
patrocínio

MICRO FOCUS

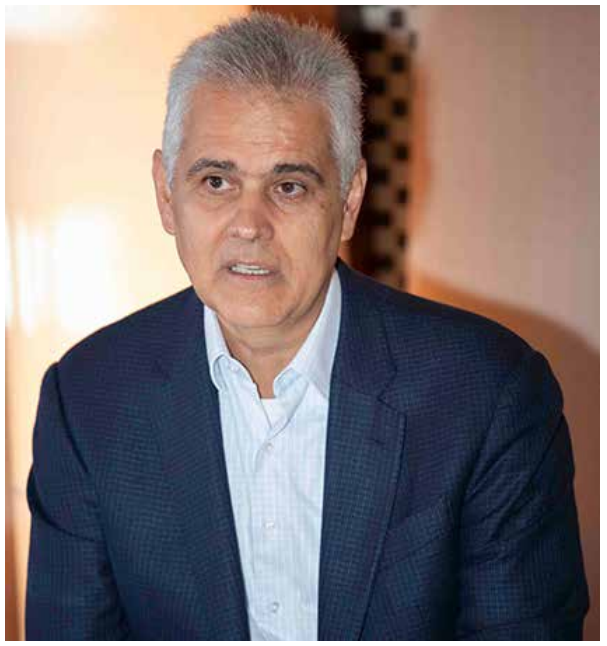
# SEGURANÇA DE ponta a ponta


patrocínio


O processo de transformação digital das empresas precisa levar em conta os desafios de segurança em todo o ciclo de desenvolvimento dos aplicativos, desde a fase de projeto até a entrega final das soluções.
Ao mesmo tempo em que desenvolvem suas competências digitais, para inovar em produtos, serviços e modelos de negócios, assim como experiências de clientes, melhorando sua eficiência operacional, as empresas não podem se descuidar dos aspectos de segurança.
Na chamada primeira plataforma (a era do mainframe), a TI era um privilégio das grandes empresas; na segunda plataforma, a TI se tornou mais competitiva e mais acessível para as médias e pequenas empresas; agora, na terceira plataforma, democratizada pelos dispositivos móveis, redes sociais e pelo acesso à nuvem, a tecnologia se tornou mais rápida, escalável e acessível, não só para grandes e pequenas empresas, mas também para as pessoas. E isso torna as soluções cada vez mais vulneráveis. Daí a necessidade de se integrarem as equipes de segurança ao desenvolvimento cada vez mais rápido e frequente de todo o ciclo de vida das aplicações
Como as empresas devem se preparar para gerar, de forma segura, mais negócios, e apoiar seus clientes nessa fase de transição para a transformação digital?
Algumas respostas estão nesta mesa-redonda, conduzida pelo diretor de redação do Informática Hoje, **Wilson Moherdaui**. Participaram do debate: **Cristiano** Barbieri, vice-presidente de transformação digital, inovoação e tecnologia da SulAmérica; **Gustavo** Vieira, CIO global da Vale; João **Bezerra** Leite, consultor; **Lilian** Hoffmann, diretora de tecnologia e operações da Beneficência Portuguesa (BP); **Luzia** Sarno, diretora de tecnologia do Grupo Fleury; Marcos **Sirelli**, CIO da Porto Seguro; **Ricardo** Moraes, responsável pela área de arquitetura e segurança da informação na Azul Linhas Aéreas; **Rogério** Pires, o diretor de TI da JHSF e dos hotéis e restaurantes Fasano; Sergio **Bambace**, CIO da Vigor; e **Wilson** Roberto Leal diretor de tecnologia e inovação da Tokio Marine.

**Informática Hoje -** Considerando que a segurança não deve mais ser só uma camada a se sobrepor ao final do desenvolvimento das soluções, como se fazia no passado, mas deve permear todo o desenvolvimento, desde a concepção do projeto até a entrega final, quero ouvir de vocês a experiência que já têm com esse tema. Especialmente se a integração das equipes de segurança com as de desenvolvimento já acontece naturalmente.

Hamilton Penna



“Cada vez mais, a segurança tem que estar integrada no primeiro minuto de concepção de um projeto”.

Bezerra

**Bezerra -** Antes de mais nada, preciso dizer que não gosto da expressão “transformação digital”. Na verdade, estamos vendo em várias empresas que estamos digitalizando formulários, digitalizando aquilo que já existia, que é um pouco de design by analogy. É preciso discutir se realmente estamos fazendo uma transformação ou, como um bom engenheiro, simplesmente melhorando o que já existe. Se você pegar as casas bancárias de hoje, elas são muito parecidas com o que existia há séculos, do ponto de vista do trabalho.
A China tem dado o exemplo, desenhando do nada, o que significa jogar fora toda a concepção anterior. Aí, sim, o digital aparece. O digital aparece quando você digitaliza e em um segundo momento consegue fazer uma disrupção. Aí aparecem três coisas: a democratização, já que fica muito mais fácil para todos utilizarem; a desmaterialização, pois hoje se pode fazer tudo pelo celular, com uma infinidade de apps; e por fim vem a desmonetização, com tudo virando custo zero, ou custo marginal. O Google pretende colocar satélite na África, e com isso vai incluir 1 bilhão de pessoas no mercado, dando Internet de graça. É custo zero para quem usa, mas, para o Google, significa incluir 1 bilhão de pessoas. Isso é realmente transformação digital.
Por outro lado – que é o que estudei muito nos últimos dois anos –, a tecnologia tem que ser ágil para permitir essas efetivas transformações digitais. Nos últimos anos, a tecnologia evoluiu muito no lado do desenvolvimento, seja o lado de enfrentar a arquitetura Agile, os trabalhos com Scrum, etc. O Scrum é Agile, mas o Agile não é Scrum, porque nem sempre o Agile tem a ver com valores e o Scrum tem a ver com papeis e regras. É preciso ter clareza disso.
Aí vem o lado do Ops. Aliás, DevOps significa parceiros no crime. Ou você faz algo com

qualidade, ou me ajude às 3 horas da manhã, quando der um problema. Nos últimos dois anos, estudei muito a junção do Dev com o Ops. Temos muitas técnicas que estão começando agora a ser introduzidas para trazer qualidade na concepção. E tem mais um lado, que é o Sec, ainda esquecido. No DevSecOps, o Ops está começando a tentar ser natural, que é fazer um Shift Left e trazer qualidade para o começo da conversa. Porque qualidade não é uma questão acessória, é uma questão do produto, pois é no produto que se tem que pensar em qualidade. Não adianta entregar um projeto de TI que não vá ficar sustentável por dois anos, dando o resultado que a empresa precisava. O Sec deveria estar incluído, quando muitas vezes é visto como área separada. Você precisa de uma área horizontal separada de Sec para entender determinado assunto e trazer as evoluções. Mas o Sec tem que ser tão integrado quanto o DevOps, só que ainda estamos muito distantes disso, dentro das organizações. Mal estamos incluindo o DevOps. A conscientização de que qualidade é uma parte fundamental de qualquer produto [e fundamental, mas o Dev no Ops só começa a acontecer agora. O MVP (Minimum Viable Product) não é a mínima qualidade viável, é o mínimo produto viável. O produto tem que ter qualidade. O Sec ainda está distante, e aí não é uma questão de departamentalização. O Sec passa a ser gradativamente um problema de segurança da empresa e de segurança nacional. Essa conscientização só vem quando acontece um desastre maior.

