Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

Segurança de Ativos

Em segurança da informação, o termo “ativo” se refere a tudo o que é importante e tem valor para uma empresa. Os ativos podem ser divididos em duas categorias: tangíveis e intangíveis.

- Ativos Tangíveis são os elementos físicos que compõem a infraestrutura de TI da empresa, como computadores, servidores, cabos, roteadores, switches etc. Também incluem os espaços físicos onde esses elementos estão localizados, como prédios, salas ou armários. Esses ativos são vulneráveis a riscos como roubo, furto, incêndio, inundação ou sabotagem.
- Ativos Intangíveis são os elementos lógicos que contêm as informações da empresa, como dados, arquivos, documentos, contratos, planos, projetos etc. Também incluem o conhecimento que os funcionários possuem sobre os processos e as tecnologias da empresa. Esses ativos são vulneráveis a riscos como invasão, vazamento, corrupção ou perda.

Proteger esses ativos é essencial para a continuidade e a competitividade do negócio. Se algo der errado, a empresa pode sofrer prejuízos financeiros, danos à sua reputação ou sanções legais. Por isso, entender e cuidar bem dos ativos, sejam eles tangíveis ou intangíveis, é uma parte fundamental do trabalho em segurança da informação. É como garantir que tudo o que é valioso para a empresa esteja seguro e em bom estado.

2.1 Classificação da Informação

Entender a classificação da informação é um pilar da segurança da informação. Esse processo determina como os dados serão manipulados e protegidos conforme sua relevância para a empresa. Aqui, abordaremos os distintos níveis de classificação, os critérios para tal e quem são os responsáveis nesta jornada.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

2.1.1 Níveis de Classificação

- **Informação Pública**: é aquela que pode ser divulgada livremente para qualquer pessoa ou entidade, sem que isso cause prejuízo à organização. São exemplos de informação pública: o nome da empresa, o endereço do site, o relatório anual, a missão e os valores organizacionais. Apesar de não exigir sigilo, a informação pública deve ser tratada com cuidado para evitar a sobrecarga informativa e garantir a sua relevância e eficácia.
- **Informação Interna (Sensível)**: é aquela que deve ser restrita aos membros da organização ou a terceiros autorizados. São exemplos de informação interna: os procedimentos operacionais, as políticas internas, os dados dos funcionários, os planos de marketing. A divulgação não autorizada desta informação pode causar danos moderados à organização, afetando a sua competitividade ou reputação. Por isso, a informação interna deve ser protegida contra alterações indevidas e acessos indevidos.
- **Informação Confidencial**: é aquela que deve ser protegida com o mais alto grau de segurança, pois a sua divulgação não autorizada pode causar danos graves à organização. São exemplos de informação confidencial: os dados dos clientes, os contratos comerciais, as informações financeiras, as estratégias de negócio. A informação confidencial deve ser acessada apenas por pessoas que tenham uma necessidade legítima e que estejam sujeitas a acordos de confidencialidade. Além disso, deve-se utilizar mecanismos de segurança como criptografia, autenticação e controle de acesso para garantir a confidencialidade e a integridade dessa informação.
- **Informação Restrita (Privada/Confidencial)**: é aquela que deve ser protegida com o mais alto nível de segurança possível, pois a sua divulgação não autorizada pode causar danos catastróficos à organização. São exemplos de informações restritas: os segredos comerciais, as patentes, as informações sensíveis do governo. A informação restrita deve ser acessada apenas por um número muito limitado de pessoas que tenham uma autorização especial e que estejam sujeitas a rigorosas medidas de segurança. Essas pessoas devem assinar termos de responsabilidade e compromisso para evitar qualquer vazamento ou uso indevido dessa informação.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

2.1.2 Critérios de Classificação

Para classificar as informações de forma adequada, é preciso levar em conta alguns fatores que determinam o seu nível de proteção necessário. Os principais critérios de classificação são:

- **Valor**: É o grau de importância da informação para a organização e para os seus objetivos. Quanto maior o valor, maior o nível de proteção necessário. O valor pode ser avaliado considerando, por exemplo, a contribuição da informação para a receita, a competitividade ou a reputação da organização.
- **Requisitos legais**: São as obrigações impostas por leis, normas ou contratos que regulam o tratamento das informações. Algumas informações podem ter um nível de confidencialidade definido por lei, como é o caso dos dados pessoais sensíveis previstos na LGPD.
- **Sensibilidade**: É o grau de exposição da informação a riscos internos ou externos. Quanto maior a sensibilidade, maior o nível de proteção necessário. A sensibilidade pode ser medida considerando, por exemplo, o impacto potencial da divulgação não autorizada, da modificação ou da destruição da informação.
- **Criticidade**: É o grau de essencialidade da informação para as operações contínuas da organização. Quanto maior a criticidade, maior o nível de proteção necessário. A criticidade pode ser avaliada considerando, por exemplo, o tempo máximo tolerável de indisponibilidade ou perda da informação.

2.1.3 Responsabilidades do Proprietário dos Dados:

O papel do proprietário dos dados é crucial para garantir a conformidade e a proteção adequada dos dados pessoais. De acordo com a LGPD, o proprietário é a figura central que detém a autoridade para decidir sobre o tratamento dos dados. Esta figura é, muitas vezes, representada por um gestor ou líder departamental. Suas principais responsabilidades incluem:

- **Classificação dos Dados**: Estabelecer a classificação correta da informação, tendo em vista critérios como valor, sensibilidade, criticidade e os requisitos legais pertinentes.

- **Monitoramento e Atualização**: O ambiente de negócios e o cenário regulatório estão em constante evolução. Portanto, o proprietário deve revisar e, se necessário, reclassificar as informações para garantir que elas reflitam o contexto atual.
- **Implementação de Controles de Segurança**: Assegurar que medidas de segurança eficazes estejam em vigor, honrando princípios essenciais como confidencialidade, integridade e disponibilidade.
- **Gestão de Acesso**: Determinar quais indivíduos ou entidades têm permissão para acessar, modificar ou distribuir informações. Isso envolve a criação de políticas claras e normas relacionadas ao uso e acesso de dados pessoais.
- **Proteção dos Direitos dos Titulares**: É imperativo que o proprietário dos dados reconheça e honre os direitos dos indivíduos cujas informações estão sob sua custódia. Isso engloba a garantia de direitos como acesso, correção, eliminação e portabilidade, bem como a possibilidade de revogação do consentimento quando aplicável.

