do antivírus nos computadores.

O acesso aos serviços computacionais deve ser realizado de forma segura, através de procedimentos que minimizem os riscos de acessos não autorizados. Da mesma forma, o acesso remoto às estações de trabalho somente deve ocorrer mediante autorização do usuário correspondente, garantindo a segurança do sistema e dos dados corporativos.

DOS PRINCÍPIOS FUNDAMENTAIS DA SEGURANÇA FÍSICA DE EQUIPAMENTOS DE TECNOLOGIA

Assegurar a segurança física dos computadores e servidores é uma medida essencial para proteger os ativos de tecnologia da HYPER CASH. Para isso, é imprescindível que a estrutura dedicada à segurança física atenda aos padrões estabelecidos e se ajuste às especificações mínimas descritas neste protocolo.

O ambiente destinado à instalação dos equipamentos deve possuir dimensões adequadas para acomodar tanto os dispositivos de rede quanto os microcomputadores. Além disso, é crucial garantir que as entradas de ar estejam desobstruídas, permitindo uma ventilação adequada para evitar o superaquecimento dos equipamentos.

A disposição dos cabos, tanto os de rede quanto os de energia, deve ser cuidadosamente planejada e instalada em canaletas específicas. Isso garante que não haja interferência na rede e que as pessoas possam transitar livremente pelo ambiente, reduzindo o risco de danos acidentais aos cabos e garantindo a segurança das operações tecnológicas da empresa.

DAS DIRETRIZES PARA O PLANO DE RETENÇÃO DE DADOS

A HYPER CASH está comprometida em estabelecer políticas abrangentes de retenção de dados, em conformidade com as normas e regulamentações pertinentes, especialmente aquelas relacionadas à proteção de dados pessoais. Garantir a segurança e a integridade dos dados é essencial para o funcionamento eficaz e ético da empresa. Nesse sentido, este plano delineia as diretrizes fundamentais para o gerenciamento responsável e sustentável dos dados, visando atender aos requisitos legais e proteger a privacidade e os direitos dos indivíduos.

DAS ESTRATÉGIAS PARA CONSCIENTIZAÇÃO E DIVULGAÇÃO DA SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

Na HYPER CASH, é primordial que os recursos e informações, sejam eles de propriedade ou sob custódia da empresa, sejam utilizados em conformidade com os interesses organizacionais. Isso implica prestar serviços alinhados com os requisitos estabelecidos e respeitar as diretrizes estabelecidas para garantir a segurança cibernética e da informação.

A disseminação efetiva das políticas, normas e padrões de segurança cibernética e da informação é essencial desde o processo de admissão e integração de novos colaboradores. Tanto as equipes de recursos humanos quanto os gestores desempenham um papel fundamental na transmissão dessas diretrizes, assegurando que

Sócio Administrador

todos os membros da equipe compreendam sua importância e aplicação.

Além disso, programas contínuos de conscientização, divulgação e reciclagem do conhecimento sobre segurança cibernética e da informação devem ser estabelecidos e implementados regularmente. Essas iniciativas visam garantir que todos os colaboradores e terceiros estejam plenamente cientes das diretrizes, práticas recomendadas e responsabilidades relacionadas à segurança das informações, promovendo assim uma cultura organizacional de proteção e conscientização.

DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO:

Na HYPER CASH, os incidentes de segurança da informação englobam todos os eventos adversos confirmados ou suspeitos que possam comprometer um ou mais princípios fundamentais da segurança da informação. Estes eventos podem colocar em risco a confidencialidade, integridade, disponibilidade e conformidade dos dados, representando uma ameaça para o negócio como um todo.

Qualquer violação, ou tentativa de violação, das políticas, normas ou controles de segurança da informação, independentemente de ser intencional ou não, é considerada um incidente de segurança. A identificação precoce, análise e resposta adequada a esses incidentes são essenciais para minimizar danos potenciais e proteger os ativos de informação da empresa.

DAS ESTRATÉGIAS DE PREVENÇÃO E DETECÇÃO DE INTRUSÕES

Na HYPER CASH, adotamos medidas rigorosas para garantir a segurança de nossos recursos de informação expostos à Internet. Implementamos sistemas de Detecção e Prevenção de Intrusões (IDS/IPS) para monitorar e proteger proativamente esses recursos contra ameaças externas mal-intencionadas.

Quando nosso sistema IDS/IPS identifica ou responde a uma tentativa significativa de intrusão que ameaça nossos ativos de informação, acionamos procedimentos de análise estruturada e resposta. Essas ações são essenciais para garantir uma abordagem eficaz na identificação precoce e mitigação de potenciais incidentes de segurança, preservando assim a integridade e confiabilidade de nossos sistemas de informação.

