Desmistificando a conformidade normativa

para líderes de segurança
e tomadores de decisão de TI

Introdução

O desenvolvimento de marcos regulatórios e padrões surgiu da necessidade de enfrentar os desafios e requisitos na gestão da tecnologia da informação e na proteção de dados. Essas estruturas e padrões não apenas evoluíram com o tempo, mas também foram moldados pelos avanços tecnológicos e pelas novas ameaças de segurança cibernética. O desenvolvimento de estruturas e padrões tem sido impulsionado principalmente pelos seguintes fatores:

- **Os órgãos reguladores** estão destacando a importância de as organizações assumirem a responsabilidade por suas práticas de segurança cibernética e atenderem aos padrões e regulamentos estabelecidos.
- **Ameaças cibernéticas avançadas** estão se tornando mais frequentes e prejudiciais. Frequentemente, essa sofisticação, que antes se restringia às ameaças apoiadas por Estados, agora está nas mãos de oportunistas e hacktivistas.
- **Infraestruturas críticas e serviços essenciais** (por exemplo, cuidados de saúde, energia, finanças) que são vitais para o funcionamento da sociedade e da economia. Isso inclui a legislação federal, como a Cyber Incident Reporting for Critical Infrastructure Act (CIRCA, Lei de Relatório de Incidentes Cibernéticos para Infraestrutura Crítica), de março de 2022.
- **Falta de uniformidade** nas práticas de cibersegurança em diferentes setores e regiões. Abordagens inconsistentes podem levar a lacunas na segurança e desafios de conformidade**.**
- **A ordem executiva** sobre a melhoria da segurança cibernética do país que foi aprovada pelo presidente dos Estados Unidos em maio de 2021.

Está claro que as organizações precisam ser resilientes diante de ameaças virtuais, garantindo que possam continuar operando e se recuperando rapidamente de interrupções. Com o aumento da coleta e processamento de dados pessoais, surge uma necessidade ainda maior de proteger essas informações contra ameaças virtuais e vazamentos de dados. Os incidentes cibernéticos não apenas causam um impacto econômico considerável, resultando em perdas financeiras e prejudicando a confiança nos serviços digitais, afetando a economia como um todo, mas, em alguns casos, podem até levar à perda de vidas, especialmente quando o setor de saúde é atingido.

A conformidade normativa é essencial para desenvolver a resiliência organizacional. As empresas que entendem a totalidade de seus riscos sabem que a conformidade não é apenas uma tarefa para cumprir requisitos, mas sim uma componente essencial de uma estratégia de segurança abrangente. Ao seguir os regulamentos e adotar as melhores práticas de segurança, as organizações conseguem se preparar de maneira mais eficaz para resistir e se recuperar rapidamente de incidentes cibernéticos. Esta abordagem garante que, quando uma crise chega, as bases para uma recuperação rápida já estão estabelecidas.

1.

Ataques virtuais

Se a infraestrutura digital de uma empresa estiver sob ataque, os efeitos podem ir muito além da simples perda de dados. Os impactos de um incidente cibernético podem incluir o tempo de inatividade, a perda de funções essenciais, possíveis interrupções nas vendas e a forma como a empresa é vista pelo público.

Na esteira dessas possibilidades, o impacto na vida humana é o fator mais importante a se ter em mente. Nos setores de serviços financeiros (FSI) e de saúde (HC), as ameaças cibernéticas podem ter impactos que alteram a vida em níveis individuais, com impacto em contas, pagamentos e acesso a cuidados médicos, entre outros serviços críticos. Preocupações e riscos como esses são um bom motivo para as organizações melhorarem sua postura de segurança ao seguirem a conformidade em suas regulamentações do setor.

Por que a conformidade é importante

A conformidade envolve a adesão a leis e regulamentos que se aplicam ao setor e à geografia da organização. Estar em conformidade pode ajudar a minimizar o impacto nos negócios, desde a perda de receita por pagamentos de resgate até interrupções operacionais, riscos de violações de dados, multas regulatórias e prejuízos à reputação. Os padrões de conformidade estão mudando rapidamente e continuarão mudando. Os regulamentos criados para atender aos objetivos atuais podem não ser eficazes no futuro. Manter-se atualizado com as novas estruturas e regulamentos, assim como suas expectativas, é uma maneira certeira de proteger sua organização.

