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

1.5 Regulamentações e Conformidades

Na era digital, a informação não apenas circula com velocidade e amplitude inéditas, mas também assume um papel central como ativo estratégico para organizações. À medida que a dependência de dados cresce, a imperatividade de garantir sua integridade, confidencialidade e disponibilidade se torna uma preocupação primordial. Neste contexto, diversos países e organizações supranacionais têm estabelecido rigorosas regulamentações visando assegurar a proteção de informações. Adotar e aderir a estas diretrizes não é somente uma obrigação jurídica, mas um imperativo ético e um sinal de comprometimento com padrões elevados, fortalecendo laços de confiança com stakeholders e blindando ativos de incalculável valor.

1.5.1 Importância da Conformidade Regulatória

Cumprir as regras não é apenas seguir à risca o que a lei diz. Claro, ninguém quer levar multas ou ser penalizado, e isso já é um bom motivo para ficar de olho nas normas. Mas, seguir as regras tem benefícios ainda maiores para as empresas:

- **Integridade Corporativa**: Quando uma empresa mostra que leva a sério as regras de segurança da informação, ela passa mais confiança. Isso faz com que ela se destaque num mercado onde todos estão buscando empresas em que possam confiar.
- **Blindagem Proativa**: Muitas dessas regras são baseadas no que há de melhor e mais moderno em segurança. Seguindo-as, a empresa fica mais protegida contra problemas que já conhecemos e até contra os que ainda vão aparecer.
- **Visão Integrada**: Quando toda a empresa se envolve e entende a importância das regras, a segurança da informação deixa de ser vista como uma chateação e passa a ser parte do jeito de trabalhar da empresa.
- **Consolidação da Confiança**: Quando os clientes e parceiros veem que a empresa segue regras rigorosas de segurança, eles sentem que suas informações estão em boas mãos. Isso fortalece a relação com eles e faz com que confiem ainda mais na empresa.

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

1.5.2 Principais Leis em Segurança da Informação

À medida que a tecnologia avança e a quantidade de dados que compartilhamos online aumenta, a preocupação com a privacidade e segurança da informação cresce em paralelo. Em resposta, vários países e organizações estabeleceram regras específicas para garantir a proteção desses dados. Aqui estão algumas das principais:

- **GDPR (Regulamento Geral sobre a Proteção de Dados)**: GDPR (General Data Protection Regulation): É o regulamento europeu sobre proteção de dados pessoais, que entrou em vigor em 2018. Ele se aplica a todas as organizações que oferecem bens ou serviços aos cidadãos da União Europeia, ou que monitoram seu comportamento online. O GDPR estabelece princípios como transparência, consentimento, limitação de finalidade, minimização de dados, qualidade dos dados, segurança dos dados, responsabilidade e prestação de contas. As organizações que não cumprirem o GDPR podem sofrer multas de até 20 milhões de euros ou 4% do faturamento global anual.
- **HIPAA (Health Insurance Portability and Accountability Act)**: É a lei americana sobre proteção de dados pessoais na área da saúde, que entrou em vigor em 1996. Ela se aplica a todas as organizações que lidam com informações médicas protegidas (PHI), como planos de saúde, prestadores de serviços médicos e entidades administrativas. O HIPAA estabelece normas para garantir a privacidade, a segurança e a portabilidade dos dados de saúde dos indivíduos. As organizações que não cumprirem o HIPAA podem sofrer multas de até 1,5 milhão de dólares por ano, ou até 50 mil dólares por violação.
- **PCI DSS (Padrão de Segurança de Dados para a Indústria de Cartões de Pagamento)**: É o padrão de segurança para a indústria de cartões de pagamento, que foi criado em 2004 por um consórcio formado pelas principais bandeiras de cartão do mundo. Ele se aplica a todas as organizações que armazenam, processam ou transmitem dados de cartão de crédito ou débito. O PCI DSS estabelece requisitos para garantir a segurança dos dados dos portadores de cartão e prevenir fraudes. As organizações que não cumprirem o PCI DSS podem sofrer multas, sanções ou perda da capacidade de aceitar cartões.

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

- **LGPD (Lei Geral de Proteção de Dados)**: É a lei brasileira sobre proteção de dados pessoais, que entrou em vigor em 2020. Ela se aplica a todas as organizações que realizam operações de tratamento de dados pessoais no Brasil, ou que oferecem bens ou serviços aos titulares dos dados no Brasil, ou que tratam dados coletados no Brasil. A LGPD estabelece princípios como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança dos dados, prevenção, não discriminação e responsabilização. As organizações que não cumprirem a LGPD podem sofrer multas de até 50 milhões de reais ou 2% do faturamento bruto anual.

Essas são apenas algumas das regulamentações existentes em segurança da informação e proteção de dados. Há outras que se aplicam a setores específicos, como o financeiro, o energético, o governamental, etc. Além disso, há normas e padrões voluntários que podem servir como referência para as boas práticas em segurança da informação, como a ISO/IEC 27001, a NIST SP 800-53, o COBIT, o ITIL, etc.

