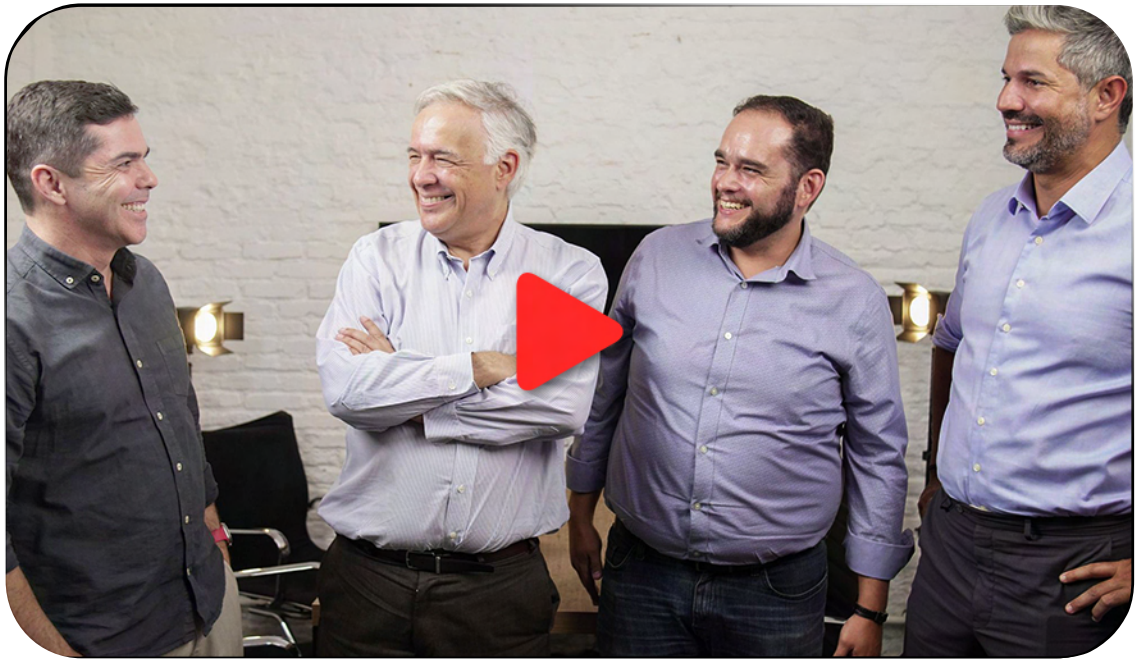
Gestão de Riscos e CIBERSEGURANÇA

Um resumo de Luiz Henrique Lobo

Idealizado por:

Conselho
& CONSELHEIROS

Luiz Henrique Lobo, um conselheiro independente, líder de comitês de risco, professor e consultor.
Sua vasta experiência como CRO (Chief Risk Officer) em empresas multinacionais e brasileiras de grande porte lhe confere uma expertise notável em gestão de riscos.



Ele foi nosso o convidado no episódio 2 do **podcast** de **Conselho & Conselheiros**. Clique na imagem acima e assista o bate-papo completo, com muito mais dicas que não foram abordadas aqui.

Principais pontos do bate-papo sobre **Gestão de Riscos e Cibersegurança** no podcast **Conselho & Conselheiros**

“Queria comentar e falar mais do episódio do ótimo Podcast Conselho & Conselheiros liderado pelo **Nycholas Szucko**, **Cristiano Adjuto Campos** e **Glauco Sampaio**, que participei como convidado em que nos aprofundamos mais no processo de transformação do risco em cibersegurança, que passou a ser um tema de alta prioridade nas agendas dos conselhos de administração e comitês de riscos e auditoria.”

Além de darmos dicas úteis sobre como engajar conselheiros neste tema técnico e preparar os #CISOs (Chief Information Security Officer) para este tipo de diálogo estratégico com a governança, se preparando para debates de alto nível a fim de aprimorar a maturidade em cibersegurança, mitigar riscos e assegurar a continuidade dos negócios, enfatizando que a cibersegurança é uma responsabilidade compartilhada.