Este papel é fundamental para que as organizações não apenas cumpram regulamentações, mas também cultivem a confiança de seus clientes e parceiros.

2.1.4 Dados e Conformidade Regulatória

A classificação de dados é vital tanto para a segurança da informação quanto para o cumprimento de regulamentos que orientam o uso e a proteção de dados, especialmente quando tratamos de informações pessoais. Regulamentações internacionais, como a GDPR na Europa, e nacionais, como a LGPD no Brasil, delineiam as responsabilidades e os cuidados que as organizações devem ter com os dados que manuseiam. Uma classificação correta permite que as empresas entendam e se adequem às normas aplicáveis, minimizando riscos de sanções por falhas.

Ainda assim, a tarefa de classificar dados é desafiadora. As informações estão em constante transformação, e o que hoje é categorizado de uma maneira, amanhã pode requerer uma reavaliação. Outro desafio é a perspectiva variada sobre um dado: enquanto uma área da empresa pode enxergá-lo como sensível, outra pode considerá-lo comum, gerando possíveis desalinhamentos. Assim, torna-

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

se crucial a capacitação contínua dos colaboradores. Todos devem compreender a relevância da correta classificação e os riscos de um erro.

Para tornar esse processo mais fluido e seguro, algumas ações recomendadas são:

Estabelecer diretrizes claras por meio de uma política de classificação de dados. Ela deve explicitar critérios, níveis de sensibilidade, responsabilidades e protocolos para uma correta categorização.

- Adotar ferramentas tecnológicas que automatizam a identificação e rotulagem dos dados conforme os padrões estabelecidos.
- Implementar auditorias regulares. Elas são fundamentais para checar a correta classificação e avaliar se as medidas de segurança adotadas estão em conformidade com a sensibilidade dos dados.
- Incentivar uma mentalidade voltada para a segurança da informação, sensibilizando os colaboradores quanto à seriedade da classificação dos dados e motivando-os a aderir rigorosamente às práticas recomendadas.

2.1.5 Cultivando uma Cultura de Segurança de Informação

Tão importante quanto as práticas e políticas formais é a promoção de uma cultura de conscientização sobre a segurança da informação. Todos os colaboradores, independentemente do nível hierárquico, devem entender a importância de proteger os ativos de informação.

Algumas estratégias para cultivar essa cultura incluem:

- **Treinamentos Regulares**: Realizar sessões de treinamento para manter os colaboradores atualizados sobre as melhores práticas e políticas da empresa.
- **Simulações**: Conduzir simulações de ataques cibernéticos, como phishing, para testar e treinar a equipe sobre como reagir em situações reais.
- **Reconhecimento e Recompensas**: Incentivar práticas seguras reconhecendo e recompensando aqueles que exemplificam uma excelente postura em segurança da informação.

- **Feedback Contínuo**: Promover canais de feedback para que os colaboradores possam reportar suspeitas ou incidentes, permitindo ações rápidas e eficientes.

2.1.6 Exemplo prático

A Empresa XYZ é uma start-up tecnológica focada no desenvolvimento de soluções de gestão para pequenas empresas. Ao longo do seu crescimento, a XYZ coleta, armazena e processa uma vasta gama de informações, desde dados financeiros de clientes até informações confidenciais sobre seus projetos de pesquisa e desenvolvimento.

A XYZ compreende que a segurança da informação não se refere apenas aos seus servidores e à infraestrutura de TI. Também reconhece o valor da informação armazenada em papéis, dispositivos móveis dos funcionários e até mesmo o conhecimento não documentado detido por sua equipe. Dada a natureza do seu negócio, a integridade e a proteção destes ativos são essenciais..

- **Classificação da Informação na Empresa XYZ**:
    - **Público**: A XYZ regularmente publica relatórios sobre suas atividades, inovações e ações sociais, tornando estas informações de livre acesso.
    - **Sensível**: Em um projeto recente, a XYZ está desenvolvendo uma nova solução de gestão. Embora não seja um segredo, os planos detalhados deste projeto são considerados sensíveis, já que a divulgação antecipada poderia dar vantagem aos concorrentes.
    - **Privado**: A XYZ armazena dados pessoais de seus clientes, incluindo nomes, endereços e informações de faturamento, o que torna essencial a proteção destes dados, tanto por razões éticas quanto legais (como a LGPD).
    - **Confidencial**: A empresa possui pesquisas de mercado, estratégias de penetração e algoritmos proprietários, que são classificados como confidenciais.
- **Critérios de Classificação na Empresa XYZ:**
    - **Valor**: A estratégia de penetração de mercado da XYZ é altamente valiosa, pois delineia sua abordagem para superar concorrentes e capturar novos mercados.
    - **Requisitos legais**: A XYZ é obrigada a proteger os dados de seus clientes por causa da LGPD.

- **Sensibilidade**: O algoritmo por trás da nova solução de gestão é altamente sensível. Se exposto, a XYZ perderia sua vantagem competitiva.
- **Criticidade**: O sistema de gestão de clientes é crítico. Se ele falhar, a XYZ não poderá processar pedidos ou faturar clientes.

- **Responsabilidades do Proprietário dos Dados na Empresa XYZ**: A Chefe de Dados, Sra. Maria, é responsável pela classificação dos dados na XYZ. Ela realiza revisões trimestrais para garantir que todas as informações estejam classificadas corretamente e que as medidas de segurança estejam alinhadas com estas classificações.
- **Dados e Conformidade Regulatória na Empresa XYZ**: A XYZ, sendo uma empresa digital, está sob constante escrutínio regulatório. Eles investiram em uma solução automatizada que rastreia e rotula dados, garantindo que sejam tratados de acordo com os regulamentos relevantes.
- **Cultivando uma Cultura de Segurança de Informação na Empresa XYZ**: Todo novo funcionário da XYZ passa por um treinamento sobre segurança da informação. Além disso, há simulações anuais de ataques cibernéticos para testar a resposta da equipe. A empresa promove uma competição anual, onde departamentos competem em desafios relacionados à segurança da informação, com prêmios para os vencedores, incentivando a adoção das melhores práticas.

Através destas práticas, a Empresa XYZ garante a proteção de seus valiosos ativos de informação, enquanto se mantém ágil e inovadora no mercado competitivo de tecnologia.

2.2 Propriedade e Responsabilidade

No mundo digital atual, é fundamental compreender quem possui e quem cuida dos dados. Esse aspecto é essencial para a segurança da informação, pois define as responsabilidades e os direitos dos agentes envolvidos no tratamento dos dados. É preciso saber claramente quem é o proprietário dos dados e quem é o custodiante bem como quais são as suas atribuições e obrigações para garantir a proteção dos dados.