Para se manter em conformidade com as regulamentações aplicáveis, as organizações devem estar atentas às mudanças no cenário legal e regulatório, bem como às expectativas dos clientes e da sociedade. Além disso, devem adotar uma cultura de segurança da informação que permeia todos os níveis da organização, desde a alta direção até os colaboradores operacionais.

1.6 Treinamento e Conscientização

Num mundo cada vez mais digitalizado, as falhas de segurança da informação muitas vezes não vêm das ferramentas tecnológicas, mas sim das pessoas que as utilizam. Dessa forma, treinar e conscientizar as equipes é fundamental para garantir a segurança das informações no ambiente corporativo.

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

1.6.1 Importância do Treinamento em Segurança

Mesmo com as tecnologias de segurança mais avançadas, o comportamento humano pode ser a porta de entrada para problemas. Entender por que o treinamento é essencial pode fazer toda a diferença:

- **Diminuição de Falhas Simples**: Acredite, muitos problemas começam com ações básicas: um clique descuidado em um e-mail duvidoso ou uma senha fácil de adivinhar. Treinar as pessoas reduz esses deslizes.
- **Estar Pronto para Desafios Futuros**: O mundo digital muda rápido e os "mal-intencionados" se reinventam. Treinamentos recorrentes preparam as equipes para novidades nesse jogo de "gato e rato".
- **Criar uma Mentalidade de Segurança**: A segurança não deve ser preocupação só da equipe de TI. Quando todos se sentem responsáveis, a empresa se torna um lugar mais seguro.

1.6.2 Estratégias para Capacitar e Conscientizar os Colaboradores

Existem diversas formas de educar e sensibilizar as pessoas sobre a importância da segurança da informação e como agir de forma segura no dia a dia. Algumas das estratégias mais eficazes são:

- **Testes Práticos**: Simular ataques, como tentativas de phishing, ajuda a equipe a entender na prática como essas ameaças funcionam. É como um treino: quanto mais você pratica, melhor fica em reconhecer e evitar problemas.
- **Encontros e Palestras**: Criar momentos de aprendizado coletivo, como palestras ou rodas de conversa, é super válido. Chamar um especialista para compartilhar experiências ou até mesmo fazer uma sessão de dúvidas pode esclarecer muitos pontos.
- **Materiais de Apoio Online**: Ter à disposição guias, vídeos ou cursos na internet é ótimo porque cada um pode estudar quando e como quiser. E se surgir uma dúvida mais tarde? É só voltar e revisar.

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

- **Retorno sobre o Aprendizado**: Depois de qualquer formação, é bom saber como foi, certo? Dizer aos colaboradores o que mandaram bem ou onde podem melhorar ajuda no crescimento de todos.

Finalizando, na segurança da informação, estar bem informado é tão importante quanto ter boas ferramentas de proteção. Por isso, investir na capacitação e na conscientização das pessoas é um passo fundamental para tornar a empresa mais segura e preparada para os desafios digitais.

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.

CONTACTA. **Importância do treinamento de segurança da informação nas empresas**. Disponível em: https:/contacta.com.br/importancia-do-treinamento-de-seguranca-da-informacao-nas-empresas/. Acesso em: 11 dez. 2023.

CHAPPLE, M.; STEWART, J. M.; GIBSON, D. **(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide**. [S. l.]: Wiley & Sons, Limited, John, 2021. 1248 p. ISBN 9781119786238.

FERREIRA, Douglas Favaro. **Análise de riscos em segurança da informação: uma abordagem baseada em processos**. 2015. 76 f. Trabalho de Conclusão de Curso (Bacharelado em Tecnologia da Informação) - Faculdade de Tecnologia de São Paulo, São Paulo, 2015. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/904/1/20152S_FERREIRADouglasFavaro_CD2454.pdf. 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.

GESTÃO DE SEGURANÇA PRIVADA. **Risco de segurança: o que é, tipos e exemplos**. Disponível em: https://gestaodesegurancaprivada.com.br/risco-de-seguranca-o-que-e-tipos-e-exemplos/. Acesso em: 11 dez. 2023.

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

RUST, Cristiano. **Segurança da informação: conceitos e práticas para a proteção dos ativos de informação nas organizações**. 2007. 114 f. Dissertação (Mestrado em Engenharia de Sistemas e Computação) - Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2007. Disponível em: http://www.nce.ufrj.br/labnet/Rust/VersãoFinal.pdf. Acesso em: 11 dez. 2023.

SITEWARE. **O que é uma ameaça em segurança da informação?**. Disponível em: https://www.siteware.com.br/blog/seguranca/o-que-e-uma-ameaca-em-seguranca-da-informacao/. Acesso em: 11 dez. 2023.