Luiz Henrique Lobo

Contextualização e Evolução Profissional

Começamos o podcast compartilhando, em especial para quem não me conhece ainda, minha trajetória em engenharia civil e de produção pela PUC do Rio até minha entrada no mercado financeiro, e posteriormente uma especialização em gestão de riscos o que inclui também os cibernéticos, o foco deste bate papo.

Destaquei a importância da adaptação profissional diante das mudanças do mercado, ilustrando a transição de carreira que muitos enfrentam ao migrar de áreas técnicas específicas para a gestão de riscos complexos como os cibernéticos.

Demonstrei a relevância de construir uma base sólida de conhecimentos técnicos, complementada por uma constante busca por atualização e especialização, particularmente em áreas emergentes como a cibernética. “Estou sempre buscando me informar das novidades da área cibernética, o que esta sendo feito aqui no Brasil e lá fora.”

Importância de Gestão de Riscos Cibernéticos

Por ter passado por dois ataques cibernéticos nas empresas que trabalhei, enfatizei a importância da gestão de riscos cibernéticos, associando a um cenário global onde as ameaças digitais se tornam cada vez mais sofisticadas e impactantes, onde o entendimento profundo e a constante atualização em segurança cibernética são fundamentais para a resiliência organizacional. Ataques bem sucedidos resultaram em significativos prejuízos financeiros e de reputação para as empresas, marcas e pessoas afetadas.

Desafios e Estratégias de Mitigação

Ao longo do podcast, discutimos diversos desafios na gestão de riscos cibernéticos, incluindo com a dificuldade de quantificação de riscos, a importância da conscientização em todos os níveis organizacionais, do conselheiro ao estagiário, e a necessidade de mitigação eficazes. Compartilhei as estratégias práticas, como a implementação de sistemas robustos de detecção e resposta a incidentes, a educação contínua de colaboradores e a importância de uma cultura organizacional que priorize a segurança cibernética.

Exemplos Práticos e Lições Aprendidas

Trouxe alguns exemplos práticos, ilustrando como as crises cibernéticas foram gerenciadas, e principalmente quais lições foram aprendidas com esses eventos, destacando como sempre a importância de planos de continuidade de negócios que integrem riscos cibernéticos e a eficácia de uma comunicação clara e direta na gestão de crises.

Outro caso onde levantei fragilidades de uma estrutura e investimentos feitos na IF (Instituição Financeira), pois achava que era minha responsabilidade fazer este comentário como conselheiro, mas nem sempre isto é entendido e interpretado desta forma pelos demais, em especial o pessoal executivo, que ao invés de melhorarem, preferem ficar dando desculpas e questionar o papel da governança independente. Um dia vão aprender da pior forma: sofrendo um ataque e com consequências.

Desafios na Quantificação e Conscientização

Falamos da quantificação dos riscos cibernéticos, que dada a sua natureza frequentemente intangível e a rápida evolução das ameaças torna-se algo não trivial de ser feito.

O uso de estratégias para mitigação dos riscos de segurança como treinamentos regulares para funcionários e a criação de planos de resposta a incidentes bem definidos visando não apenas a prevenção, mas também a rápida recuperação pós-ataque, são algumas dessas estratégias.

