

Por Débora Soares



Conscientizar os funcionários sobre a importância da segurança da informação é pilar essencial e contínuo na jornada de transformação digital. Com esse propósito, a Abrapp realizou um workshop em março com a participação do especialista, referência na área, [Longinus Timochenco](#), CISO – Chief Information Security Officer e Diretor de Governança Corporativa do KaBuM!

Nesta entrevista, Longinus compartilha alguns ensinamentos transmitidos ao time da Abrapp, e que podem ser replicados pelas associadas:

**BLOG ABRAPP EM FOCO: A Abrapp tem promovido workshops que levam conhecimentos aos funcionários sobre a importância da segurança da informação. Como iniciativas desse tipo, considerando o papel da Associação em induzir boas práticas, podem contribuir para a proteção do segmento das entidades fechadas de previdência complementar?**

**LONGINUS TIMOCHENCO:** Quero destacar e parabenizar essa bela iniciativa da Abrapp. Esse tema atual Segurança da Informação remete a todos, sem exceção. Nosso mundo e negócios estão cada vez mais “digitais” e o cidadão “online”. Dessa forma, nossa segurança é até uma necessidade de sobrevivência e continuidade.

**Por que “segurança da informação”? Poderia esclarecer esse conceito?**

O que há de mais valioso no mundo atual é “informação”, por esse motivo existem ambos os interesses, do bem e do mal. O crime digital já é uma indústria “do mal” bastante organizada,

atualizada e estruturada, e com isso as nossas vulnerabilidades só aumentam a cada minuto globalmente.

Corrupção é a “capacidade de degradar e de fazer apodrecer aquilo que deveria ser decente”.

**Em sua palestra, o sr. ressaltou que a segurança da informação começa com as pessoas. Poderia comentar?**

Correto. “Pessoas” são o elo mais forte da iniciativa de Segurança. Não podemos nos enganar acreditando que iremos responder aos problemas de segurança da informação somente ou através da tecnologia. É importante clarificar que “tecnologia é apenas o meio e suporte”; as regras são construídas e mantidas por pessoas.

Para que as prevenções aconteçam assertivamente é de extrema importância que pessoas sejam treinadas, capacitadas, estejam em concordância com as regras, e sejam monitoradas e penalizadas quando necessário. Mas, lógico, tudo com critério e direcionamento do negócio. O objetivo não é punir, e sim proteger negócios e pessoas.

Negócios são construídos e mantidos por Pessoas. Por isso, devemos iniciar e manter a maior parte da atenção e cuidado na Pessoas e, depois, Processos, Tecnologia e Inteligência, nessa ordem.

**O sr. também afirma que a responsabilidade por essa segurança não pode ser terceirizada. Por quê?**

As atividades de segurança podem ser terceirizadas, desde que as regras e a governança fiquem dentro de casa. É importante ficar claro que a responsabilidade legal das informações é de sua empresa e o board será cobrado por prover esses controles.

**Poderia explicar a importância de os colaboradores manterem uma “mesa limpa”?**

Mesa Limpa é sinal de segurança. Muitas das técnicas realizadas para se subtraírem informações aproveitam-se dos maus cuidados relacionados aos dados sensíveis deixados sobre a sua mesa. Reforço que esse item também é gap de auditoria por não aderência as boas práticas de segurança.

Assim, destaco que: informações devem ser guardadas em local apropriado; impressões, cópias e fax devem ser recolhidos; celulares e demais aparelhos devem ficar sempre em posse do responsável; necessário o bloqueio da tela do computador; notebooks devem ter trava de segurança.

**O que são os ataques de “engenharia social” e como podem afetar as entidades?**

O objetivo da engenharia social é enganar as pessoas de forma que forneçam informações valiosas ou acesso a essas informações. As técnicas de engenharia social, se baseiam em características do comportamento humano. Pessoas normalmente querem: ajudar; acreditar; e evitar problemas. **Em todos os lugares temos pessoas bem-intencionadas e mal-intencionadas.**

**Por que a segurança da informação não deve se limitar à proteção de dados pessoais?**

Informação está em todos os lugares, tanto físico como lógico, e deve ser protegida em uma abordagem 360 graus. A informação é o nosso maior ATIVO. A segurança da informação protege a informação de diversas ameaças, humanas e não-humanas.

**Ao encerrar sua apresentação, o sr. trouxe uma frase de Nelson Mandela: “Tudo é considerado impossível até acontecer”. Como isso se aplica à segurança da informação?**

Sou profissional que aprecio demais a reflexão diária, digo que a **reflexão é a real manutenção**

**da alma** para que sejamos melhores diariamente. Aplico essa mensagem do mestre Nelson Mandela à segurança, porque muitos ainda pagam para ver o desastre, não acreditam que acontece, e depois correm para corrigir custando muito mais caro e, muitas vezes, fazendo o mínimo.

### **Gostaria de deixar uma mensagem final?**

Prezados, tenham a consciência que a nossa vida é DIGITAL e ONLINE. Tudo isso é muito bom e válido pela comodidade, agilidade e escalabilidade que ganhamos. Mas para que possamos desfrutar de tudo com Disponibilidade, Integridade, Confidencialidade e Autenticidade, não devemos jamais abrir mão da nossa Segurança, caso contrário colocaremos em alto risco a nossa vida e a continuidade.

**A segurança não atrapalha, se atrapalhar é porque está sendo mal aplicada; ela provê a evolução. Segurança é responsabilidade de todos nós e um “novo estilo de vida”. Não abram mão disso!**

**Fonte:** [Abrapp em Foco](#), em 13.04.2022.