**IH -** Claro que você já não pode falar em nome do Itaú, já que não está mais no banco, mas pode nos contar como era lá. Já havia pelo menos uma preocupação embrionária em fazer isso ou não?
**Bezerra -** O Itaú tem uma estrutura espetacular em termos de segurança da informação e de consciência e de defesa de perímetro. Em uma comunidade Agile, você busca quatro coisas:

Hamilton Penna

> “Temos esse modelo do DevSecOps mais bem resolvido. Por quê? Porque já temos algumas coisas implementadas nas esteiras. E porque também não temos legado”.
>
> Ricardo, da Azul

primeiro, tem que entregar rápido, porque o mundo é muito competitivo e você tem que ser veloz; segundo, você tem que entregar em sprints cada vez menores, porque tem que encantar o cliente a cada cinco dias; depois, tem que fazer com o custo mais barato e, por fim, tem que ter qualidade. O ponto é que para você entregar rápido e com sprints cada vez menores, tem que incluir nesse desenvolvimento teste e qualidade. Não pode haver delivery contínuo se não tiver teste contínuo. Não dá para acabar de desenvolver e mandar lá para o departamento de testes e esperar voltar. O mesmo acontece com a segurança, mas a segurança incluída na esteira de desenvolvimento ainda está muito distante. Já a segurança para garantir a proteção das empresas está muito evoluída, mas o Sec precisa estar na esteira contínua de desenvolvimento. Esse ainda é um desafio, pois depende de cultura, de treinamento e depende de ferramentas. A batalha de fechar o perímetro está vencida e é uma preocupação constante. Mas, cada vez mais, a segurança tem que estar integrada no primeiro minuto de concepção de um projeto. Segurança é algo com que o pessoal produto tem que estar preocupado, e não simplesmente o pessoal de segurança da informação, numa batalha solitária.

**IH -** Com a palavra, então, o Ricardo, que é justamente alguém da área de segurança da informação.
**Ricardo -** A Azul é uma empresa jovem, onde temos esse modelo do DevSecOps mais bem resolvido. Por quê? Porque já temos algumas coisas implementadas nas esteiras. E porque também não temos legado. A Azul tem dez anos e não temos nenhum desenvolvedor interno, atuamos só com fábricas de software. Então é mais fácil pedir e cobrar. Qualquer desenvolvedor, quando começa um projeto, já tem o mindset de segurança. Nós fizemos um trabalho muito grande de conscientização do time todo, com palestras e orientações. Acho que o segredo para conseguirmos fazer isso de forma mais simples é, primeiro, não ter legado. No aeroporto de Congonhas, 85% dos passageiros já chegam com o check-in feito. Você tem que ter um aplicativo que seja intuitivo e que seja rápido e fácil, em que a pessoa consiga fazer tudo isso, sem expor seus dados.

Para conseguir isso, o principal ponto é a conscientização, é você ter desde o agente do aeroporto, que pega o seu documento para fazer o check-in, até o desenvolvedor com o mesmo mindset de prestar o melhor serviço, preservando os dados pessoais.

**IH -** O fato de não ter o desenvolvimento interno não dificulta a integração entre a área de segurança e a de desenvolvimento?
**Ricardo -** Na verdade, a vantagem de não ter desenvolvimento interno é o fato de você conseguir cobrar as coisas mais rápido. Eu posso pedir, por exemplo, uma pessoa com certificação em segurança para acompanhar o desenvolvimento. É só uma contratação a mais, um aditivo no contrato. Existem várias ferramentas que permitem conferir se o código não está vindo bom. Aí é só devolver para a fábrica. É mais prático e mais rápido do que o desenvolvimento interno. Nós trabalhamos com umas oito ou dez fábricas, com diferentes linhas de produto para diferentes coisas. Mas a maioria tem um nível de maturidade muito bom. Acho que hoje a segurança também é uma preocupação dos desenvolvedores, eles querem se aprimorar. Eles já têm essa preocupação em não expor o dado além do estritamente necessário.

**IH -** Já que falamos em legado, quero ouvir o Gustavo, porque a Vale deve ser uma das campeãs nesse quesito.
**Gustavo -** Hoje, na Vale, mantemos em torno de 650 sistemas no mundo todo. O nosso projeto de transformação digital começou há dois anos e meio. Na época, chamávamos até de otimização digital, porque era muito mais uma questão de melhorar o que já existia. Agora, no último ano, já começamos a implementar soluções transformacionais, que quebram paradigmas da empresa: implementamos um centro de inteligência artificial para levar advanced analytics e video analytics para as operações. Então agora estamos começando a colher os frutos da transformação realmente. Mas é uma jornada de pelo menos três a cinco anos para conseguirmos atingir o objetivo que almejamos, que é levar tecnologia para ajudar a empresa a ser mais eficiente, a melhorar os níveis de segurança e a aumentar a produtividade. Por ser uma indústria, nós focamos muito em áreas operacionais. Hoje o nosso maior custo está na manutenção industrial. É uma empresa com muitos e grandes ativos, com alto custo de manutenção. Então colocar advanced analytics ou um algoritmo de inteligência artificial, para mostrar ao engenheiro de manutenção que ele pode fazer o trabalho de forma diferente, foi um processo em que precisamos mostrar que realmente gera benefícios, até efetivamente mudar a forma de ele operar. Um exemplo: nós temos cerca de 500 caminhões aqui no Brasil, mas caminhões do tamanho de um avião. Imaginem o custo de manutenção desse caminhão. Normalmente, a manutenção era feita como a gente faz em nossos carros: a cada 10 mil quilômetros, trocam-se alguns componentes e pronto. Com inteligência artificial e analytics, conseguimos mostrar que não é preciso necessariamente trocar determinada peça se ela ainda estiver boa. Isso trouxe um aumento muito grande de produtividade na operação e, claro, redução de custos. Agora estamos indo para o caminho realmente da transformação, mostrando que não é preciso parar o caminhão, porque ele está rodando bem. Na medida em que em que o analytics manda um alerta de que pode haver um problema, aí sim é hora de parar o caminhão. Esse é um processo transformacional. O difícil é mudar a cabeça de um engenheiro que está trabalhando há 30 anos da mesma forma. Por isso é que a gente passou pelo que chamamos de otimização digital até chegar na transformação real.