2.2.1 Propriedade dos Dados

A propriedade dos dados é um conceito que define quem tem o direito legal e a responsabilidade de gerenciar uma informação. Existem dois atores principais quando se trata de propriedade de dados: o titular dos dados, que é a pessoa física a quem os dados se referem, e o controlador dos dados, que é a entidade ou organização que coleta e processa esses dados.

- **Titular dos Dados:** É quem fornece os dados, seja de forma voluntária ou como requisito para acessar determinado serviço ou produto. O titular dos dados tem os seguintes direitos:
    - **Acesso**: Solicitar e receber os dados que o controlador tem sobre ele.
    - **Correção**: Pedir para retificar dados incompletos, desatualizados ou incorretos.
    - **Exclusão**: Solicitar a exclusão de seus dados, em certas circunstâncias.
    - **Informação**: Saber como, onde e por que seus dados estão sendo processados.
    - **Portabilidade**: Solicitar a transferência de seus dados para outro controlador, se possível.
- **Controlador dos Dados**: É quem reúne e processa os dados fornecidos pelo titular, para uma finalidade específica e legítima. O controlador dos dados tem os seguintes direitos:
    - **Uso**: Utilizar os dados coletados para os fins que foram informados e consentidos pelo titular.
    - **Armazenamento**: Guardar os dados de forma segura e por um período conforme regulamentações ou necessidades operacionais.
    - **Transferência**: Em certos contextos, compartilhar os dados com parceiros ou outras entidades, desde que com consentimento ou dentro do que a legislação permite.
    - **Proteção**: Assegurar que os dados estejam protegidos contra acessos não autorizados, perdas ou vazamentos.
    - **Conformidade**: Processar os dados em conformidade com regulamentações locais e internacionais, como LGPD e GDPR.
    - **Transparência**: Informar ao titular sobre como os dados serão usados e quais são seus direitos em relação a esses dados.

Portanto, enquanto o titular tem o direito inerente sobre seus dados pessoais, o controlador assume uma série de direitos e responsabilidades ao coletar, processar e armazenar essas informações. Ambas

as partes devem estar cientes de seus direitos e deveres para garantir uma gestão de dados ética e conforme a lei.

2.2.2 Custodiante dos Dados

O custodiante dos dados é um profissional que atua como um guardião, encarregado de zelar pela integridade e segurança das informações que não são de sua propriedade, mas que estão sob sua responsabilidade. Em geral, esse papel é atribuído a departamentos ou profissionais de TI nas organizações. Diferentemente do proprietário dos dados - que pode ser o titular dos dados ou o controlador dos dados - o custodiante não define como os dados são usados, mas garante que sejam manuseados de maneira segura e ética.

Deveres do Custodiante:

- **Proteção**: Implementar e manter atualizadas medidas de segurança para defender os dados contra qualquer tipo de vulnerabilidade ou ameaça, como ataques cibernéticos, desastres naturais ou erros humanos.
- **Manutenção**: Garantir o armazenamento correto dos dados, realizar backups periódicos e, em caso de falhas, assegurar a pronta recuperação da informação.
- **Conformidade**: Trabalhar em alinhamento com as políticas estabelecidas pelo proprietário dos dados e, adicionalmente, cumprir as normativas legais relacionadas à proteção e privacidade de dados. Isto inclui, por exemplo, manter registros de qualquer acesso ou alteração feita aos dados e atender às solicitações dos titulares dos dados.

Ao compreender as diferenças entre proprietário e custodiante, fica evidente a importância de uma comunicação clara e de políticas bem definidas, para que ambas as partes estejam alinhadas no objetivo comum de proteger a informação.

2.2.3 Usuário dos Dados

Os usuários dos dados são aqueles que interagem diretamente com as informações, seja para consulta, edição ou outros fins operacionais. Embora não sejam os guardiões primários dos dados, têm um

papel crucial no ecossistema de segurança da informação, pois seu comportamento pode afetar a integridade e a confidencialidade das informações.

Responsabilidades do Usuário:

- **Uso Adequado**: Acessar e utilizar os dados respeitando os limites e propósitos estabelecidos pelo proprietário ou pelo controlador dos dados, evitando ações que possam colocá-los em risco ou violar os direitos dos titulares dos dados.
- **Adesão às Normas**: Cumprir rigorosamente as diretrizes e políticas estipuladas pela organização ou pela legislação, garantindo que os dados sejam manuseados de forma correta e segura.
- **Comunicação Proativa**: Ao identificar qualquer anomalia, falha ou suspeita de comprometimento dos dados, é dever do usuário reportar prontamente à equipe responsável ou ao custodiante dos dados.

Entender e respeitar estas responsabilidades não apenas protege os dados, mas também fortalece a cultura de segurança dentro de uma organização, promovendo um ambiente mais seguro para todos.

2.2.4 Implicações Legais e Éticas na Propriedade de Dados

Os dados, especialmente quando se referem a informações pessoais, estão no centro de um cenário jurídico em rápida transformação. Legislações como a GDPR (Regulamento Geral de Proteção de Dados) da Europa e a LGPD (Lei Geral de Proteção de Dados) do Brasil são testemunhos de um esforço global para garantir que os direitos dos indivíduos sejam respeitados e protegidos. Essas leis estabelecem não apenas direitos para as pessoas sobre suas informações, mas também definem as responsabilidades das organizações na coleta, armazenamento e processamento desses dados.

A ética, no entanto, vai além da mera conformidade jurídica. Ela explora o território do que é “certo” ou “justo”, independentemente da legalidade. Em relação aos dados, isso pode se traduzir em perguntas como: “Estamos usando esses dados de uma maneira que respeite a dignidade e privacidade do indivíduo?” ou “Os interessados estão cientes e consentiram com a maneira como seus dados estão sendo utilizados?”. Mesmo que a lei permita certas ações, como compartilhar informações com

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

terceiros, a ética requer uma reflexão mais profunda sobre o impacto e as consequências dessas decisões.

Por isso, as organizações devem alinhar suas políticas e práticas não apenas às diretrizes jurídicas, mas também aos princípios éticos sólidos, garantindo que o tratamento dos dados ocorra de forma transparente, justa e responsável.

