CÓDIGO DE QUALIDADE E SEGURANÇA DE DADOS

NOSSAS CRENÇAS

Garantir QUALIDADE & SEGURANÇA DE DADOS é fundamental para promover o SUCESSO e transmitir CONFIANÇA nas operações da organização. A INTEGRIDADE e a CONFORMIDADE dos dados é um pilar essencial para uma tomada de decisão precisa e formulação de estratégias eficazes.

Além disso, é imperativo ressaltar a importância da proteção dos nossos dados, já que qualquer comprometimento causado por um ataque cibernético traz riscos de PENALIDADES FINANCEIRAS e danos à REPUTAÇÃO da Brainvest. Dessa forma, a adoção de práticas para garantir a qualidade de dados, abrangendo procedimentos de validação e padronização, é indispensável para manter a confiabilidade e a uniformidade das nossas informações. Igualmente crucial é a priorização de medidas de segurança de dados para impedir o acesso não autorizado e garantir sua confidencialidade.

A segurança cibernética assume um papel fundamental na fortificação das defesas contra ameaças online. Medidas proativas, como a implantação de *firewalls*, sistemas de detecção de intrusão e atualizações de segurança de rotina, são indispensáveis para evitar ataques e manter a confiança entre as partes interessadas.

Este CÓDIGO descreve nosso COMPROMISSO em IDENTIFICAR e MITIGAR todos os RISCOS por meio da comunicação sistemática de tentativas de invasão interna e externa. Além disso, comparamos esses dados com o número crescente de funcionários para avaliar possíveis vulnerabilidades. A Brainvest coleta dados para garantir a qualidade e a segurança de nossos ativos, e monitora os principais *key performance* indicators (KPIs) destinados a manter a integridade e a proteção de nossos dados organizacionais.

ESCOPO

As diretrizes descritas neste CÓDIGO são aplicáveis a todas as unidades da Brainvest em todas as regiões em que operamos.

SUPERVISÃO E IMPLEMENTAÇÃO

A ÁREA DE TI GLOBAL é responsável por reunir as amostras de dados necessárias a cada mês e reportá-las à ÁREA DE ESG, a qual é responsável por consolidar todas as informações em um *template* próprio, calcular os KPIs e monitorá-los ao longo do tempo.

FREQUÊNCIA DE ATUALIZAÇÃO

A 'BASE DE QUALIDADE & SEGURANÇA DE DADOS' deve ser atualizada uma vez por semestre e seus resultados serão informados ao CEO Global e à Equipe de TI Global.

REGISTRO DE DADOS

Para monitorar a eficácia de nossas iniciativas e nossa eficiência em garantir a excelência na QUALIDADE DOS DADOS, fortalecer nossa estrutura de SEGURANÇA da informação e melhorar a efetividade da segurança cibernética, as seguintes informações serão coletadas:

- A 'BASE DE QUALIDADE & SEGURANÇA DE DADOS', será monitorada e avaliada pela equipe de ESG sistematicamente a quantidade e as diferentes intensidades dos riscos apresentados aos nossos ativos de informação, categorizando-os em classificações de baixo, médio, alto e crítico. Isso envolve o rastreamento de métricas como a FREQUÊNCIA DE TENTATIVAS DE INVASÃO EXTERNA, incidentes relacionados a ACESSOS EXTERNOS NÃO AUTORIZADOS e identificação de VULNERABILIDADES INTERNAS.

Essas avaliações serão realizadas mensalmente e em alinhamento com quaisquer flutuações em nossa força de trabalho. É importante enfatizar que os riscos são delineados tanto pela probabilidade quanto pelo impacto potencial nos sistemas e na integridade dos dados da Brainvest. Além disso, é crucial reconhecer que todos os dados acessíveis nesse banco de dados são usados estritamente com a finalidade de gerar *key performance indicators* (KPIs), excluindo, portanto, quaisquer dados auxiliares.