Do ponto de vista da segurança, acho que ainda falta o mindset durante o desenvolvimento. Acho que estamos no caminho, mas ainda não chegamos lá. Algumas fábricas de software usam o Open Innovation, com ferramentas abertas para ganhar velocidade, mas surgiram algumas fragilidades. Um exemplo é o desenvolvimento em que usuário e senha estão dentro do código, o que é uma clara vulnerabilidade. Nós ainda não temos a garantia de que o código é seguro.

Hamilton Penna

“O nosso projeto de transformação digital começou há dois anos e meio. Chamávamos na época até de otimização digital, porque era muito mais uma questão de melhorar o que já existia”.

Gustavo, da Vale

mesa-redonda

patrocínio

MICRO FOCUS

A gente precisa fazer auditorias e testes de vulnerabilidade para ganhar confiança. Eu gosto muito da metodologia Agile, porque sem dúvida é preciso fazer rápido, mas também é preciso pensar em gerar valor rápido. Gerar valor não é fazer a qualquer custo e de qualquer jeito. Esse é um dos nossos grandes desafios. Em indústrias muito grandes, a exposição de algumas informações pode gerar um impacto tremendo. Estamos implementando os caminhões autônomos, sem motoristas. Temos três deles em uma mina em Minas Gerais. Se houver um desenvolvimento frágil para um desses caminhões, dá para imaginar o tamanho do risco que isso representa. A gente ainda está numa postura reativa, fazendo auditorias. Precisamos evoluir nesse mindset, é uma mudança de cultura mesmo. Todas as áreas da empresa e do próprio departamento de tecnologia precisam pensar a segurança. Os grupos de inovação estão sempre com o viés de transformação, de fazer rápido, e muitas vezes não se preocupam tanto com segurança.

**Ricardo -** Uma das coisas que nos ajudaram muito foi a autonomia e o empowerment que a área de segurança teve. Chegamos ao ponto de impedir um sistema de rodar. E aí a própria fábrica voltou e perguntou: "O que nós precisamos fazer antes, para que não seja preciso parar a implementação de um App, de uma página, seja o que for?

**IH -** Já que falamos da questão cultural, de quebra de paradigmas, quero ouvir a Lilian, porque essa é uma questão crucial na área de saúde. Você já nos disse que no hospital há alguma resistência à mudança cultural.

**Lilian -** É isso. Acho que, em termos de segurança, para nós é um fato que todos seremos atacados, a gente só não sabe o tamanho do ataque. Então temos que nos preparar para que seja o menor possível, já que fechar todas as portas é praticamente impossível. Enquanto, na maioria dos setores, confidencialidade, integridade e

Hamilton Penna

"Se desde a concepção do projeto você não colocar condições de segurança para que garanta, seja a propriedade, seja a confidencialidade e a integridade do dado, você tem um problema bastante sério".

Lilian, da BP

disponibilidade costumam ser colocados no mesmo patamar, na área de saúde o que mais pega é a disponibilidade. Claro que devemos nos preocupar muito com a confidencialidade dos dados. O médico que entrega sua senha ao colega faz isso em nome da disponibilidade, para que um paciente não fique sem um medicamento, por exemplo. Esse é um desafio enorme.

Já a transformação digital na saúde passa muito pelo processo de integração: integração com o equipamento médico, integração desde uma máquina de tomografia com um monitor à beira do leito ou uma bomba de infusão. O nível de cuidado com a segurança de todos os componentes dessa cadeia não é o mesmo. A indústria de equipamentos médicos, por exemplo, evolui muito do ponto de vista de recursos de diagnóstico, mas ainda não é a mesma coisa no nível de segurança. Existem casos, por exemplo, de tomógrafos que têm a mesma senha para todos os hospitais. Por aí se vê o tamanho do desafio de segurança nessa cadeia de players dentro dos hospitais. Especialmente em função da pressão por disponibilidade: o médico precisa entregar determinado diagnóstico e não quer saber das vulnerabilidades de segurança. Por isso, o desafio que enfrentamos é o de criar essa cultura de segurança, não só interna, mas também nos players que fazem parte de toda a cadeia da saúde.
A gente fala muito em desonerar, por meio da transformação digital, o tempo assistencial; o tempo, por exemplo, que a enfermeira tem de dedicação ao paciente. A enfermeira não precisa ter que olhar o resultado do monitor cardíaco para depois digitar no prontuário. Mas na hora em que se coloca o monitor num processo de integração, é preciso tomar cuidado para que ele não se torne um ofensor de um dado que vai mudar determinada conduta. Esse é um ponto de grande preocupação para nós.
Outro ponto tem a ver com a agilidade: quando se trata de inovação, obviamente há certa dose de sedução no processo, mas essa sedução muitas vezes faz com que a segurança fique em segundo plano. Pode-se, por exemplo, ficar seduzido por testar a inteligência artificial fazendo a análise de uma imagem médica. É o caso típico em que a segurança pode acabar ficando em segundo plano.




Temos um projeto que usa inteligência artificial sobre ressonância magnética. Uma das fases desse projeto, é óbvio, era anonimizar o dado. A segunda fase era garantir que o paciente doou o dado dele. Isso porque, independentemente de eu ser a detentora do dado da ressonância do paciente, não sou proprietária desse dado, sou simplesmente uma fiel depositária. Portanto, mesmo que eu anonimize, não temos o direito de usar aquele dado, se não tivermos a autorização do paciente. Usamos o termo "doação de dados" dentro da BP, depois de um longo processo de discussão. Fazendo uma analogia com DevOps, embora eu não tenha a linha de desenvolvimento dentro da TI, se desde a concepção do projeto você não colocar condições de segurança para que garanta seja a propriedade do dado, seja a confidencialidade e integridade, você tem um problema bastante sério. Temos na nossa equipe, por exemplo, um eixo de segurança seríssimo, que parametriza um sistema que dá apoio à decisão. Se a equipe não parametrizar com precisão a identificação do deflagrador de uma sepse [*infecção no sangue*], que é algo gravíssimo em um hospital, pode-se alterar totalmente o comportamento da deflagração, o que pode gerar um dano para o hospital. Essa é uma questão de segurança. Mais do que uma questão de segurança técnica, é uma questão de segurança de processo, mas que pode causar um problema muito maior. De toda forma, concordo que o fator comportamental é a primeira etapa a ser levada em conta. Do ponto de vista técnico, as ferramentas existem, basta poder investir.

**IH -** Então, vocês ainda encaram a segurança, do ponto de vista estratégico, como a camada de proteção em um modelo tradicional, que entra depois do desenvolvimento.
**Lilian -** Na área da saúde, ainda é assim, embora não fase de integração já exista essa preocupação. Mas eu preciso considerar a questão de segurança, por exemplo, até na entrega do produto que recebo de cada fornecedor. E esse nem sempre é um assunto técnico, mas de acesso. Então quando falo do comportamental no modelo tradicional ele é ainda na base do teste e do pós, e não durante a concepção do desenvolvimento.