2.2.5 Exemplo prático

Propriedade dos Dados

- **Titular dos Dados**: João Silva, um cliente da Loja Virtual ABC. Ele forneceu seus dados, como nome, endereço e informações de cartão de crédito, ao fazer uma compra no site.
    - João pode, a qualquer momento, entrar no site e verificar suas informações de compra, solicitar correção se o endereço estiver errado ou pedir para que seus dados sejam deletados do sistema da loja.
- **Controlador dos Dados**: Loja Virtual ABC. Eles coletaram e processaram os dados do João para enviar o produto que ele comprou.
    - A loja usa esses dados para enviar o produto ao endereço correto e processar o pagamento. Eles também armazenam esses dados de forma segura e só compartilham com parceiros, como a empresa de entrega, para garantir que o produto chegue até o João.

Custodiante dos Dados

- A equipe de TI da Loja Virtual ABC. Eles garantem que o site esteja seguro e que os dados dos clientes, como o João, estejam protegidos de hackers.
    - Eles fazem backups regularmente para evitar perda de informações e estão sempre atualizando o sistema para proteger contra qualquer tipo de ameaça digital.

Usuário dos Dados

- Atendente do Suporte ao Cliente da Loja Virtual ABC. Quando João tem uma dúvida sobre sua compra, ele entra em contato com o suporte.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

- O atendente acessa os dados da compra do João para ajudá-lo, mas não pode fazer alterações ou compartilhar essas informações. Se ele identificar algum problema, como suspeita de fraude, ele comunica imediatamente à equipe de TI.

Implicações Legais e Éticas

- A Loja Virtual ABC opera no Brasil, então eles precisam seguir a LGPD. Isso significa que, se o João pedir, eles devem mostrar exatamente quais dados têm sobre ele e como estão usando. Se João decidir que não quer mais que a loja tenha seus dados, ele pode pedir para ser "esquecido", e a loja tem que deletar todas as informações que tem dele.
- Além disso, mesmo que legalmente eles possam enviar ofertas de parceiros para o João por e-mail, eticamente eles decidiram só fazer isso se o João der permissão explícita. Então, quando João fez sua compra, havia uma caixinha perguntando se ele gostaria de receber ofertas de parceiros, e ele poderia escolher sim ou não.

2.3 Ciclo de Vida dos Dados

O Ciclo de Vida dos Dados é um processo que inclui várias fases, tais como criação, processamento, armazenamento, uso, compartilhamento, arquivamento e descarte de dados. Cada fase tem suas próprias práticas e considerações de segurança, que são fundamentais para proteger as informações contra acessos não autorizados, perdas ou vazamentos.

- **Criação de Dados**: A fase inicial do ciclo de vida dos dados é a sua criação. Aqui, os dados podem ser gerados internamente, como documentos, planilhas, ou através de transações online, bem como podem ser obtidos de fontes externas. Importante destacar que, desde a origem, é essencial garantir a confidencialidade e integridade dos dados, aplicando práticas seguras e controles apropriados, como criptografia e autenticação.
- **Coleta e Processamento**: Nesta etapa, os dados são coletados para serem processados conforme as necessidades operacionais. Durante o processamento, os dados são transformados, organizados ou analisados para extrair informações úteis. Durante estas fases, deve-se garantir que os dados sejam manipulados e armazenados de forma segura, mantendo sua precisão e confiabilidade através de controles e políticas de segurança rigorosos.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

- **Armazenamento**: O armazenamento refere-se à manutenção segura dos dados em diversos meios, como servidores, nuvens ou bases de dados. Durante esta fase, é crucial assegurar que os dados estejam protegidos contra acessos não autorizados e ameaças, como vazamentos ou ataques cibernéticos. Estratégias, como a criptografia de dados e a implementação de permissões de acesso restritivas, são práticas recomendadas para salvaguardar as informações armazenadas.
- **Transmissão**: Na fase de transmissão, os dados são transferidos entre locais, sistemas ou partes interessadas. Aqui, a integridade e a confidencialidade dos dados devem ser rigorosamente mantidas, utilizando protocolos de transmissão seguros, como HTTPS, e métodos de encriptação robustos para evitar interceptações maliciosas ou perda de dados.
- **Uso**: Durante o uso, os dados são acessados e manipulados por usuários autorizados. Políticas de controle de acesso e monitoramento contínuo são essenciais para garantir que os dados sejam utilizados de maneira apropriada e eticamente responsável, e para evitar o uso indevido ou o acesso não autorizado às informações.
- **Descarte**: Na fase final, os dados que não são mais necessários são excluídos ou destruídos. É fundamental garantir que o descarte seja realizado de maneira segura e irreversível, prevenindo a recuperação não autorizada das informações. Práticas como a destruição física de dispositivos de armazenamento e a utilização de técnicas de limpeza de dados são essenciais para garantir que os dados sejam eliminados de forma definitiva e segura.

2.4 Proteção de Dados Pessoais

A proteção dos dados pessoais é um aspecto fundamental da segurança de ativos, pois envolve o respeito aos direitos e liberdades das pessoas que confiam suas informações a uma organização. Os dados pessoais são aqueles que permitem identificar ou tornar identificável um indivíduo, como nome, endereço, e-mail, telefone, CPF, entre outros. Esses dados podem ser alvo de ataques cibernéticos, vazamentos, uso indevido ou abusivo por parte de terceiros, gerando danos morais, materiais ou reputacionais aos titulares e às organizações responsáveis pelo seu tratamento.

O tratamento de dados pessoais é toda operação realizada com esses dados, desde a coleta até a eliminação, passando pelo armazenamento, processamento, compartilhamento e transferência. Para realizar o tratamento de dados pessoais de forma segura e ética, é preciso observar os princípios e as normas estabelecidos pela legislação aplicável, como a Lei Geral de Proteção de Dados (LGPD) no Brasil1, o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei de Privacidade do Consumidor da Califórnia (CCPA) nos Estados Unidos.

2.4.1 Privacidade por Design

A privacidade por design é uma metodologia que visa garantir a proteção dos dados pessoais desde a concepção de um produto ou sistema, colocando o usuário no centro do processo. Essa metodologia consiste em integrar princípios e medidas de privacidade em todos os aspectos e fases do desenvolvimento de um produto ou sistema, assegurando que a privacidade seja um requisito fundamental e não um adicional. Aqui estão os pilares essenciais da Privacidade por Design:

- **Proatividade, não Reatividade**: Adotar medidas antecipadas e preventivas para proteger a privacidade do usuário.
- **Privacidade como Configuração Padrão**: Garantir que as configurações padrão estejam configuradas para proteger os dados do usuário.
- **Privacidade Embutida no Design**: Integrar a privacidade nas especificações e arquitetura dos sistemas e práticas.
- **Funcionalidade Total**: Manter a funcionalidade desejada sem sacrificar a privacidade.
- Segurança de Ponta a Ponta: Proteção completa ao longo do ciclo de vida dos dados.
- **Visibilidade e Transparência**: Manter a operacionalidade de maneira transparente, garantindo que as práticas de privacidade estejam verificáveis.
- **Respeito ao Interesse do Usuário**: Priorizar os interesses e necessidades do usuário em termos de privacidade.