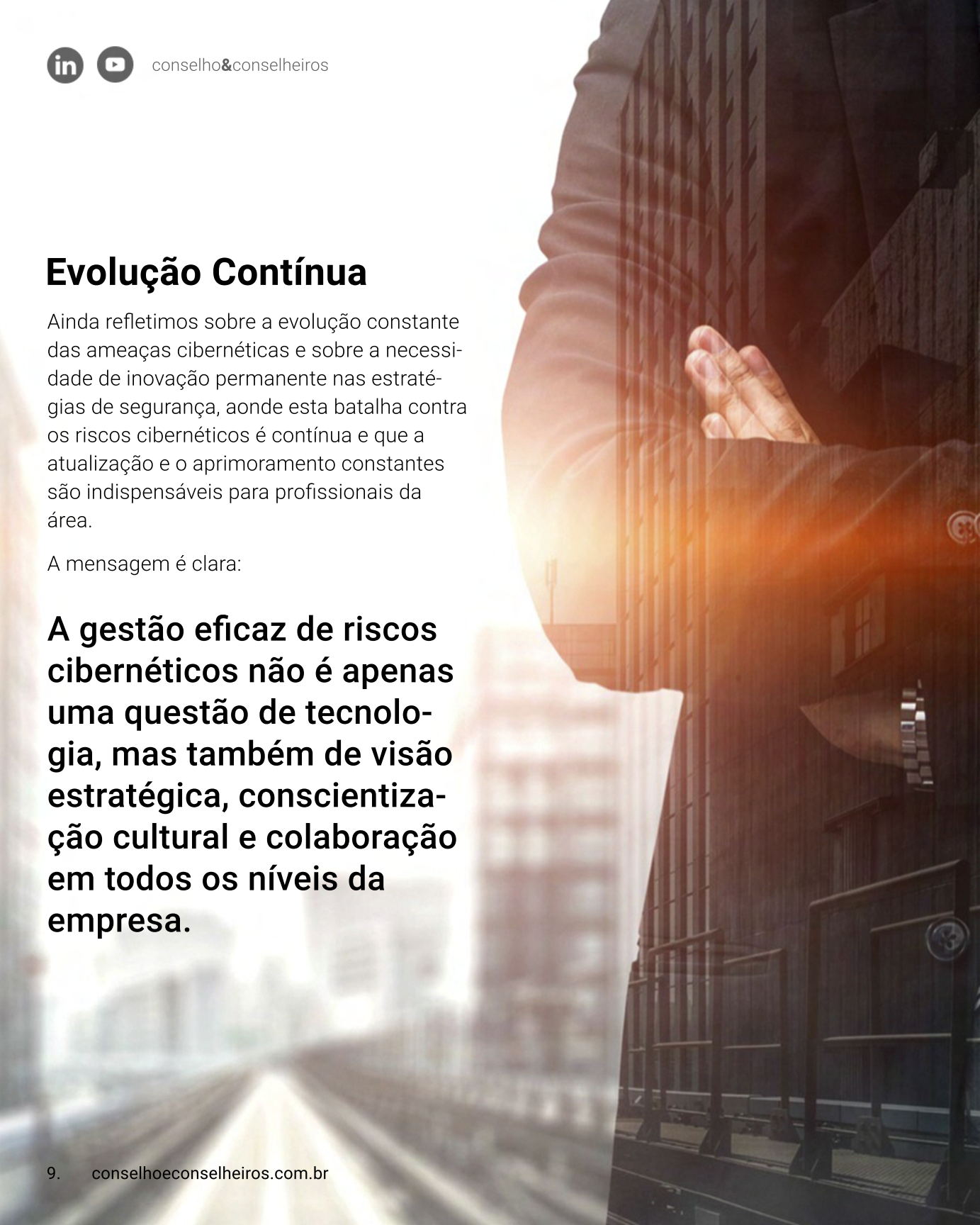
Crises Cibernéticas

Outro tema de grande importância que todos devem ter conhecimento e estejam preparados é a gestão de crises cibernéticas, onde diferentes abordagens de condução da crise podem levar a desfechos distintos. Enfatizo a importância de uma preparação prévia e simulada, além de uma estratégia de comunicação eficaz durante crises.

CRISTIANO ADJUTO

“Não consigo te dizer somente com um indicador se a empresa está ruim, média ou boa. Acredito que é muito alto para vocês compreenderem a correta sensação de segurança e do risco, entenderem onde é que tem que ajudar, onde é que tem que por os esforços e a concentração para elevar a resiliência da empresa. No desenvolvimento da aplicação? Nas pessoas?"