**IH -** Luzia, é assim também no Fleury?
**Luzia -** Eu trabalhei em algumas indústrias, como a financeira, em que a gente percebe um nível de maturidade bem maior. Se eu lhe pedir o seu banco, agência, conta e senha, você vai olhar para mim e dizer: "Está maluca?" Agora, você certamente não se preocupa em dar seu login e senha para sua secretária pegar os resultados do seu checkup. Até quando libera o acesso para o médico, dá para admitir, porque tem toda a questão ética envolvida. Mas do ponto de vista da maturidade do paciente com relação aos seus dados, a gente vê que há muita vulnerabilidade. Imagine o tamanho do desafio, não só dentro da empresa, mas até em relação ao paciente, que precisa ser sensibilizado para a importância das informações sobre a saúde dele. A partir da entrada em vigor da LGPD, então, a coisa se torna ainda mais complexa. Diferentemente de uma pesquisa, se há um exame de caráter epidemiológico, você é obrigado a reportar aos órgãos públicos responsáveis. E não é possível anonimizar a informação: é preciso identificar o paciente. Portanto há aí uma espécie de esquizofrenia entre o que é obrigatório e o que é necessário, em prol da saúde pública, seja a coletiva, seja a individual; e de outro lado a consciência do paciente sobre a relevância da informação que ele tem em mãos.

Hamilton Penna

"Hoje, na dark web, o registro de saúde é o mais valorizado mundialmente; mais até do que o dado financeiro".

Luzia, do Fleury

**IH -** Mas dá para confiar que os órgãos reguladores têm maturidade para delimitar essas exigências?
**Lilian -** Em geral, não. Recentemente aconteceu um caso que se tornou público, em que os pacientes são abordados para fazer depósitos citando o nome do médico e até o número do quarto em estava internado. Fizemos uma campanha de esclarecimento com os pacientes, mas ainda assim acaba acontecendo. Quando me perguntam quem pode saber o nome do médico e o número do quarto, eu respondo: "O mundo". Rastrear isso é um desafio enorme. Porque na verdade essa informação precisa seguir nomeada, se não ela perde o sentido.

**IH -** Provavelmente o próprio paciente colocou essas informações nas redes sociais.
**Lilian -** Sim, também.

mesa-redonda

patrocínio

MICRO FOCUS

**Bezerra -** Em relação à segurança de dados médicos, já há empresas adotando blockchain, para colocar dados de pacientes de maneira segura. Em um segundo passo, essas empresas estão se viabilizando por meio da monetização desses dados para os próprios pacientes.
O paciente permite que seus dados sejam utilizados, e é remunerado a cada vez que seu dado for utilizado. Aí, a informação de um exame em determinado laboratório pode ser valiosa para 50 outros laboratórios do Brasil, então cada um vai pagar uma certa quantia por isso. Então estão surgindo empresas que começam com a abordagem de oferecer segurança, mas ao mesmo tempo monetizo o dado, porque o cliente consente. Quando se fala em liberar o dado de um paciente é sempre no sentido de isso ser em benefício do próprio paciente.
**Luzia -** Nessa questão da monetização de dados, na dark web um dado ou um registro de saúde hoje chega a valer US$ 400. Só a título de comparação, hoje, na dark web, o registro de saúde é o mais valorizado mundialmente; mais até do que o dado financeiro. Há pouco tempo atrás, vários hospitais foram invadidos e prejudicados pelo ransomware WannaCry. Mesmo que haja o consentimento do paciente, é preciso promover a educação dele, porque em geral ele não tem noção do que está liberando quando dá um opt-in. Nós, do setor de saúde, precisamos orientá-lo, porque quando ele recebe login e senha – e já tem produto no mercado fazendo isso – da BP, do Sírio ou do Fleury, já informam que ele vai ter todos os seus exames em um único lugar. Em um primeiro momento parece muito interessante, mas não se tem clareza do que vai acontecer com aqueles dados. No setor de seguros, pode-se até dizer ao cliente que ele vai ter desconto se dirigir corretamente, se não tomar multas, etc. Em saúde, não se pode fazer coisa semelhante, por exemplo, com um diabético. Por mais que ele se alimente corretamente e tome seus remédios, não é certo

Hamilton Penna

> “Não importa se as empresas têm mais ou menos tecnologia voltada para a segurança. A grande questão é comportamental”.
>
> Rogério, da JHSF/Fasano

você oferecer um valor de prêmio de seguro saúde diferente, porque ele tem uma situação crônica.
A monetização que está por detrás disso é muito preocupante e as pessoas não têm noção.
Enfim, acho que o desafio de segurança é muito maior que tecnologia, é uma mudança cultural muito mais abrangente, porque estamos falando do paciente, do médico, da operadora, de sensibilizar e catequizar os envolvidos sobre os riscos da má utilização desses dados. Agora falando de TI, no nosso caso a gente tem sim que apostar no DevSecOps. Quando começamos a transformação digital, designamos uma pessoa específica para a área de segurança digital. Mas de fato, é um aprendizado, uma evolução de cultura, de estilo, de ferramentas. Tem hora que você está pressionado pelo prazo e, se não tem o processo correto, acaba passando muita coisa que não deveria.

**IH -** Rogério, você pode nos dar uma visão do que ocorre em várias indústrias que estão sob o guarda-chuva do grupo.
**Rogério -** De fato, atuamos em vários segmentos. Nós temos a incorporação, a administração der shopping centers e temos lojas de varejo, com marcas exclusivas. Estamos construindo um aeroporto executivo em São Roque, que deve ser inaugurado agora no final do ano, só para jatos e helicópteros. Mais recentemente, assumimos os hotéis e restaurantes Fasano.
A área de TI tem a parte de infraestrutura, segurança e desenvolvimento de todas as empresas. O pessoal de desenvolvimento, com aquela cultura de querer entregar rápido, não tinha muito foco em segurança, e o pessoal de segurança cobrando o pessoal de desenvolvimento. Recentemente, passamos por um processo que ajudou muito na mudança dessa cultura. Nós fizemos o lançamento do primeiro market place de um shopping center de luxo, o Cidade Jardim. E com alguns diferenciais. Por exemplo, o o cliente que compra até as 14 h, em São Paulo, recebe o produto até as 20 h do mesmo dia. No projeto foi definido o escopo, calculamos o retorno de investimento e ele foi implantado em três meses. O conceito é que nós não temos estoque: nós olhamos o estoque do lojista que faz parte desse market place. Então tivemos um gigantesco processo de integração de sistemas. Afinal, quase 85% dos lojistas até usavam o mesmo sistema, mas os outros 15% eram personalizados.
Esse projeto é bastante significativo, porque

dele participaram o presidente do conselho, o presidente da empresa e as unidades de negócio envolvidas. E a grande preocupação na primeira discussão foi segurança. Eles entenderam que segurança não é um projeto de TI, é um projeto da empresa. Hoje nós trafegamos dados de clientes, cartões de crédito, de débito, portanto o vazamento de uma informação dessas é muito grave. A partir desse projeto, conseguimos mudar a cultura da empresa. Não importa se as empresas têm mais ou menos tecnologia voltada para a segurança. A grande questão é comportamental. Nós estamos fazendo um trabalho de conscientização das pessoas sobre a importância da segurança, não só dentro da empresa, mas na vida pessoal de cada um. Temos uma política de segurança, de risco e compliance muito forte, com restrições rigorosas de acesso. Isso ajuda bastante a alavancar essa cultura. Internamente, estamos muito atentos à nova Lei Geral de Proteção de Dados: estamos criando um comitê, do qual a TI faz parte, mas não é a responsável, para estudar o assunto. O sponsor é da área jurídica. Apesar de hoje não termos desenvolvimento interno, temos uma empresa que faz uma avaliação sempre que entra uma nova aplicação. Eles fazem testes de vulnerabilidade antes de uma nova aplicação ser colocada em produção.