Como exemplo, considere o desenvolvimento de uma nova aplicação móvel para serviços de saúde. Desde o início do projeto, a equipe de desenvolvimento poderia implementar medidas de "privacidade por design", como:

- **Autenticação forte**: Exigir que os usuários insiram credenciais seguras, como uma senha robusta ou autenticação de dois fatores, para acessar seus dados de saúde pessoais.
- **Criptografia**: Proteger os dados do usuário, como informações de saúde e histórico médico, usando métodos de criptografia para armazená-los de forma segura e transmiti-los com segurança através de redes.
- **Minimização de Dados**: Coletar e armazenar apenas os dados estritamente necessários para o propósito pretendido, evitando a coleta excessiva de informações pessoais.
- **Consentimento Informado**: Garantir que os usuários estejam completamente informados sobre quais dados serão coletados e como serão utilizados, e obter o consentimento claro e afirmativo deles.

Esse compromisso inicial com a privacidade facilita a criação de sistemas robustos, que salvaguardam as informações do usuário, respeitam seus direitos e fomentam a confiança desde o início, contribuindo para um ecossistema digital mais seguro e responsável.

2.4.2 Minimização de Dados

A minimização de dados é um princípio que visa garantir a proteção dos dados pessoais, restringindo o tratamento dos dados ao mínimo indispensável para a realização das finalidades pretendidas. Esse princípio é fundamental para preservar as informações do usuário, diminuindo a quantidade de dados expostos a potenciais ameaças, como vazamentos ou acessos indevidos.

- Por exemplo, ao criar um formulário online para um webinar, em vez de solicitar uma variedade de informações como nome completo, endereço, número de telefone e profissão, pode-se solicitar apenas o nome e o endereço de e-mail, que são suficientes para o registro e a participação no evento. Dessa forma, a quantidade de dados pessoais coletados e armazenados é minimizada, reduzindo a superfície de ataque em caso de um incidente de segurança.

Ao aplicar a minimização de dados, organizações e desenvolvedores devem estar constantemente questionando quais informações são realmente necessárias para a execução de uma tarefa ou serviço,

garantindo que apenas os dados essenciais sejam tratados e armazenados, contribuindo assim para a proteção da privacidade e da segurança dos dados.

A minimização de dados também está relacionada aos princípios da finalidade, da adequação e da necessidade, que estabelecem que os dados pessoais devem ser tratados para fins legítimos, específicos e explícitos; compatíveis com as finalidades informadas ao usuário; e limitados ao que for necessário em relação às finalidades.

2.4.3 Consentimento Informado

O consentimento informado é um direito fundamental dos usuários na gestão ética de dados pessoais, baseado na obtenção de autorização expressa e bem informada dos usuários para o tratamento de suas informações. Esse direito é centrado na transparência e no empoderamento dos usuários, permitindo que tenham controle efetivo sobre como suas informações serão coletadas, processadas e utilizadas.

- Por exemplo, ao se inscrever em um serviço online, o usuário deve receber informações claras e completas sobre como seus dados serão utilizados, incluindo as finalidades, os destinatários, os riscos e os direitos do usuário. Se um site deseja utilizar os dados do usuário para fins de marketing, ele deve informar isso de maneira clara e acessível, dando ao usuário a opção de aceitar ou recusar. Se o usuário concordar, seu consentimento deve ser ativamente dado, como, por exemplo, através do clique em um botão que diga “Concordo”.

Importante ressaltar que o consentimento informado deve ser tão fácil de ser retirado quanto foi concedido, garantindo ao usuário flexibilidade e controle contínuo sobre suas informações. Dessa maneira, o direito ao consentimento informado reforça o respeito pela autonomia dos usuários e contribui para construir um ambiente digital mais seguro e confiável.

2.4.4 Direito ao Esquecimento

O direito ao esquecimento é um direito que assegura a autonomia dos indivíduos sobre seus dados pessoais em ambientes digitais. Esse direito permite que pessoas solicitem a eliminação ou a

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

desindexação de suas informações pessoais de websites, bancos de dados ou serviços online, garantindo que possam exercer controle contínuo sobre a visibilidade e o uso de suas informações.

Esse direito está previsto no artigo 18 da LGPD, que estabelece os direitos dos titulares dos dados pessoais. Segundo a LGPD, os titulares têm o direito de solicitar a eliminação dos seus dados pessoais quando:

- Os dados não forem mais necessários para a finalidade que motivou a sua coleta;
- Os titulares retirarem o seu consentimento para o tratamento dos dados;
- O tratamento dos dados foi baseado exclusivamente no consentimento do titular e não houver outro fundamento legal;
- O tratamento dos dados for ilícito;
- Os dados foram tratados com base no legítimo interesse do controlador ou de terceiro e o titular se opôs à sua continuidade.

No entanto, o direito ao esquecimento não é absoluto e pode ser limitado por outros direitos e interesses, como a liberdade de expressão e informação, o cumprimento de obrigações legais ou regulatórias, a realização de atividades de interesse público ou a defesa de direitos em processos judiciais.

- Por exemplo, considere uma pessoa que tenha participado de um fórum online ou rede social e compartilhado informações pessoais ou opiniões em um momento específico. Se, por qualquer motivo, ela decidir posteriormente que não quer mais que essas informações estejam disponíveis publicamente, ela pode solicitar ao controlador do site que elimine tais dados, apoiando-se no direito ao esquecimento. No entanto, se essas informações tiverem relevância pública ou histórica, ou se forem necessárias para garantir o exercício da liberdade de expressão e informação de outras pessoas, o controlador do site pode negar o pedido de eliminação.

Esse direito é particularmente relevante em casos de informações desatualizadas ou irrelevantes, que podem continuar a afetar a reputação e a privacidade do indivíduo se permanecerem acessíveis. Ao permitir que os titulares tenham um papel ativo na gestão de suas informações online, o direito ao

esquecimento é uma ferramenta essencial para a proteção da privacidade e da dignidade pessoal no contexto digital.

