Por **Alexandre Sammogini**

“Prato do dia: Feijoada Completa !!!”. Este é, sem dúvida alguma, um ícone da culinária popular brasileira, com presença garantida nos cardápios de restaurantes de norte a sul do País. Em algumas regiões, tradicionalmente servida às quartas-feiras e, em outras, aos sábados, para a satisfação dos mais variados perfis de fiéis consumidores. Gorda ou magra, a depender do gosto freguês, a Feijoada vem mantendo sua posição de sucesso gastronômico, não apenas pela sua diversidade de sabor, como também, pelo seu valor nutritivo, custo acessível e seu papel – catalizador – social. De fato, motivos não faltam para justificar este sucesso e, para chegarmos até eles, a palavra-chave é Processo. Afinal, estamos falando de um prato cujo preparo envolve uma diversidade de ingredientes, com etapas e momentos de cozimentos distintos, temperos na medida correta e que exige um planejamento de dias, orientado por uma receita testada e fielmente seguida. Não há, portanto, espaço para improvisos de última hora.

Assim como no preparo da nossa tradicional Feijoada, a preparação e a manutenção de um ambiente resiliente a ataques cibernéticos em nossas entidades requerem processos planejados, bem definidos e formalmente registrados e observados. A partir desta edição, apresentaremos processos relacionados com a segurança da área de tecnologia capazes de proporcionar a mitigação de ameaças cibernéticas.

E nada mais conveniente e oportuno do que começarmos esta série pelo Processo de Conscientização e Treinamento.

Este processo consiste, basicamente, na promoção do engajamento e da aptidão de todos os dirigentes, colaboradores e prestadores de serviços da entidade na busca e manutenção contínuas de boas práticas de segurança da informação e de ambiente tecnológico eficiente e seguro, garantindo o desempenho apropriado de suas tarefas.

A execução do processo, portanto, não se limita à criação de políticas e estabelecimento de normativos internos voltados para a segurança da informação, já que o fator humano é de suma importância para o cumprimento das diretrizes estabelecidas.

De acordo com a norma ABNT NBR ISO 27002, convém que todos os colaboradores da organização recebam treinamento, educação e conscientização apropriados. Além disso, as políticas e os procedimentos organizacionais relevantes para as suas funções devem ser regularmente atualizados, sempre levando em consideração a segurança da informação e a proteção de dados.

Ainda nesta linha, a NIST 800-16 (1) estabelece, para o seu público alvo, que a conscientização de segurança seja obrigatória para todos os colaboradores, incluindo empregados, contratados, estagiários e quem estiver envolvido, de alguma forma, com sistemas de tecnologia da informação.

A área de Recursos Humanos, com o patrocínio da alta administração, deve trabalhar na criação e aplicação de um Programa de Treinamento e Conscientização, além de incentivar o respeito às políticas internas e o uso de canal de comunicação para consultas e reportes de desvios. O referido programa compreende atividades coordenadas e planejadas de acordo com as melhores especificações e as necessidades de cada assunto abordado. As ações para conscientização são diversas, não se limitando a: – criação de materiais criativos e atrativos, canais e ações fora do comum, palestras periódicas, treinamentos, aplicação de questionários, de jogos e realização de sorteios.

A seguir, apresentamos um quadro resumo de todos os pontos que devem ser observados para perfeita aplicação do Programa de Treinamento e Conscientização.

| | |
|---|---|
| 1 – Realizar Análise de gap de Habilidades. | Para entendimento das habilidades e comportamentos dos funcionários e terceiros da |

| | |
|---|---|
| | entidade e o quanto não estão aderindo às boas práticas, usando essas informações para criar um roteiro de linha de base da educação. |
| 2 – Realizar treinamentos para mitigação dos gaps de habilidades. | Para abordagem dos gaps de habilidades identificados, buscando impactar positivamente o comportamento de segurança dos membros da força de trabalho. |
| 3 – Atualizar conteúdo de conscientização com frequência. | Verificando se o programa de conscientização de segurança da organização é atualizado com frequência (pelo menos anualmente) para atender: (i) rotatividade de pessoal; (ii) evolução tecnológica permanente; (iii) melhora da maturidade de Governança Corporativa pelo aumento e/ou aperfeiçoamento dos controles internos; (iv) mudanças de paradigmas operacionais; e (v) mudança da legislação. |
| 4 – Oferecer treinamentos de autenticação segura a todos os funcionários. | Envolvendo todos os membros da força de trabalho, no sentido de entenderem sobre a importância de habilitar e utilizar a autenticação segura. |
| 5 – Treinar os funcionários na identificação de ataques de engenharia social. | Envolvendo todo o quadro de funcionários e terceiros da entidade no sentido de entenderem como identificar diferentes formas de ataques de engenharia social, como phishing, golpes telefônicos e fraudes telefônicas. |
| 6 – Treinar os funcionários no manuseio de dados. | Envolvendo todo o quadro de funcionários e terceiros da entidade, no sentido de entenderem como identificar e armazenar, transferir, arquivar e distribuir informações confidenciais adequadamente. |
| 7 – Treinar os funcionários sobre as causas de exposição não intencional de dados. | Envolvendo todos os funcionários e terceiros da entidade, para que os mesmos venham a conhecer as causas de exposições não intencionais de dados, como em casos de perda de dispositivos móveis ou em casos de envio de e-mail para a pessoa errada devido ao preenchimento automático do e-mail. |
| 8 – Treinar os funcionários na identificação e comunicação de incidentes. | Envolvendo todos os funcionários e terceiros da entidade para que eles possam identificar os indicadores de incidentes mais comuns e relatar esses incidentes à área de segurança para tratamento. |
| 9 – Garantir que o time de desenvolvimento de software seja treinado em codificação segura. | Certificando que todas as equipes de desenvolvimento de software recebam treinamento para escrever código seguro para seu ambiente, assim como responsabilidades específicas de desenvolvimento. |

** Parte 1*
*Nota: 1) Nacional Institute of Standards and Technology (NIS) – U.S Department of Commerce)*

**Fonte**: Abrapp em Foco, em 20.08.2021.