**Bezerra -** Gostei muito do que o Rogério falou. Se você pega a Apple ou a Amazon, elas não têm head de digital. O Jeffrey Bezos e o Tim Cook são os heads de digital das empresas. O CEO é o head de digital, como você falou do presidente do conselho. Independentemente do nível de conhecimento de tecnologia que eles tenham hoje, todo CEO vai ter que ser um digital no futuro. Segurança e qualidade estão na cabeça deles no início, então tecnologia e negócios não podem ficar mais distantes.

**IH -** Vamos ouvir a experiência dos representantes do setor de seguros.

**Cristiano -** Acho que estamos em uma tremenda transformação de tudo. Tudo que estamos pensando, vivendo e comprando está mudando. A segurança também. A SulAmérica é uma empresa de 123 anos, que tem 5.200 pessoas, sendo entre 500 e 600 delas em tecnologia. Portanto, tenho legado de tudo quanto é tipo. Tem legado em mainframe, que tem todas as dificuldades que vocês conhecem. Temos uns 30 squads rodando, que desenvolvem muito sobre esse mundo novo, mas também tem gente de Cobol, porque nós temos que fazer a integração de tudo. A transformação cultural está em todos os níveis. Temos tido que inovar mais, decidir mais rápido, pensar com a melhor experiência digital e entregar através dos MVPs. Por exemplo, fomos buscar um médico epidemiologista que já tinha sido product owner. Temos enfermeiros que são product owners ou líderes de vários squads. Começamos uma experiência há cerca de um ano, que chamamos de Security by Design, em que criamos as figuras de segurança que são ligadas aos squads. Então, tem alguém de segurança que também responde pelo conceito da LGPD e que está ligado a dois ou três squads, com o objetivo de, na hora em que começa a concepção do ativo digital, a consciência de segurança nascer junto. De tudo o que temos feito, onde vemos mais resultado é onde conseguimos colocar o conceito de Security by Design. É onde a pessoa de segurança está desde o início da concepção do que a gente chama de "fase de discovery dos squads", participando, escutando, entendendo e recomendando o que vai ser feito. Temos uns 25 squads rodando, e em uns 15 temos Security by Design de fato funcionando. É onde conseguimos os melhores resultados. A pessoa de segurança consegue, desde o início, aculturar e participar das decisões. Nos últimos meses, passamos a abordar a LGPD, porque LGPD e segurança têm que fazer parte do mesmo Security by Design. Então temos, na área de saúde, uma tremenda preocupação com vazamento de dados e agora, portanto, também com a LGPD. Todo ativo digital já nasce direito, com os dados protegidos e atendendo a LGPD. Junto com isso, também é bastante importante uma catraca de automação para que a gente garanta que o que está sendo desenvolvido está sendo desenvolvido corretamente. Portanto, temos software e processo para garantir o que está sendo desenvolvido, seja na fábrica interna ou do desenvolvedor de fora.

Hamilton Penna

"Na hora em que começa a concepção do ativo digital, a consciência de segurança tem que nascer junto".

Cristiano, da SulAmérica

**IH -** Você tem como medir o resultado dessa estratégia ou é puro feeling?
**Cristiano -** Isso ainda é feeling. Para a segurança como um todo, passamos a usar um framework chamado Sys Control: é um grande ISO-9000 da segurança da informação. É uma espécie de autoquestionário, em que nós respondemos sobre nós mesmos. Através do Sys Control a gente tem métricas que mostram que estamos chegando mais próximo do mundo ideal. Mas ainda é um pouco mais feeling do que métrica. Os ativos digitais que nascem nas células ou nas squads, em que temos o Security by Design do v-zero, são aqueles mais protegidos.

**IH -** Do ponto de vista de tecnologia, vocês têm ferramentas adequadas para fazer isso?
**Cristiano -** Acho que ainda não estamos atendidos por ferramentas adequadas. Mas a gente tem colocado algumas ferramentas integradas a uma esteira de DevOps que olha se o código está sendo gerado da melhor forma. Mas em algumas plataformas consigo muito mais aderência a essa esteira de DevOps do que em outras. Por exemplo, naquilo que fazemos em aplicativo móvel e em Java, é muito fácil e muito integrado, mas no que fazemos em Salesforce, nada é integrável, nada é fácil. Eu ainda tenho dificuldade em fazer o DevOps acontecer nesse mundo. Então a gente consegue colocar a consciência, mas ainda não consegue ter a esteira automatizada permeando tudo dentro de um squad. Mas está melhorando. A gente vê que há dois anos não tinha nada e hoje já temos muita coisa permeando esse mundo novo. Se a cultura nasce melhor desde o v-zero, a gente consegue um resultado melhor. Mas ainda falta ferramental.

**IH -** Imagino que seja necessário muito treinamento para criar essa cultura, com gente que está habituada a métodos convencionais, de só considerar a segurança numa camada posterior ao desenvolvimento.
**Cristiano -** É preciso muito treinamento, muito. Nós colocamos todo mundo no auditório e treinamos. Isso ainda atinge um percentual pequeno do grupo, mas já estamos ampliando a cobertura. Para desenvolver software na SulAmérica, é preciso fazer quatro ou cinco horas de DevOps, outras tantas de código seguro e do Security by Design. Pretendemos atingir 100% desse grupo para depois medirmos resultado. Eu acredito que sem treinamento a gente não faz nada, independentemente do nível das pessoas envolvidas no desenvolvimento. Mas a consciência no dia a dia, dentro das squads, que esse conceito de Security by Design traz, é o que mais transforma. Quando a pessoa vê a discussão nascer do v-zero, se engaja mais e aí ela mesmo passa a buscar o treinamento, o conhecimento.
**Lilian -** Ainda há alguma dificuldade para introduzir a questão de segurança como pré-requisito no treinamento. É algo que ainda não está em uma esteira de DevOps, mas em um processo comportamental. A gente também usou isso em relação aos médicos. Por ser um corpo clínico aberto, existe uma dificuldade, pois o médico está dentro da sua instituição porque tem pacientes lá, mas não pertence à instituição. E chamá-lo para um processo de treinamento em segurança muitas vezes é complicado. Uma das nossas iniciativas é um processo de recredenciamento anual, em que esses médicos precisam ter participado dos processos de treinamento em segurança. É difícil, porque no fundo o médico para nós não é um colaborador, é um cliente. Um dos caminhos que encontramos foi o de usar o apelo de uma certificação, um modelo de adoção, que já existe no mercado de saúde. Um dos requisitos desse modelo é que pelo menos 95% do seu corpo clínico seja treinado em segurança da informação. No processo de convencimento, precisamos dizer que, mais do que o conteúdo que o médico vai receber, vamos garantir a qualidade da adoção do prontuário eletrônico. Então, no momento do recredenciamento, introduzimos o treinamento. E o mote foi que a BP chegou a um estágio digital em que um dos critérios é segurança; portanto, para pertencer a esse grupo, o médico também precisa colaborar. Acho que são estratégias que a gente, junto com as