2.4.5 Portabilidade dos Dados

A portabilidade dos dados é um direito que assegura aos usuários maior controle e autonomia sobre suas informações pessoais, permitindo que transfiram seus dados entre diferentes sistemas ou serviços de maneira segura, organizada e sem comprometer a integridade das informações. Esse direito não apenas promove a liberdade de escolha do usuário, mas também estimula a competição e inovação entre os serviços, uma vez que facilita a mudança entre diferentes plataformas conforme as preferências e necessidades dos usuários.

A portabilidade dos dados está relacionada ao conceito de interoperabilidade, que é a capacidade de sistemas ou serviços de se comunicarem e trocarem dados de forma eficiente e padronizada. Para que a portabilidade dos dados seja possível, é preciso que os dados sejam armazenados e transmitidos em formatos estruturados, comuns e legíveis por máquina, como XML ou JSO. Além disso, é preciso que os sistemas ou serviços adotem protocolos e interfaces abertas e compatíveis, que permitam a integração e a comunicação entre eles.

- Vamos considerar um exemplo prático para ilustrar esse direito: Suponha que uma pessoa use um aplicativo de monitoramento de saúde e bem-estar para rastrear seus exercícios, nutrição e padrões de sono. Após alguns anos, um novo aplicativo com funcionalidades mais avançadas e uma interface de usuário melhorada é lançado no mercado. Com o direito à portabilidade dos dados, o usuário pode facilmente transferir todos os seus dados históricos de saúde e bem-estar do aplicativo antigo para o novo aplicativo, permitindo-lhe continuar monitorando suas atividades sem perder informações valiosas acumuladas ao longo do tempo.

Esse direito, portanto, oferece aos usuários a flexibilidade necessária para mudar para serviços que considerem mais adequados às suas necessidades, sem o obstáculo de perder o acesso ou o controle sobre suas informações pessoais previamente compartilhadas ou armazenadas. A portabilidade dos dados também beneficia os provedores de serviços, pois incentiva a melhoria contínua da qualidade

e da segurança dos seus sistemas ou serviços, aumentando a satisfação e a fidelização dos seus usuários.

2.4.6 Melhores Práticas para Proteger Dados Pessoais

A proteção dos dados pessoais é um desafio constante no cenário atual, onde as ameaças cibernéticas são cada vez mais sofisticadas e frequentes. Para garantir a segurança e a privacidade dos dados pessoais, é preciso adotar uma série de boas práticas que envolvem aspectos técnicos, organizacionais e humanos. Algumas dessas boas práticas são:

- **Criptografia**: A criptografia é essencial para a segurança dos dados, ajudando a proteger as informações tanto quando estiverem armazenadas (dados em repouso) quanto durante transmissões (dados em trânsito). É como colocar um cadeado robusto nos dados, só que quem tem a chave são os sistemas autorizados e usuários. Exemplo: Ao salvar informações pessoais de um usuário em um banco de dados, essas informações são criptografadas, tornando-se inacessíveis para quem não possui a chave de descriptografia.
- **Controle de Acesso**: O controle de acesso é a linha de defesa que restringe o acesso a dados apenas a usuários e sistemas autorizados. Exemplo: Um sistema de saúde pode permitir que apenas médicos e enfermeiros tenham acesso a registros médicos completos, enquanto a recepção tem acesso limitado.
- **Auditoria e Monitoramento**: Essas práticas envolvem o rastreamento, registro e revisão de atividades dentro dos sistemas para identificar e reagir a ações suspeitas rapidamente. Exemplo: Se um empregado acessa uma grande quantidade de registros de clientes sem um motivo claro, um sistema de monitoramento pode alertar os administradores.
- **Atualizações e Patches de Segurança**: Manter os sistemas e aplicativos atualizados é crucial. Patches corrigem vulnerabilidades, ajudando a proteger os dados contra ameaças novas e emergentes. Exemplo: Um sistema operacional lançou uma atualização. Aplicá-la prontamente ajuda a proteger o sistema contra malwares que exploram vulnerabilidades.
- **Educação e Conscientização**: A educação contínua ajuda as equipes a entender as melhores práticas de segurança, conscientizando sobre os riscos e as maneiras de prevenir incidentes de

segurança. Exemplo: Realizar workshops regulares para educar os funcionários sobre os tipos de phishing e como evitar tais ataques.

Implementando essas melhores práticas, é possível criar uma fundação sólida para a proteção de dados pessoais, promovendo um ambiente onde a privacidade dos indivíduos é priorizada e mantida segura.

2.5 Políticas de Backup e Armazenamento

No ecossistema robusto de segurança da informação, as políticas e procedimentos de backup e armazenamento assumem uma posição de destaque, funcionando como pilares no alicerce de proteção dos ativos informacionais de uma organização. Eles desempenham papéis cruciais na preservação, recuperação e eliminação segura de dados, assegurando assim sua disponibilidade, integridade e confidencialidade.

2.5.1 Objetivos e Responsabilidades

As políticas de backup e armazenamento devem ser definidas com base em objetivos claros e mensuráveis, que reflitam as necessidades e prioridades da organização em relação à proteção dos dados. Uma estrutura de responsabilidades deve ser estabelecida, atribuindo indivíduos ou equipes específicas para gerenciar e executar os processos de backup, recuperação e eliminação de dados, de acordo com as melhores práticas e os requisitos legais. Ao garantir que cada etapa esteja sob a supervisão de partes claramente identificadas e qualificadas, podemos promover uma execução eficiente e consistente, reduzindo assim a probabilidade de ocorrerem erros e inconsistências.

A atribuição de responsabilidades contribui para uma operacionalização mais ágil e integrada, garantindo que todas as tarefas essenciais sejam realizadas com rigor e precisão. Isso não apenas fortalece a integridade do processo como um todo, mas também facilita a rápida identificação e correção de qualquer anomalia ou falha que possa surgir, melhorando assim a resiliência e confiabilidade das práticas de backup e armazenamento.

2.5.2 Requisitos Legais, Regulatórios e Contratuais

Para garantir que as políticas e procedimentos de backup e armazenamento estejam adequados e seguros, eles precisam estar em conformidade com as leis, regulamentos e contratos aplicáveis. Essa conformidade não apenas assegura que a organização esteja operando dentro da legalidade, mas também reforça a ética e a integridade na gestão das informações e ativos da organização.

A maneira como os dados e informações são mantidos e, eventualmente, descartados, precisa ser cuidadosamente planejada e executada. Primeiro, a decisão sobre quanto tempo manter os dados deve considerar seu valor e utilidade para a organização, bem como os requisitos legais, regulatórios e contratuais que podem afetar a retenção e o descarte dos dados.

