MÓDULO 7

A Visão do Líder

Gestão de risco, Cultura de segurança e o papel estratégico da liderança na cibersegurança

A segurança cibernética não é apenas uma questão técnica, mas uma decisão de **governança** e **liderança**. Este artigo é direcionado aos gestores e líderes da cooperativa, destacando seu papel crucial como **exemplo** e **patrocinador** da cultura de segurança. Analisamos a conexão direta entre um **incidente cibernético** e o **risco operacional e financeiro** da instituição, mostrando como a cibersegurança impacta o balanço patrimonial e a reputação. Por fim, delineamos as **ações essenciais que a liderança deve tomar durante um incidente**, garantindo uma resposta coordenada e minimizando o impacto.

Palavras-chave: Liderança em Segurança, Cultura de Segurança, Gestão de Risco Cibernético, Risco Operacional, Resposta a Incidentes, Governança.

---

1. Introdução: Segurança começa no topo

Em qualquer organização, a cultura é definida pelo que a liderança tolera e pelo que ela prioriza. Na segurança cibernética, a máxima é clara: **a segurança começa no topo** [1]. Se o gestor não segue as regras de ouro (MFA, senhas fortes, tela bloqueada), ele desautoriza a política de segurança, independentemente dos investimentos em tecnologia.

O papel da liderança vai além da aprovação de orçamentos de TI; é ser o **principal agente de mudança** e o **exemplo** que todos os colaboradores seguirão.

2. O papel do gestor como exemplo e agente de mudança

O gestor é a ponte entre a estratégia de segurança da cooperativa e a prática diária da equipe.

2.1. Liderar Pelo Exemplo

A adesão da liderança às políticas de segurança é o fator mais importante para o sucesso de um programa de conscientização.

Ação do Gestor	Impacto na Cultura de Segurança
Usa MFA em todas as contas	Demonstra que a segurança é prioridade, não um inconveniente.
Bloqueia a tela ao sair da mesa	Reforça a importância da segurança física e da política de "Tela Bloqueada".
Reporta e-mails suspeitos	Incentiva a equipe a reportar sem medo de culpas (Módulo 8).
Participa ativamente dos treinamentos	Mostra que a educação em segurança é relevante para todos os níveis.

2.2. Promover a Cultura de Segurança

A cultura de segurança é a soma dos hábitos e crenças de todos os colaboradores em relação à proteção de dados. O líder deve:

- **Comunicar Constantemente:** Integrar a segurança nas reuniões de equipe e nos comunicados internos.
- **Recompensar o Comportamento Seguro:** Reconhecer publicamente a equipe ou o colaborador que reportou um risco ou seguiu um protocolo de forma exemplar.
- **Transformar o Erro em Aprendizado:** Garantir que um incidente ou erro seja tratado como uma oportunidade de aprendizado, e não como motivo para punição imediata (exceto em casos de má-fé).

3. A Conexão entre Incidente Cibernético e Risco Operacional/Financeiro

Em uma cooperativa de crédito, um incidente cibernético é, por definição, um **incidente de risco operacional** e, quase sempre, um **risco financeiro** [2].

3.1. Risco Operacional

Um ataque de *ransomware* que paralisa os sistemas de atendimento ou de transações online impede a cooperativa de funcionar.

- **Perda de Produtividade:** Colaboradores ficam inoperantes, gerando perda de receita e custo de mão de obra.
- **Interrupção de Serviço:** O cooperado não consegue acessar sua conta, sacar ou fazer pagamentos, gerando insatisfação e perda de confiança.

3.2. Risco Financeiro

Os custos de um incidente cibernético são multifacetados e podem ser catastróficos.

Tipo de Custo	Descrição
Custos de Resposta	Contratação de especialistas forenses, *softwares* de recuperação, horas extras da equipe de TI.
Custos Regulatórios	Multas da LGPD (ANPD) ou do Banco Central por falha na proteção de dados.
Custos de Reputação	Perda de cooperados, queda na captação de recursos e dificuldade em atrair novos membros.
Custos de Litígio	Processos judiciais movidos por cooperados afetados pelo vazamento de dados.

Estudo de Caso: Um estudo do Fundo Monetário Internacional (FMI) aponta que ataques cibernéticos geraram perdas de bilhões de dólares ao setor financeiro em menos de duas décadas, sublinhando a necessidade de investimento contínuo em prevenção e resiliência [3].

4. O Que a Liderança Deve Fazer Durante um Incidente

Ter um **Plano de Resposta a Incidentes (PRI)** não é opcional, é obrigatório. Durante uma crise, a liderança deve focar em três pilares:

4.1. Comunicação Estratégica

A liderança é a voz da cooperativa durante a crise.

- **Comunicação Interna:** Informar os colaboradores sobre o que está acontecendo (o que está afetado e o que deve ser feito) de forma clara e calma, evitando pânico.
- **Comunicação Externa:** Comunicar o incidente aos cooperados, à mídia e aos órgãos reguladores (ANPD e Banco Central) de forma transparente e no prazo legal, demonstrando controle da situação.

4.2. Tomada de Decisão Rápida

O líder deve autorizar imediatamente as ações necessárias para conter o ataque.

- **Isolamento:** Autorizar a equipe de TI a isolar sistemas e redes comprometidas, mesmo que isso signifique interromper temporariamente serviços. A contenção é prioridade.
- **Recursos:** Autorizar a contratação imediata de *experts* externos (advogados especializados, empresas de resposta a incidentes) para auxiliar na remediação e na conformidade legal.

4.3. Apoio à Equipe Técnica

A liderança deve proteger a equipe de TI e segurança de pressões externas e internas, permitindo que eles se concentrem na remediação técnica.

- **Foco:** Garantir que a equipe técnica tenha os recursos e o tempo necessários para seguir o PRI, sem a pressão de restaurar os serviços antes da hora.

5. Conclusão

A segurança cibernética é uma questão de **Gestão de Risco** que exige o envolvimento ativo da liderança. Ao ser o exemplo, ao promover uma cultura de segurança e ao estar preparado para responder a um incidente de forma estratégica, o líder garante que a cooperativa não apenas sobreviva às ameaças digitais, mas que saia delas mais forte, preservando seu patrimônio e, acima de tudo, a **confiança** de seus cooperados.

Referências Bibliográficas

[1] Motivarte. **O papel da liderança na cultura de segurança: por que começa no topo?**. Disponível em: https://motivarte.com.br/o-papel-da-lideranca-na-cultura-de-seguranca-por-que-comeca-no-topo/
[2] Illumio. **Principais riscos cibernéticos enfrentados pelas instituições financeiras**. Disponível em: https://www.illumio.com/pt-br/resource-center/key-cyber-risks-facing-financial-institutions
[3] Exame. **Ataques cibernéticos geram perdas de US$ 12 bi ao setor financeiro em duas décadas, diz FMI**. Disponível em: https://exame.com/economia/ataques-ciberneticos-geram-perdas-de-us-12-bi-ao-setor-financeiro-em-duas-decadas-diz-fmi/
[4] Marsh. **Guia do CISO para risco cibernético: Respondendo a um incidente cibernético**. Disponível em: https://www.marsh.com/pt-br/services/cyber-risk/insights/cisos-guide-to-cyber-risk-responding-to-cyber-incident.html
[5] (Adicionar referências adicionais conforme aprofundamento da pesquisa, se necessário).