Hamilton Penna

> “As equipes de segurança têm que estar tão integradas e conhecendo tão bem o negócio a ponto de entender que tipo de peça o desenvolvedor precisa criar”.
>
> Sirelli, da Porto Seguro

áreas de compliance e jurídica, precisa criar, tanto para o cliente quanto para o colaborador.

**IH -** A colaboração entre equipes que estão acostumadas a trabalhar isoladamente é um desafio importante. Sirelli, como é a situação na Porto Seguro?

**Sirelli -** Antes de responder diretamente ao seu ponto, o Bezerra tocou em uma questão inicial, a da transformação digital de fato. Eu acho que talvez já estejamos no estágio de revolução digital mais do que de transformação. A gente está modificando o comportamento e a cultura das empresas, da forma de se pensar o produto desde o seu início. É algo que muda o processo de criação e não simplesmente a digitalização ou a adaptação de processos. Vejo de forma natural essa evolução da maturidade. A diferença, talvez, seja que no nosso mercado a velocidade é diferente. A indústria automobilística, por exemplo, não consegue conceber um novo automóvel sem incorporar o conceito de segurança. Nós estamos vivendo exatamente isso na indústria de tecnologia. Na Porto Seguro, temos a Oxigênio como aceleradora de algumas startups. Nas primeiras discussões, os executivos de negócio que participam do processo de seleção das startups, as perguntavam: se o modelo funcionava, se atendia o negócio dele, qual seria o custo, o design. Cabia à TI fazer perguntas de segurança. Fiquei muito surpreso e feliz de ver que no último ciclo de conversas, a pergunta sobre segurança foi a primeira e partiu de uma pessoa de negócio – o que demonstra que esse mindset começa a mudar. Na Porto Seguro, por ser uma empresa de seguros, o risco é o nosso negócio – e segurança está diretamente ligada a isso. Daí o fato de termos que trata esse assunto de maneira cada vez mais aprofundada. As ferramentas já não são mais problema, estão disponíveis, obviamente com custos ainda elevados, mas hoje o grande segredo é a forma como você vai integrar a segurança ao processo de desenvolvimento. Além da cultura, de que já se falou bastante aqui, é necessário criar uma estrutura que facilite a adoção desse conceito para que o desenvolvedor não precise criar coisas básicas a cada iniciativa. Então é necessário que exista um arcabouço de pequenas peças que ele vai juntar, para obter agilidade. As equipes de segurança têm que estar tão integradas e conhecendo tão bem o negócio a ponto de entender que tipo de peça o desenvolvedor precisa criar. Esse é o nosso desafio: a Porto Seguro é bastante conhecida pelo ramo de automóveis, mas temos diversos negócios, como cartão de crédito, investimentos, etc. E a integração é o desafio da segurança, pois é preciso integrar todos esses diversos negócios mantendo o mesmo nível de segurança. Também temos dezenas de squads funcionando com equipes multidisciplinares, e a intenção é a integração das pessoas de segurança nesses times, mas não só com o propósito de fazer o software sair com qualidade e segurança, mas de disseminar a cultura. Nesse ponto, a capacitação do profissional de segurança talvez seja um desafio ainda maior. O que estamos vivendo agora com a LGPD só vai intensificar a cobrança sobre esses profissionais, porque com ela se introduzem novas abordagens, como, por exemplo, as questões jurídicas. E, claro, vai haver um impacto muito grande sobre a tecnologia, por causa dos efeitos do novo quadro sobre todos os processos. Por isso, partimos também para a formação, para a criação interna de cursos e de estruturas para formar internamente pessoas que possam trabalhar nos nossos projetos.

Hamilton Penna

> “Hoje vivemos em um modelo mais tradicional, com auditorias, testes de invasão e de vulnerabilidade, mas já temos projetos e iniciativas no sentido de trazer isso para a esteira de desenvolvimento”.
>
> Bambace, da Vigor

**Ricardo -** Como todos sabem, na aviação a segurança é algo levado muito a sério. Desde o agente do aeroporto ao funcionário que coloca a mala no avião, todos têm autonomia para intervir, caso detectem algum problema de segurança. E isso facilita a criação de uma cultura de segurança muito apurada dentro da empresa. As pessoas que identificam algum problema de segurança, e interrompem algum processo por isso, são reconhecidas, são premiadas por exercerem a prevenção. É uma característica desse tipo de indústria.

mesa-redonda



**Sirelli -** Você tem razão: isso já está impregnado no processo e no conceito. Se formos pensar em nós como usuários e motoristas, por exemplo, basta lembrar que há até pouco tempo atrás, o cinto de segurança não era obrigatório. Os carros tinham o equipamento, mas as pessoas só passaram a usá-lo intensivamente no momento em que a obrigatoriedade de usar virou lei. Num primeiro momento, as pessoas passaram a usar não em função do conceito, da mudança do mindset, mas sim porque queriam evitar a multa. Hoje, quem de nós aqui deixaria de usar o cinto se não fosse mais obrigatório? Essa é a grande questão: como é que nas corporações a gente introduz a cultura de segurança da informação, que não está só em tecnologia? Acho que esse é o grande desafio.

**IH -** Mas a integração das áreas de TI el de segurança é fundamental. Isso acontece porque as pessoas já estão imbuídas de que é necessário desde o começo, ter o conceito de segurança embutido no desenvolvimento?

**Sirelli -** Sim. Inclusive nos nossos processos já existem mecanismos automáticos, desde o deploy, em que você garante que alguns conceitos não passam, que há barreiras. Obviamente é sempre um processo evolutivo. Na construção de apps já há mecanismos de segurança pré-montados e que são reutilizados, o que garante também atualizações mais rápidas e conceitos mais simples. Como a Porto é bastante ampla, tendo vários negócios, o nosso desafio está nessa integração. Há níveis de maturidade diferentes por estrutura de negócio. Queremos equalizar para que adotemos, como um todo, um patamar maior de maturidade.