- **Retenção**: Os dados devem ser mantidos enquanto forem úteis e relevantes, considerando também os requisitos legais e operacionais. Alguns exemplos de requisitos legais e regulatórios que podem determinar o período de retenção dos dados são: a Lei Geral de Proteção de Dados (LGPD) no Brasil, o General Data Protection Regulation (GDPR) na União Europeia, o Health Insurance Portability and Accountability Act (HIPAA) nos Estados Unidos e o ISO 27001:2022 Annex A 5.344. Alguns exemplos de requisitos contratuais que podem determinar o período de retenção dos dados são: acordos de nível de serviço (SLAs), termos de uso, políticas de privacidade e contratos com clientes ou fornecedores.
- **Descarte**: Quando os dados não são mais necessários, o processo de descarte deve ser seguro e definitivo, prevenindo a possibilidade de recuperação ou acesso não autorizado após a eliminação. É crucial garantir que os métodos utilizados para o descarte estejam alinhados com as melhores práticas e políticas de segurança, garantindo a proteção contínua da informação até seu descarte final. Alguns exemplos de métodos de eliminação segura dos dados são: sobregravação, degaussing e destruição física.

As políticas e procedimentos de backup e armazenamento são essenciais para a segurança dos ativos de informação, pois permitem preservar e recuperar os dados em caso de necessidade, bem como eliminar os dados que não são mais relevantes ou legais para a organização. As políticas e procedimentos devem ser revisados periodicamente e testados regularmente para garantir a sua eficácia e conformidade.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

2.5.3 Retenção e Descarte de Ativos

A gestão estratégica de retenção e descarte de ativos é vital para a segurança, a confidencialidade e a disponibilidade das informações de uma organização. Esta seção se concentra na criação de protocolos seguros e eficazes para a manutenção e eliminação de dados. Aqui estão as considerações essenciais para uma prática robusta de retenção e descarte:

- **Planejamento Estratégico de Retenção**: A decisão de quanto tempo reter os dados deve ser cuidadosamente calculada, levando em conta o valor do negócio dos dados, sua relevância e aplicabilidade no decorrer do tempo. Cada tipo de dado deve ser avaliado individualmente para determinar o período de retenção adequado, considerando também os requisitos legais, regulatórios e contratuais que podem afetar a retenção e o descarte dos dados.
- **Critérios de Retenção**: A retenção de dados deve ser baseada em critérios claramente definidos, como requisitos legais, relevância operacional e importância estratégica. A política de retenção deve ser revisada regularmente para assegurar que permaneça alinhada com as necessidades e objetivos organizacionais.
- **Processo de Descarte**: Quando os dados não são mais necessários ou atingem o fim do seu ciclo de vida útil, devem ser descartados de maneira segura e irreversível. O descarte deve garantir que os dados sejam completamente inacessíveis e irrecuperáveis, evitando riscos de vazamento ou acesso não autorizado.
- **Técnicas de Descarte**: Utilizar métodos de eliminação que garantam a destruição completa e irrecuperável dos dados. Isso pode incluir a sobregravação de dados, destruição física de dispositivos de armazenamento, ou utilização de soluções de descarte certificadas e seguras.
- **Documentação e Auditoria**: Manter registros precisos dos processos de retenção e descarte. Estes registros devem incluir detalhes como o tipo de dado, razão para retenção ou descarte, e métodos utilizados no descarte. Esta documentação é essencial para fins de auditoria e conformidade.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

Incorporando essas práticas, as organizações podem assegurar que seus dados sejam mantidos de maneira segura pelo tempo necessário e descartados de maneira eficaz e segura quando não forem mais necessários.

2.5.4 Técnicas de Eliminação Segura

A eliminação segura dos dados é um requisito fundamental para a proteção da privacidade e da confidencialidade das informações. Diversas técnicas podem ser empregadas para assegurar que os dados sejam irrecuperavelmente apagados, dependendo da natureza dos dados e do meio em que estão armazenados. Aqui estão algumas das técnicas principais:

- **Sobregravação:** Esse método consiste em substituir os dados originais por dados aleatórios ou padrões predefinidos, repetindo o processo várias vezes para dificultar a recuperação dos dados. É uma técnica comumente utilizada em meios de armazenamento regraváveis, como discos rígidos ou unidades flash. A sobregravação pode ser feita por software ou hardware específicos.
- **Degaussing:** Esse processo consiste em aplicar um campo magnético intenso sobre o meio de armazenamento magnético (como fitas ou discos rígidos), alterando ou apagando os dados gravados. O degaussing pode ser feito por dispositivos chamados degaussers. Essa técnica também pode danificar o meio de armazenamento, tornando-o inoperante ou ilegível.
- **Destruição física:** Uma forma definitiva de garantir que os dados não sejam recuperados, destruindo fisicamente o meio de armazenamento (como discos rígidos ou CDs). A destruição física pode ser feita por métodos como perfuração, trituração, incineração ou fragmentação. Essa técnica requer cuidados especiais para evitar riscos ambientais ou de segurança.

A aplicação dessas técnicas deve ser meticulosamente planejada e documentada para garantir que a eliminação dos dados seja irreversível, protegendo assim contra qualquer tentativa de recuperação não autorizada.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

2.5.5 Políticas de Backup

As políticas de backup são essenciais para a preservação e a segurança dos dados, e devem ser estruturadas de maneira criteriosa e abrangente. Aqui estão os elementos que essas políticas deveriam abranger:

- **Frequência**: Estabelecer quão frequentemente os backups devem ser realizados, se serão diários, semanais, mensais ou baseados em outro cronograma, conforme a necessidade e a natureza dos dados. A frequência dos backups deve considerar o volume, a criticidade e a variabilidade dos dados, bem como o tempo de recuperação aceitável em caso de perda.
- **Métodos**: Identificar quais métodos serão usados para o backup, como cópias integrais, diferenciais ou incrementais, escolhendo o que melhor atenda às necessidades específicas da organização. Os métodos de backup devem considerar o desempenho, a eficiência e a confiabilidade do processo, bem como o espaço de armazenamento disponível.
- **Formatos**: Determinar em quais formatos os backups serão salvos, garantindo que possam ser recuperados eficientemente quando necessário. Os formatos de backup devem considerar a compatibilidade, a portabilidade e a segurança dos dados, bem como as possíveis mudanças tecnológicas que possam afetar a recuperação dos dados.
- **Processo Metódico**: Assegurar que o processo de backup seja realizado de maneira sistemática e metódica, para garantir a integridade e a consistência dos dados e facilitar a restauração em casos de falha, corrupção ou perda dos dados primários. O processo de backup deve seguir um plano pré-definido e documentado, que especifique os objetivos, as responsabilidades, as etapas, os recursos e os testes do processo.
- **Armazenamento Seguro**: Garantir que as cópias de backup estejam armazenadas de maneira segura, protegidas contra acessos não autorizados, danos físicos ou qualquer outra forma de comprometimento. O armazenamento seguro deve seguir o princípio da redundância (ter mais de uma cópia dos dados), da diversidade (usar mais de um tipo de meio de armazenamento) e da dispersão (manter as cópias em locais diferentes).