Clique no texto acima e veja esse trecho/corte do Podcast



Evolução Contínua

Ainda refletimos sobre a evolução constante das ameaças cibernéticas e sobre a necessidade de inovação permanente nas estratégias de segurança, aonde esta batalha contra os riscos cibernéticos é contínua e que a atualização e o aprimoramento constantes são indispensáveis para profissionais da área.

A mensagem é clara:

A gestão eficaz de riscos cibernéticos não é apenas uma questão de tecnologia, mas também de visão estratégica, conscientização cultural e colaboração em todos os níveis da empresa.

GLAUCO SAMPAIO

“Você como empresa é responsável pelo que acontece com todo o seu entorno. Se você terceiriza um serviço e um incidente cibernético acontece com aquele, o responsável é você.”

Clique no texto acima e veja esse trecho/corte do Podcast

O Papel da Governança Corporativa

Mostrei a **importância da governança corporativa na estruturação e implementação de estratégias eficazes de gestão de riscos cibernéticos**, com a responsabilidade dos conselhos de administração e seus comitês de assessoramento de riscos e auditoria, em assegurar que as empresas não apenas cumpram com regulamentações específicas, mas também adotem as melhores práticas para proteção contra ameaças digitais.

Falamos também da necessidade de conselheiros bem informados e a interação entre conselhos e equipes técnicas para uma tomada de decisão informada. O especialista em segurança cibernética do conselho tem que estar próximo do Líder de Segurança, compreendendo os desafios para um aconselhamento mais eficaz, além de apoiar na tradução do risco para os demais conselheiros.

A Integração entre Riscos Financeiros e Não Financeiros

Abordei ainda a convergência entre riscos financeiros e não financeiros, ilustrando como os ataques cibernéticos podem afetar ambos os aspectos simultaneamente, por isto a necessidade de uma abordagem holística na gestão de riscos, que considere tanto as implicações financeiras diretas dos ataques, como resgates em criptomoedas exigidos por hackers, quanto os impactos indiretos, como danos à reputação e perda de confiança dos clientes.

Tecnologias de Segurança

Durante o bate papo, falamos de várias tecnologias essenciais para a proteção contra riscos cibernéticos, desde sistemas básicos de segurança, como firewalls e softwares antivírus, até soluções mais complexas, como sistemas de detecção e resposta a incidentes avançadas (EDR) e técnicas de segmentação de rede para limitar o comprometimento em caso de um incidente e logicamente da importância da criptografia para proteger dados confidenciais.

Preparação e Resposta a Incidentes

Um ponto crítico que foi abordado é a importância de uma preparação adequada para incidentes cibernéticos, incluindo a existência de planos de resposta detalhados, para que a empresa tenha a capacidade de responder rapidamente e de maneira coordenada a um ataque, o que pode significar a diferença entre um incidente controlável ou um caos no momento da resposta.

A discussão passou também na necessidade de simulações e treinamentos regulares para assegurar que as equipes estejam prontas para agir efetivamente sob pressão.

A Importância da Educação Continuada

A educação continuada foi apontada como um pilar central na estratégia de defesa contra ameaças cibernéticas, aonde a conscientização e o treinamento regulares de todos os colaboradores, incluindo os conselheiros, são essenciais, dado que muitos ataques bem-sucedidos começam com engenharia social ou phishing.

A formação contínua ajuda a criar uma primeira linha de defesa sólida, onde os colaboradores são capazes de reconhecer e evitar potenciais ameaças. Com um plano adequado de educação as pessoas passam de uma superfície de ataque vulnerável para uma das principais defesas das corporações.

Desafios Regulatórios e de Conformidade

Falamos dos desafios regulatórios e de conformidade enfrentados pelas empresas no contexto de segurança cibernética e como a complexidade e constante evolução das regulamentações podem ser desafiadoras. A discussão inclui a importância de sistemas de governança de dados para garantir a conformidade com leis como GDPR na Europa e LGPD no Brasil.