**Bezerra -** Tem um aspecto importante que é o fato de códigos serem desenvolvidos de maneira colaborativa. Em muitas situações, tem acontecido de colaboradores incluírem códigos maliciosos no corpo do código colaborativo que está sendo desenvolvido. Os desenvolvedores

Hamilton Penna

> “O time to market é um grande complicador. Acho que esse é o grande obstáculo cultural a ser superado, tanto na área de negócio quanto na área de tecnologia”.
>
> Wilson, da Tokio Marine

não perceberam, porque é algo muito bem construído, e aquilo entra em produção, expondo os dados de clientes. Então mesmo dentro de um ambiente que seja colaborativo, tem que haver uma forma de auditar. Ou seja, a segurança transcende um pouco a técnica e até o processo como um todo. Não dá para ser amador.

**Wilson -** Quero voltar ao cerne da discussão, o de ser digital e, ao mesmo tempo, se preocupar com segurança. Acho que, do ponto de vista da tecnologia, precisamos considerar alguns pontos fundamentais: desenvolvimento; infraestrutura própria; e serviços, tanto em nuvem quanto em empresas parceiras. Todo mundo falou aqui e eu concordo: acho que o ponto principal é a cultura. Somos uma empresa multinacional, com 40 subsidiárias ao redor do mundo. A Tokio enfatiza muito a importância de investir em segurança. É uma cultura que está sendo moldada desde o CIO global até chegar ao analista básico de tecnologia. Esse para mim é o diferencial, é onde vamos ganhar o jogo. Concordo com o Sirelli em que o time to market é um grande complicador. Acho que esse é o grande obstáculo cultural a ser superado, tanto na área de negócio quanto na área de tecnologia. Quanto ao desenvolvimento, há mais de um ano, mudamos bastante a forma de fazer sistemas dentro de casa. Hoje temos quase 100% de desenvolvimento interno. Praticamente não temos pacotes, a não ser contabilidade e RH, para as coisas básicas. Então, ao mesmo tempo em que traz um pouco mais de desafio, isso nos dá flexibilidade. A gente decidiu que o pessoal de desenvolvimento tem que participar em todos os projetos de segurança. Além de dispor de ferramental, pois isso já é básico. É fundamental sempre olhar além de cada projeto. LGPD é um ponto relevante agora, então vamos olhar além. Como vamos tratar disso? Você precisa expor o dado para o parceiro? Isso precisa estar na tela do app? Então você começa a pensar sobre uma porção de coisas na área de segurança, e começa a quebrar paradigmas. Outra coisa importante é dar ao profissional de segurança o poder de travar um deploy: não vai entrar isso aqui porque não está seguro. Ele tem autonomia para barrar e mudar o curso de projetos. Criamos o programa Tokio Winners, que todo mês tem um novo tema. Por exemplo, por que não usar pendrive, os cuidados a se tomar com o Whatsapp, etc. É uma conscientização não só de tecnologia da empresa, mas de tecnologia pessoal. Isso




está mudando a mentalidade dos funcionários, e está nos auxiliando a andar nessa jornada.

**Bambace –** A partir do momento em que chegam à empresa notícias de ocorrências, cresce a sensibilização com a questão da segurança. Fiz uma reunião há pouco tempo com o CFO global em que ele mostrou casos de invasão de outras empresas. A preocupação dele denota uma mudança de cultura. Ainda é um um desafio, porque a preocupação das empresas ainda com a segurança ainda está muito centrada em tecnologia e não tanto na no conjunto dos negócios, mas começo a ver executivos que até recentemente tinham pouco envolvimento começarem a se envolver com a questão da segurança em fóruns de tecnologia. Tenho experimentado isso a partir da fusão da Vigor com a Lala, mexicana, há pouco menos de dois anos. Começou-se a dar mais força ao setor de segurança da informação para entrar na esteira de desenvolvimento, em um processo mais constante do dia a dia. Hoje vivemos em um modelo ainda mais tradicional, com auditorias, testes de invasão e de vulnerabilidade, mas já temos projetos e iniciativas no sentido de trazer isso para a esteira de desenvolvimento.

**IH –** Essa barreira é decorrente da cultura mais conservadora de uma indústria de alimentos como a Vigor?

**Bambace –** Exatamente. É a questão de você, cada vez mais, romper barreiras do custo de trazer segurança como componente essencial e não como componente acessório. Você tem que ter em todo o modelo. A Vigor é uma empresa tradicional, de mais de 100 anos no segmento de alimentos e que faz 90% de todo o desenvolvimento dentro de casa. Então existe uma política nesse tipo de empresa, de trabalhar as ideias na concepção. Tem-se a concepção de que que, quando se terceiriza o desenvolvimento, há um custo conhecido do processo; quando se faz dentro de casa, tem sempre a visão de que não custa nada. Então você precisa começar a trabalhar as ideias lá atrás, para saber exatamente no que vai colocar seu esforço para agregar valor ao negócio. A partir do momento em que entrou no desenvolvimento, é lá que se vai acompanhar até a ponta. Se você tem um problema lá na produção, é o Dev que vai se envolver para resolver. Lá na ponta, temos que atender a um prazo, pois toda empresa precisa de agilidade, mas de outro lado tem que atender a um nível de excelência em qualidade, para manter o ambiente de tecnologia sempre de forma sustentável e estabilizado nas implantações. Mas o cuidado é nessa passagem, que o Dev acompanhe o Ops lá na ponta.

**Lilian –** Acho que a segurança tem o viés de ser um custo não materializável para o cliente. Eu não vou pagar uma taxa de administração maior para ser cliente do banco A ou B, porque um deles é mais seguro que o outro. Quando consome, a gente não leva em conta o benefício da segurança da informação, leva em conta o diferencial do produto. Quando a gente fala da informação, o dinheiro se materializa na perda, no dano. Isso cria um desafio maior quando se fala em investimento, porque não se consegue ser tangível para o cliente, e nos faz parar para pensar no tamanho das nossas equipes. Será que tenho o contingente necessário de segurança, ou centralizo porque é uma questão técnica, ou é uma questão de orçamento porque não consigo?

**Sirelli –** Acho interessante o ponto que você traz, de que as pessoas não tratam a sua informação com o viés de segurança. Mas talvez por aquilo que o Bezerra falou, que ainda é estranho ainda de considerar a informação um ativo efetivo, a ponto de a pessoa poder vende-la, e aí talvez esteja um acelerador para essa conscientização. Todo mundo entende que dinheiro é um ativo, que não se deixa em qualquer lugar, porque pode perder. Quando o dado passar a ser um asset, que pode ser monetizado, a percepção de valor passa a ser maior e, consequentemente, a preocupação com a segurança também passa a ser maior.

**Lilian –** A gente tem a sedução pelo aplicativo, mas acaba fornecendo dados que não gostaria que fossem usados por terceiros.

**Wilson –** Mas acho que a LGPD vai levar à monetização do dado pessoal.

**Lilian –** Também acho isso.

**Wilson –** A lei prevê a chamada portabilidade do dado, que vai permitir isso.

**IH –**Mas isso vai exigir a manifestação explícita do dono do dado e aí ele vai poder cobrar um preço pela portabilidade, por exemplo.