Ao considerar esses aspectos nas políticas de backup, você estará promovendo uma estratégia sólida que contribui para a resiliência e a segurança da informação dentro da organização.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

2.5.6 Melhores Práticas de Armazenamento de Dados

O armazenamento de dados é uma fase crucial na gestão da informação, e deve ser conduzida com cuidado e rigor para assegurar a segurança e a qualidade dos dados. Aqui estão algumas práticas recomendadas para um armazenamento de dados seguro e eficiente:

- **Soluções de Segurança**: Implementar tecnologias robustas, como criptografia, para proteger os dados armazenados contra acessos não autorizados e outras ameaças. A utilização de protocolos de segurança avançados é essencial para garantir que os dados estejam sempre protegidos, independentemente do meio ou do local de armazenamento
- **Armazenamento em Nuvem**: Considerar o uso de soluções de armazenamento em nuvem confiáveis, que possuam robustas medidas de segurança, para proporcionar uma maior flexibilidade e escalabilidade. O armazenamento em nuvem pode oferecer benefícios como redução de custos, aumento de disponibilidade e facilidade de acesso
- **Políticas de Acesso**: Definir e implementar políticas rigorosas de acesso aos dados, garantindo que somente indivíduos autorizados possam acessar as informações. As permissões devem ser concedidas com base na relevância e na necessidade de acesso para realizar funções específicas, seguindo o princípio do menor privilégio .
- **Classificação de Dados**: Implementar uma política de classificação de dados que identifique e categorize os dados com base na sua sensibilidade e importância. Isso auxiliará na aplicação de controles de segurança apropriados e na tomada de decisões relativas às políticas de acesso, retenção e descarte.
- **Monitoramento e Auditoria**: Implementar ferramentas e práticas de monitoramento e auditoria para acompanhar e revisar o acesso e as atividades relacionadas aos dados armazenados, garantindo um ambiente de dados seguro e em conformidade com as políticas organizacionais e regulamentações pertinentes .

Adotando essas melhores práticas, a organização pode maximizar a segurança dos dados armazenados, assegurando uma base sólida para a gestão de informações e a operação contínua e eficiente dos processos de negócios.

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

Centro Administrativo Governador Virgílio Távora
Av. Gal. Afonso Albuquerque Lima, s/n - Cambeba
CEP: 60822-325 • Fortaleza/CE
CNPJ nº 07.954.514/0001-25

Referências

BITRIX24. **O guia definitivo de estratégia de resposta a riscos.** Disponível em: https://www.bitrix24.com.br/articles/o-guia-definitivo-de-estrategia-de-resposta-a-riscos.php. Acesso em: 11 dez. 2023.

BRASIL. Ministério da Cidadania. **Guia de boas práticas para adequação à Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 2020. Disponível em: https://www.mds.gov.br/webarquivos/MDS/1_Acesso_a_Informacao/Privacidade_e_Protecao_de_Dados/LGPD/Arquivos/Guia_de_boas_praticas_LGPD.pdf. Acesso em: 11 dez. 2023.

CERTIFIQUEI. **Titular de dados pessoais: o que é e quais são seus direitos?**. Disponível em: https://www.certifiquei.com.br/titular-dados-pessoais/. Acesso em: 11 dez. 2023.

ECO IT. **Política de backup: o que é e como fazer na sua empresa**. Disponível em: https://blog.ecoit.com.br/politica-de-backup/. Acesso em: 11 dez. 2023.

EXPERT LGPD. **LGPD e a responsabilidade das empresas na proteção de dados pessoais**. Disponível em: https://expertlgpd.com/lgpd-e-a-responsabilidade-das-empresas-na-protecao-de-dados-pessoais/. Acesso em: 11 dez. 2023.

GAEA. **Mitigação de riscos: o que é e como fazer na sua empresa**. Disponível em: https://gaea.com.br/mitigacao-de-riscos/. Acesso em: 11 dez. 2023.

IBM. **Data lifecycle management: o que é e como funciona**. Disponível em: https://www.ibm.com/br-pt/topics/data-lifecycle-management. Acesso em: 11 dez. 2023.

INVESTOPEDIA. **What is the difference between tangible and intangible assets?**. Disponível em: https://www.investopedia.com/ask/answers/012815/what-difference-between-tangible-and-intangible-assets.asp. Acesso em: 11 dez. 2023.

MACHER TECNOLOGIA. **O que é data minimization ou minimização de dados (LGPD)**. Disponível em: https://www.machertecnologia.com.br/o-que-e-data-minimization-ou-minimizacao-de-dados-lgpd/. Acesso em: 11 dez. 2023.

MARCELJM. **Segurança da informação: conformidade**. Disponível em: https://marceljm.com/seguranca-da-informacao/conformidade/. Acesso em: 11 dez. 2023.

MARCELJM. **Segurança da informação: níveis de classificação da informação**. Disponível em: https://marceljm.com/seguranca-da-informacao/niveis-de-classificacao-da-informacao/. Acesso em: 11 dez. 2023.

ONETRUST. **Privacidade por design: o que é e como aplicar na sua empresa**. Disponível em: https://www.onetrust.com/br/blog/privacidade-por-design/. Acesso em: 11 dez. 2023.

SPIEGATO. **O que faz um custodiante de dados?**. Disponível em: https://spiegato.com/pt/o-que-faz-um-custodiante-de-dados. Acesso em: 11 dez. 2023.

VIANNA, William Barbosa; VIANNA, Marco Antonio Carvalho. **Segurança da informação: uma análise sob a ótica da gestão do conhecimento**. Perspectivas em Ciência da Informação, Belo Horizonte, v. 12, n. 3, p. 168-185, set./dez. 2007. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/. Acesso em: 11 dez. 2023.