MÉTRICAS DE QUALIDADE & SEGURANÇA DE DADOS

Após a coleta dos dados descritos acima, calcularemos as seguintes métricas uma vez ao semestre:

- A razão de TENTATIVAS DE INVASÕES EXTERNAS pelo TOTAL DE FUNCIONÁRIOS EM TEMPO INTEGRAL ao longo do tempo.
- A razão de ACESSOS EXTERNOS NÃO AUTORIZADOS E BEM-SUCEDIDOS pelo TOTAL DE FUNCIONÁRIOS EM TEMPO INTEGRAL ao longo do tempo.
- A razão DE VULNERABILIDADES INTERNAS (baixa, média, alta e crítica) pelo TOTAL DE FUNCIONÁRIOS EM TEMPO INTEGRAL ao longo do tempo.
- A razão de TENTATIVAS DE INVASÕES INTERNAS PELO TOTAL DE FUNCIONÁRIOS EM TEMPO INTEGRAL durante o período.

- **TIPO DE INTERVENÇÃO:**

Material Educacional: envolve o desenvolvimento de recursos como vídeos, infográficos, guias e sessões de treinamento para educar os funcionários sobre as práticas recomendadas de cibersegurança. Esses materiais abordam tópicos como criação de senhas fortes, prevenção de *phishing* e os perigos de compartilhar informações confidenciais online.

Esforços de Conscientização: concentram-se em comunicar regularmente aos funcionários ameaças à segurança cibernética e medidas preventivas. Isso inclui o envio de e-mails de conscientização, a organização de eventos com a participação de especialistas em

cibersegurança, a exibição de pôsteres com dicas de cibersegurança no local de trabalho e o incentivo aos funcionários para que relatem atividades suspeitas.

Restrição de Navegação na Web: envolve medidas para limitar o acesso a sites e downloads potencialmente prejudiciais. Isso inclui o uso de filtros de conteúdo da web, a configuração de restrições de acesso durante o horário de trabalho, o bloqueio de downloads de fontes não confiáveis, a restrição de acesso a redes sociais e serviços de mensagens e o monitoramento do tráfego da web em busca de atividades suspeitas.

OBJETIVO FINAL

Nosso OBJETIVO é monitorar e aprimorar continuamente esses indicadores, garantindo a EXCELÊNCIA NA QUALIDADE DOS DADOS, fortalecendo nossa estrutura de SEGURANÇA DA INFORMAÇÃO e melhorando nossa EFICÁCIA EM CIBERSEGURANÇA. Essa análise visa otimizar a nossa tomada de decisão, promover a conformidade com os padrões de segurança e garantir a resiliência contra ameaças cibernéticas, contribuindo para a integridade e a confiabilidade de nossos sistemas e dados.

Além disso, reconhecemos que a segurança aprimorada dos dados não apenas protege aos interesses internos, mas também influencia positivamente a percepção externa da empresa. Com a garantia da segurança de dados, a empresa é vista pelos investidores e pelos *stakeholders* com maior confiança, fortalecendo assim sua reputação no mercado. A TRANSPARÊNCIA e a EXCELÊNCIA no GERENCIAMENTO DE DADOS e em CIBERSEGURANÇA tornaram-se componentes essenciais para a Brainvest se estabelecer como uma referência confiável e sólida para nosso setor.

BRAINVEST
WEALTH MANAGEMENT

DATA QUALITY & SECURITY CODE

OUR BELIEFS

Ensuring DATA QUALITY & SECURITY is paramount for fostering SUCCESS and instilling TRUST in the operations of the organization. The INTEGRITY and ACCURACY of data serve as foundational pillars for making informed decisions and formulating effective strategies.

Moreover, it is imperative to underscore the significance of safeguarding our data, as any compromise caused by a cyber-attack poses dual risks of FINANCIAL PENALTIES and REPUTATIONAL HARM to Brainvest. Therefore, the adoption of robust data quality practices, encompassing validation, standardization, and cleansing procedures, is indispensable to uphold our information reliability and uniformity. Equally crucial is the prioritization of data security measures to thwart unauthorized access and ensure the confidentiality of sensitive data.

Cybersecurity assumes a pivotal role in fortifying defenses against online threats. Proactive measures, such as the deployment of firewalls, intrusion detection systems, and routine security updates, are indispensable for preempting cyber-attacks and sustaining trust among stakeholders.