DO PLANO DE RESPOSTA A INCIDENTES: GARANTINDO A CONTINUIDADE OPERACIONAL

Na HYPER CASH, reconhecemos a importância de um plano de resposta a incidentes para garantir a continuidade de nossas operações em face de eventos adversos. Durante os testes de continuidade de negócios, elaboramos cenários de incidentes para identificar potenciais eventos que possam afetar nossa operação, comprometendo o desempenho e a execução de nossos processos organizacionais.

Em caso de incidentes, é fundamental que os terceiros e colaboradores notifiquem imediatamente o Departamento de Tecnologia da HYPER CASH. Essa pronta notificação permite que medidas de segurança sejam rapidamente implementadas, minimizando qualquer impacto adverso em nossos serviços e garantindo a proteção de nossos ativos de informação.

Nosso compromisso com a segurança e a continuidade operacional nos impulsiona a desenvolver e aprimorar constantemente nosso plano de resposta a incidentes, garantindo que estejamos preparados para lidar eficazmente com qualquer desafio que possa surgir.

DAS ESTRATÉGIAS DE DEFESA CONTRA AMEAÇAS DIGITAIS: SALVAGUARDANDO OS EQUIPAMENTOS DE PROCESSAMENTO DE INFORMAÇÃO

Na HYPER CASH, priorizamos a segurança de nossos sistemas contra ameaças digitais, incluindo códigos maliciosos que possam comprometer a integridade de nossos equipamentos de processamento de informação. Implementamos rigorosos controles tecnológicos projetados para prevenir, detectar, corrigir e erradicar qualquer código executável malicioso que possa representar uma ameaça para nossos sistemas.

Nossa abordagem proativa inclui a adoção de soluções avançadas de segurança cibernética, tanto para os dispositivos de usuário final quanto para os servidores, garantindo uma defesa abrangente contra uma variedade de ameaças digitais. Ao manter nossos sistemas protegidos contra códigos maliciosos, estamos comprometidos em salvaguardar a integridade e a confidencialidade de nossas operações e dados.

DA AUDITORIA DE CONFORMIDADE E PROTEÇÃO DE DADOS: GARANTINDO A INTEGRIDADE OPERACIONAL

Na HYPER CASH, priorizamos a conformidade e a proteção de dados em todas as nossas operações. Como parte desse compromisso, reservamo-nos o direito de conduzir auditorias em qualquer dispositivo utilizado por indivíduos sujeitos a esta política durante o desempenho de suas atividades comerciais ou funções. Essas auditorias podem incluir solicitações de acesso a diversos aspectos, tais como:

Nível de usuário e/ou acesso em nível de sistema a qualquer computação ou comunicação.

Acesso a informações (eletrônicas, impressas etc.) que possam ser produzidas, transmitidas ou armazenadas em equipamentos ou instalações da HYPER CASH.

Acesso a áreas de trabalho, como escritórios, cubículos, áreas de armazenamento, data centers e centros de operações.

Acesso para monitorar e registrar interativamente o tráfego nas redes da HYPER CASH.

É fundamental observar que todas as auditorias realizadas estão em conformidade com as regras estabelecidas pela Lei Geral de Proteção de Dados. Além disso, os colaboradores da HYPER CASH são plenamente informados sobre a possibilidade e os procedimentos relacionados a essas auditorias por meio de uma comunicação interna de privacidade. Essas medidas visam garantir a integridade operacional e o cumprimento das regulamentações de proteção de dados em todas as nossas atividades comerciais.

DAS SANÇÕES E VIOLAÇÕES:

O descumprimento de qualquer diretriz estabelecida nesta Política acarretará sanções disciplinares, medidas administrativas e/ou criminais, conforme previsto na legislação em vigor. Tais penalidades serão aplicadas considerando a gravidade do evento e seus impactos correspondentes.

DAS DISPOSIÇÕES FINAIS:

A HYPER CASH manterá os dados e informações cadastrais de clientes, parceiros, colaboradores e prestadores de serviços em conformidade com os prazos estabelecidos pelas legislações aplicáveis e pelos critérios internos da instituição. Além disso, as instituições parceiras autorizadas pelo Banco Central do Brasil também deverão respeitar os prazos específicos de conservação de dados e informações conforme estipulado.

DA ATUALIZAÇÃO DA POLÍTICA:

Esta Política será atualizada sempre que houver alterações legislativas ou regulatórias relevantes, mudanças no cenário de negócios da empresa ou quando a revisão da análise de risco assim o exigir. A responsabilidade pela atualização e submissão à aprovação da Alta Administração recai sobre a Alta Administração ou o setor de compliance, se já implementado.

DA APROVAÇÃO E VIGÊNCIA:

Esta Política foi aprovada pela alta administração da HYPER CASH e entra em vigor na data de sua aprovação. Sua vigência é por prazo indeterminado, podendo ser substituída apenas por uma versão atualizada, mediante aprovação da alta administração.

Cuiabá, Mato Grosso, 3 de junho de 2024

Ismael Nazario Cardoso
Sócio Administrador