Regulamentos x Estruturas

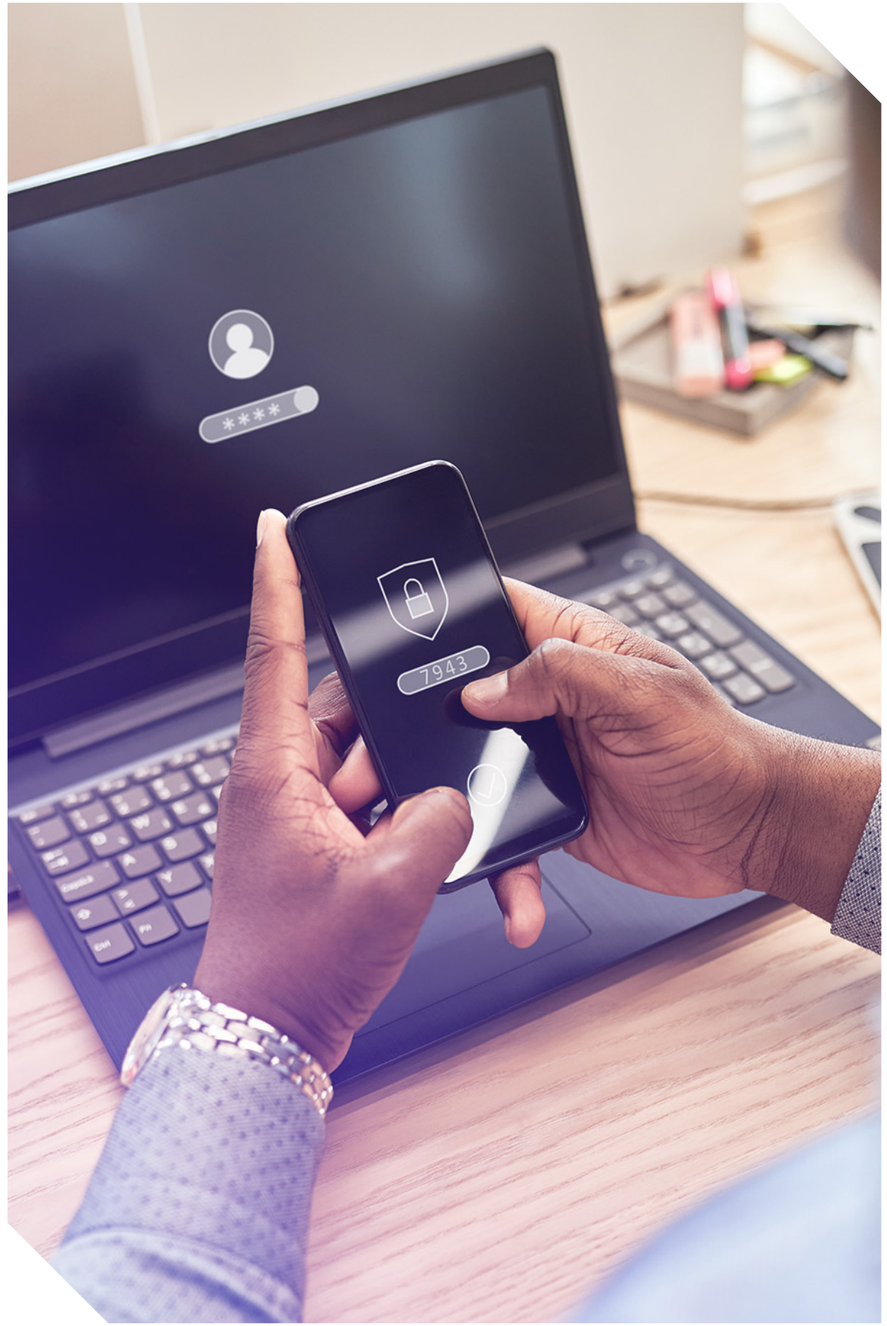
A principal diferença entre regulamentos e estruturas é o que você está tentando realizar. As estruturas fornecem um conjunto estruturado de diretrizes, práticas recomendadas e padrões que as organizações podem usar para gerenciar e melhorar sua postura de segurança cibernética. As regulamentações são exigências legais estabelecidas por governos ou entidades reguladoras para garantir que todas as organizações adotem um padrão mínimo de práticas de segurança cibernética. Alguns regulamentos amplamente utilizados incluem:

- **GDPR** (Regulamento Geral de Proteção de Dados) — Regulamento da União Europeia para proteção de dados e privacidade.
- **HIPAA** (Lei de Portabilidade e Responsabilidade do Seguro de Saúde) — Regulamentação dos EUA para proteção de informações de assistência médica.
- **SOX** (Lei Sarbanes-Oxley) — Regulamentação dos EUA para práticas financeiras e governança corporativa.
- **PCI DSS** (Padrão de Segurança de Dados da Indústria de Cartões de Pagamento) — Padrões para proteger transações com cartão de crédito.
- **FISMA** (Lei Federal de Gestão de Segurança da Informação) — Lei dos EUA para proteger informações governamentais.

Regulamentos como esses funcionam em conjunto com estruturas. Por exemplo, as estruturas fornecem a base para a conformidade com os regulamentos, e os regulamentos impulsionam a adoção de estruturas. As estruturas auxiliam as organizações a ultrapassarem os requisitos normativos mínimos, facilitando a conformidade e a auditoria, enquanto as regulamentações asseguram um padrão básico de segurança consistente em todos os setores. Algumas estruturas amplamente utilizadas incluem:

- **NIST Cybersecurity Framework (CSF)** — Fornece uma abordagem abrangente para gerenciar riscos de cibersegurança.
- **Controles CIS** — Um conjunto de melhores práticas para se defender contra ameaças virtuais.
- **COBIT** — Fornece uma estrutura para gerenciamento e governança de TI, com um forte foco em objetivos de controle para TI, incluindo segurança cibernética.

As estruturas oferecem as melhores práticas para a gestão da segurança cibernética, enquanto as regulamentações estabelecem padrões mínimos para garantir a segurança essencial em todos os setores.



Gestão de riscos e conformidade

Uma abordagem orientada pelo risco começa com uma análise detalhada dos riscos. Esse processo deve contar com a colaboração de diversas partes interessadas, como equipes de segurança, profissionais de TI, consultores jurídicos e líderes empresariais.

Por exemplo, um prestador de serviços de saúde pode considerar a proteção dos registros eletrônicos de saúde (EHRs) como uma prioridade crítica, devido à natureza sensível dos dados e às possíveis consequências de uma violação, como a perda de informações dos pacientes e penalidades regulatórias previstas pela HIPAA. Ao priorizar a segurança dos registros eletrônicos de saúde (RES), o prestador pode direcionar seus esforços de conformidade para implementar controles que reduzam os riscos mais críticos.

À medida que os requisitos normativos continuam a aumentar em complexidade, as organizações estão recorrendo cada vez mais a ferramentas de governança, geranciamento de riscos e conformidade (GRC) para simplificar seus processos de conformidade, melhorar a visibilidade e garantir monitoramento e melhoria contínuos.

Uma abordagem orientada pelo risco para a conformidade ajusta os esforços de segurança aos riscos específicos de cada organização, assegurando que as ameaças mais críticas sejam priorizadas.

Visão geral das ferramentas GRC e seus benefícios:

As ferramentas GRC são projetadas para ajudar as organizações a automatizar e gerenciar vários aspectos de conformidade, incluindo desenvolvimento de políticas, avaliações de risco, controle de auditoria e resposta a incidentes. Essas ferramentas oferecem vários benefícios principais:

- **Gerenciamento centralizado de conformidade:** As ferramentas de GRC permitem que as organizações consolidem as atividades de conformidade em uma única plataforma.
- **Automação de tarefas de conformidade:** Ao automatizar tarefas rotineiras de conformidade, como monitorar registros de acesso ou gerar relatórios de auditoria, as ferramentas de GRC liberam um tempo valioso.
- **Visibilidade aprimorada e geração de relatórios:** As ferramentas de GRC proporcionam visibilidade em tempo real do status de conformidade, facilitando para os líderes de segurança o acompanhamento do progresso, a identificação de lacunas e a demonstração de conformidade a reguladores e auditores.
- **Monitoramento e melhoria contínua:** As ferramentas de GRC dão suporte ao monitoramento contínuo das atividades de conformidade, permitindo que as organizações identifiquem e abordem problemas de forma proativa, em vez de reativa.

2.