This CODE outlines our COMMITMENT to IDENTIFYING and MITIGATING all risks through the systematic reporting of internal and external intrusion attempts. Additionally, we compare these figures with the evolving count of employees to gauge potential vulnerabilities. Brainvest collects data to ensure the quality, security, and cybersecurity of our data assets, and monitors key performance indicators (KPIs) aimed at upholding the integrity and safeguarding our organizational data.

SCOPE

The guidelines described in this CODE are applicable to all Brainvest units in all regions in which we operate.

OVERSIGHT AND IMPLEMENTATION

The GLOBAL IT AREA is responsible for gathering the required data points on a monthly basis and reporting them to the ESG AREA, which is responsible for consolidating all data points into Brainvest's template, calculating the KPIs, and monitoring them over time.

UPDATE FREQUENCY

The 'DATA QUALITY & SECURITY CODE' shall be updated once a semester, and its results will be reported to the Global CEO and Global IT Team.

DATA POINTS

In order to monitor our INITIATIVES' EFFICACY and EFFECTIVENESS in ensuring excellence in DATA QUALITY, strengthening our information SECURITY framework, and improving cyber security effectiveness, the following data points will be gathered:

> •For the ' DATA QUALITY & SECURITY DATABASE', the ESG team will systematically monitor and assess the quantity and varying intensities of risks posed to our information assets, categorizing them into low, medium, and high-risk. This involves tracking metrics such as the FREQUENCY OF EXTERNAL INTRUSION ATTEMPTS, incidents related to UNAUTHORIZED EXTERNAL ACCESS, and identification of INTERNAL VULNERABILITIES.

These assessments will be conducted on a monthly basis and in alignment with any fluctuations in our workforce. It is imperative to emphasize that the risks at these levels are delineated by both probability and potential impact on Brainvest's systems and data integrity. Furthermore, it is crucial to recognize that all data accessible within this database is used strictly for the purpose of generating key performance indicators (KPIs), thus excluding any auxiliary data.

DATA QUALITY & SECURITY METRICS

After the gathering of the data points described above, we will calculate the following metrics once a semester:

- The ratio of EXTERNAL INTRUSIONS ATTEMPTED by the TOTAL FULL-TIME EMPLOYEE over the time.
- The ratio of SUCCESSFUL EXTERNAL UNAUTHORIZED ACCESS by the TOTAL FULL-TIME EMPLOYEE OVER the time.
- The ratio of INTERNAL VULNERABILITIES (low, medium, high, and critical) by the TOTAL FULL-TIME EMPLOYEES OVER the time.
- The ratio of INTERNAL INTRUSIONS ATTEMPTED by the TOTAL FULL-TIME EMPLOYEES OVER the time.

- **TYPE OF INTERVENTION:**

Educational Material: involves the development of resources such as videos, infographics, guides, and training sessions to educate employees on cybersecurity best practices. These materials cover topics like strong password creation, phishing prevention, and the dangers of sharing confidential information online.
Awareness efforts: focus on regularly communicating cybersecurity threats and preventive measures to employees. This includes sending awareness emails, organizing events featuring cybersecurity experts, displaying posters with cybersecurity tips in the workplace, and encouraging employees to report suspicious activities.

Web Restriction: involves implementing measures to restrict access to potentially harmful websites and downloads. This includes using web content filters, configuring access restrictions during work hours, blocking downloads from untrusted sources, restricting access to social networks and messaging services, and monitoring web traffic for suspicious activity.

ULTIMATE OBJECTIVE

Our GOAL is to continuously monitor and enhance these indicators, ensuring EXCELLENCE IN DATA QUALITY, strengthening our information SECURITY framework, and improving our CYBERSECURITY EFFECTIVENESS. This analysis aims to optimize decision-making, promote compliance with security standards, and ensure resilience against cyber threats, contributing to the integrity and reliability of our systems and data.

Moreover, we acknowledge that improved data security not only protects internal interests but also positively influences the external perception of the company. With increased data security, the company is perceived by investors and stakeholders with greater confidence, thereby fortifying its reputation in the market. TRANSPARENCY and EXCELLENCE in DATA MANAGEMENT and CYBERSECURITY have become essential components for establishing Brainvest as a trustworthy and robust reference in our industry.