NYCHOLAS SZUCKO

“Tem pessoas que são mais abertas, elas decidem entregar mais informações para ter uma experiência mais personalizada, outras já não, pois prezam por privacidade.”

Clique no texto acima e veja esse trecho/corte do Podcast

Perspectivas Futuras sobre Inteligência Artificial e Machine Learning

Como não poderia deixar, falamos das perspectivas futuras relacionadas ao uso de inteligência artificial (IA) e machine learning na detecção e prevenção de ataques cibernéticos, aonde embora estas tecnologias ofereçam potencial significativo para melhorar a segurança, elas também trazem novos desafios e vulnerabilidades que devem ser gerenciados cuidadosamente.

Estes pontos adicionais complementam a compreensão sobre a gestão de riscos cibernéticos, destacando a complexidade do tema e a necessidade de uma abordagem multifacetada que **envolva tecnologia, governança, educação e preparação constante**.

Cultura de Segurança Organizacional

Um tema transversal que permeia muitas das discussões é a importância da construção de uma cultura de segurança robusta dentro das empresas, pois mais o que simplesmente implementar tecnologias e processos de segurança, as empresas devem promover uma mudança cultural, onde **a segurança cibernética é vista como uma responsabilidade compartilhada por todos os colaboradores**, independentemente do nível hierárquico ou função. Isso envolve educar e engajar a equipe, desde a alta direção até os colaboradores da linha de frente, sobre os riscos cibernéticos e a importância de práticas seguras no dia a dia.

Engajamento e Comunicação Efetiva

A comunicação efetiva sobre riscos, políticas e procedimentos de segurança é fundamental para o engajamento dos colaboradores, por isto mesmo a necessidade de estratégias de comunicação que transcendam os jargões técnicos, alcançando uma compreensão clara e a adesão de todos na empresa.

Exemplos práticos, histórias reais de ataques e suas consequências, bem como treinamentos interativos, foram mencionados como ferramentas eficazes para aumentar a conscientização e promover uma cultura de segurança.

Feedback e Melhoria Contínua

Outro ponto é a importância de sistemas de feedback que permitam a colaboradores reportar potenciais ameaças ou vulnerabilidades de maneira fácil e segura, através da melhoria contínua das práticas de segurança cibernética, que deve ser baseada em aprendizados contínuos, o que inclui analisar incidentes de segurança, adaptar-se às novas ameaças e ouvir as preocupações e sugestões dos colaboradores.

Este ciclo de feedback positivo contribui não apenas para a resiliência técnica, mas também para a fortaleza da cultura de segurança dentro da organização.

Evolução Contínua

Destacamos a importância da liderança em segurança cibernética, onde os **líderes e gestores das organizações devem demonstrar um compromisso visível com a segurança**, estabelecendo uma direção clara e promovendo valores que priorizem a proteção de dados e a segurança dos sistemas. Não esqueçam que o exemplo vem de cima e que a liderança consciente e efetiva é fundamental para incutir uma cultura de segurança duradoura.

Esses pontos reforçam a ideia de que a gestão de riscos cibernéticos vai além das ferramentas e tecnologias, englobando **aspectos comportamentais, culturais e de liderança**, essenciais para uma abordagem holística e eficaz à segurança cibernética.

Como podemos ver através da reflexão acima sobre as perspectivas futuras da gestão de riscos cibernéticos, somado a inevitabilidade da evolução das ameaças digitais e a consequente necessidade de inovação constante nas estratégias de segurança, importante que os profissionais da área a manterem-se atualizados, proativos e resilientes diante dos desafios emergentes, sublinhando que a **gestão eficaz de riscos cibernéticos é fundamental para a sustentabilidade e o sucesso a longo prazo das empresas**.

Conselho
& CONSELHEIROS

conselhoeconselheiros.com.br