Por que é importante adotar regulamentos de conformidade

O objetivo de compreender os riscos da sua organização e como abordá-los não é apenas identificar falhas. Em vez disso, é importante encontrar fatos para que você possa ajudar sua organização a se proteger e avançar. Embora os executivos possam pensar que sua organização está preparada e seria ciberresiliente, a realidade pode ser muito diferente — colocando as organizações em risco.

Garantir que haja envolvimento e comprometimento do conselho é a principal maneira de alcançar a conformidade. As organizações precisam promover uma cultura de conformidade em toda a organização para reduzir os riscos. A gestão é responsável pela implementação de processos e tecnologia de acordo com as normas. É fundamental dar um passo atrás e garantir que as leis e os regulamentos sejam cumpridos dentro do contexto do setor e da localização geográfica da empresa.

À medida que o setor evolui e se adapta, os padrões de conformidade e regulamentação também passarão por mudanças. No entanto, é importante evitar que sua empresa fique atrás em termos de conformidade, pois isso pode resultar em negligência, colocando executivos ou membros do conselho sujeitos a sanções punitivas. Pode haver penalidades financeiras e danos à reputação causados por uma paralisação ou um ataque de ransomware. Mas quanto mais madura a sua organização se torna em relação às diferentes conformidades normativas, maiores serão as chances de se recuperar rapidamente.

Conformidade em todo o mundo

Em todo o mundo, ao analisar a legislação cibernética, mais de 150 países possuem algum tipo de legislação cibernética em vigor. Alguns deles incluem o DORA na UE, bem como o NIS/NIS2 no Reino Unido. O Japão tem a FSA, enquanto o Oriente Médio conta com a NESA e as Leis de Proteção de Dados DIFC. Globalmente, os países podem recorrer ao NIST. Quando as pessoas nos EUA pensam em ransomware e multas regulatórias, frequentemente associam à Comissão de Valores Mobiliários (SEC). Apesar da ampla gama de opções regulatórias, menos de 100 países têm regulamentação de infraestrutura crítica. Isso mostra que muitos países não estão lidando com segurança em alto nível, embora exista uma necessidade muito real de se concentrar nesses ambientes de infraestrutura crítica. Ao olhar especificamente para o setor de saúde, incluindo pesquisa e biotecnologia, é comum que as regras variem de acordo com o país.

Os regulamentos de conformidade garantem que sua organização esteja preparada para incidentes cibernéticos, com o envolvimento do conselho crucial para promover uma cultura de segurança.

Como os Serviços Financeiros e os Setores de Saúde Diferem

Nos EUA, o Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) define 16 setores críticos que precisam cumprir diferentes regulamentos de segurança cibernética. Quando as pessoas pensam em indústrias críticas, normalmente pensam em barragens, redes elétricas e, obviamente, saúde. Os serviços financeiros e de saúde desempenham um papel fundamental no dia-a-dia das pessoas em todo o mundo. Ao analisar os efeitos negativos que a falta de conformidade de segurança pode ter nas organizações de saúde, o impacto afeta a vida das pessoas.

A HIPAA é uma das principais regulamentações que vem à mente quando se fala em conformidade na área da saúde. A Regra de Privacidade da HIPAA estabelece padrões nacionais para a proteção de certas informações de saúde, enquanto a Regra de Segurança da HIPAA estabelece um conjunto nacional de padrões de segurança para proteger certas informações de saúde que são mantidas ou transferidas em formato eletrônico. Se um provedor de serviços de saúde não estiver adequadamente protegido ou em conformidade, ele poderá correr o risco de ter os dados de seus pacientes comprometidos em caso de um ataque de ransomware.

No setor financeiro, uma das principais regulamentações é a GLBA, ou Lei Gramm-Leach-Bliley. Essa lei exige que as empresas financeiras que oferecem aos consumidores produtos ou serviços financeiros, como empréstimos, consultoria financeira ou de investimento ou seguros, expliquem suas práticas de compartilhamento de informações a seus clientes e protejam dados confidenciais. Quando uma empresa financeira não está em conformidade com estruturas ou regulamentos, ela corre o risco de enfrentar custos em potencial, como perdas financeiras significativas, multas, instabilidade econômica e danos à reputação.

As organizações precisam se adaptar continuamente às novas regulamentações para garantir a conformidade e se manter à frente da evolução das ameaças cibernéticas.

3.

Recomendações de melhores práticas e implementação

A conformidade está longe de ser um evento único. Os requisitos normativos não são imutáveis; eles evoluem com o tempo à medida que novas ameaças emergem e as regulamentações são revisadas. Portanto, existem algumas melhores práticas que devem ser implementadas para garantir que sua empresa esteja alinhada com todas as estruturas e regulamentações essenciais.

Monitoramento Contínuo

O monitoramento contínuo é um componente crítico da gestão eficaz da conformidade. As ferramentas GRC facilitam o monitoramento contínuo, integrando-se à infraestrutura de segurança existente, como sistemas SIEM (Security Information and Event Management), para acompanhar a conformidade em tempo real.

Por exemplo, uma empresa de serviços financeiros sujeita à SOX pode usar uma ferramenta GRC para monitorar continuamente o acesso a sistemas financeiros, garantindo que apenas pessoas autorizadas tenham acesso a dados financeiros confidenciais. Ao integrar ferramentas de GRC em suas estratégias de segurança cibernética, as organizações podem agilizar seus esforços de conformidade, reduzir o risco de não conformidade e garantir que suas práticas de segurança evoluam em conjunto com os requisitos regulatórios.

Auditorias e Avaliações Periódicas

Durante um ataque, não se trata de saber se você tem um plano de resposta a incidentes implementado. Você deve *saber que* seu plano vai funcionar. Uma das melhores maneiras de garantir isso é por meio de testes. Testar o plano da sua organização e demonstrar que o teste foi bem-sucedido é como você garante o nível de conformidade.

Etapas principais para conformidade

Ao avaliar as regulamentações que as organizações podem adotar para garantir a conformidade, é essencial adotar uma abordagem abrangente. Cada parte da sua organização pode tocar outro aspecto do seu ambiente. O planejamento e a antecipação desempenharão um papel crucial para garantir a conformidade da sua organização. Algumas etapas a serem consideradas incluem:

- **Desenvolver um processo de gestão de riscos:** Isso envolve identificar todos os riscos potenciais de TI que podem afetar seus negócios, bem como avaliar suas vulnerabilidades.
- **Analise e priorize seus riscos:** Isso pode ser feito por meio do desenvolvimento de uma estratégia de mitigação de riscos e do treinamento de sua equipe.
- **Desenvolva um plano de resposta a incidentes:** Nesse plano, você pode considerar aspectos como a transferência de risco, ao mesmo tempo em que mantém a visibilidade e o entendimento do seu ambiente.
- **Estabeleça uma cultura de segurança:** Isso pode envolver todas as partes interessadas relevantes, selecionar as tecnologias adequadas e, acima de tudo, garantir que tudo seja bem documentado, documentado — e documentado.

Desenvolva um processo de geranciamento de riscos, priorize riscos e estabeleça uma cultura de segurança para manter a conformidade e aumentar a resiliência.

Conclusão

O futuro da conformidade regulatória se concentrará na resiliência, com as empresas precisando se antecipar a novas regulamentações e criar programas de conformidade adaptáveis e proativos.

O cenário regulatório é dinâmico e é improvável que o ritmo das mudanças regulatórias diminua, particularmente à medida que governos e órgãos reguladores respondem aos rápidos avanços na tecnologia. Pensando nisso, a orientação é que as organizações adaptem as estruturas de segurança e continuem atendendo à conformidade normativa. Um objetivo secundário seria a padronização das melhores práticas de segurança, visando atingir um ponto em que as organizações adotem uma postura de segurança considerada aceitável.

Em resumo, a conformidade normativa é uma jornada constante que exige esforço, adaptação e colaboração.

Não é suficiente apenas alcançar a conformidade; as organizações devem se dedicar a manter e aprimorar seus programas de conformidade à medida que as ameaças e as regulamentações evoluem. Líderes de segurança e tomadores de decisão de TI têm um papel fundamental nesse processo, guiando suas organizações em direção a uma estratégia de conformidade que vai além de evitar penalidades, focando a construção de uma organização mais robusta e resiliente no âmbito cibernético. Ao incorporar a conformidade à estrutura das operações e à cultura da organização, e ao se manterem informadas e ágeis diante das mudanças, as organizações podem navegar pelas complexidades do cenário regulatório com confiança e sucesso.