**Sirelli –** Ele vai poder fazer isso.

**Wilson –** Ainda não está claro na LGPD, mas pode acontecer essa monetização, sim.

**IH –** Trazendo um pouco a discussão para os testes de qualidade de software, vocês já adotam alguma estratégia de automação para chegar ao Shift Left nesses testes?

**Ricardo –** Na Azul, até como parte do DevOps, a gente já começa a fazer muita coisa. Na nossa linha do tempo tem um marco que é assim: de um determinado ponto para a frente, começamos a realmente usar as práticas de DevOps. Nós trouxemos arquitetos do mercado para nos ajudarem com isso. Então, desse ponto para a frente, por exemplo, já desenvolvemos com o teste automatizado, uns 60% do total. Mas existe, sem dúvida, aquilo que está desse marco para trás, uns 40%, e aí a gente parte para o teste tradicional, com todos os desafios que se conhece. É o caso de alguns legados, coisas muito específicas, como o software de controle de combustível. Esse ainda está lá em uma plataforma não muito automatizada.

**IH –** Bezerra, os bancos já fazem isso regularmente?

**Bezerra –** Eu diria que há alguns desafios que são vencidos por etapas, em que você vai colocando stakes de disciplinas. O primeiro desafio no




banco é o de realmente aumentar a cobertura de testes. Isso significa desde o básico, de você ter RTF em um projeto. Por incrível que pareça, isso é um problema. É preciso ter, antes da automação, um ambiente de testes e um ambiente de homologação, e ter massa de dados para, aí sim, ter automação. No Itaú, foi até criado um programa chamado Zero Erro. Depois disso, na medida em que aumenta a cobertura, ela começa a trazer alguns benefícios adicionais, como reduzir o tempo de homologação.

A partir daí tem um outro ponto, que é o de reduzir live time para você ir além do funcional. Quer dizer, testar performance, acessibilidade, que é muito diferente de funcionalidade. A acessibilidade é outro mundo. Então você tem que aumentar a cobertura de testes, reduzir o live time de homologação e ir além do funcional. Aí vem o último ponto, que é o descobrir erros mais cedo, que é o Shift Left, que é você trazer qualidade para o começo do processo. Uma vez que vai bem nesse Shift Left, aí se pode fazer o Shift Right, que significa ir para Case Engineering. Tem muita gente que parte direto para Case Engineering, sem saber onde está se metendo. Então tem alguns passos que lhe permitem: expandir a cobertura de testes; reduzir o live time de homologação; fazer testes além do funcional; e descobrir erros mais cedo.

A qualidade tem um escopo de trabalho enorme, que nos obriga a trabalhar para que o sistema se deteriore o mínimo possível. A qualidade vai além do teste: é trazer qualidade no contexto de pensar no projeto, já pensando na pessoa de operação no primeiro minuto. E é preciso pensar em monitoramento, em debuging, em login, em várias outras situações que a princípio hoje se costuma deixar para o pessoal de operação descobrir na hora em que o projeto está no ar.

**Gustavo -** Essa é uma área superimportante e que evoluiu muito. São vários temas e várias disciplinas relacionados à qualidade como um todo. Hoje nós temos na Vale um grupo específico de aplicações, que a gente considera de alto impacto. Do total de 650, 45 classificamos como de alto impacto. Para essas, nós temos toda uma estrutura de qualidade envolvendo automação e envolvendo testes, inclusive de performance, não só com os robôs das ferramentas, mas com patches nas regiões. Porque o que acontece muito conosco é que uma ferramenta desenvolvida que está hospedada no nosso datacenter do Canadá, tem uma performance lá, mas na Indonésia pode ter outra. Então, nós colocamos robôs espalhados pelas regiões onde são acessadas, para garantir a qualidade devida para o usuário final, quando é feito o deploy.

Em função da qualidade e também da segurança, assumimos recentemente a área de automação industrial da empresa. É uma área em que o tema da qualidade tem essa disciplina, que é a primeira que a gente implementa quando assume. Vimos que na área industrial não se testa, por exemplo, o sistema de controle da usina: coloca-se em produção e depois se vê o que acontece. Com as disciplinas, começamos a ver benefícios, como os de horas de disponibilidade na área industrial, em função da atenção prévia com testes de qualidade, de performance. Mas, de novo, a gente investe especificamente onde é prioritário. Então, no nosso caso, evoluímos para os ambientes de alto impacto. Aí, sim, tem toda uma esteira diferente de qualidade para garantir o produto ao final.

**Sirelli -** Acho que o Bezerra deu uma boa organizada nas escalas que temos de evolução de qualidade, de como é que a gente avança. Mas por mais que a gente fique sofisticado, vão existir falhas. Existe uma componente importante, que é a reação à falha, que ainda é preciso sofisticar. Porque por mais que a gente ache que aumentou o nível de qualidade, testando e simulando melhor a performance, quando vamos para o ambiente produtivo muitas vezes é impossível reproduzir a situação em 100% dos contextos que acontecem em ambiente integrado, inclusive com coisas externas à companhia. O que a gente precisa buscar cada vez mais é reações à falha de maneira mais rápida e estratégias de implantação que mitiguem esse impacto. É em uma camada básica e que a gente sempre fez com força bruta, mas agora as ferramentas são mais sofisticadas e os processos são mais automatizados. Mesmo assim, vai haver um limite em que vamos ter que assumir certo nível de risco, em favor de sermos mais rápidos e ágeis. A questão é que esse risco tem que ser mitigado por uma estratégia e uma arquitetura que possam possibilitar uma reação rápida. A gente falou muito aqui dos legados, mas muito de tecnologia é limitado nesse aspecto. É essa evolução que precisa acontecer. Acho que a questão dos parceiros é um capítulo à parte nesse processo, porque as escolhas precisam ser bem discutidas. Não são simplesmente SLAs que vão limitar isso. É preciso haver parcerias mais orgânicas do ponto de vista de propósito. Se eu estou atendendo a um hospital, por exemplo, qual é o meu compromisso final com aquele cliente? Se não houver isso, vai ser muito difícil gerenciar somente por força de contrato.

**Wilson -** Mas, esse é um ponto complicadíssimo, porque estamos nos voltando contra a indústria do crime. A gente sempre está atrás, tentando corrigir aquilo que está vulnerável a ataques. Esse é outro ponto em que não vejo saída. A gente vai continuar investindo em parceiros e em soluções de segurança lá na ponta, mas vai ter que conviver com isso o resto da vida

**Lilian -** Uma iniciativa eficaz é falar desde o compliance, já começa por aí. Quando se fala em equipamento médico, isso é muito mais gritante. É preciso trazer o fornecedor para perto e fazer com que ele entenda que é um dos requisitos para que ele continue sendo seu fornecedor. Isso ainda é muito complicado, especialmente no segmento de saúde.

MicroFocus

# Enterprise DevOps

## Produza softwares com agilidade e qualidade

A entrega de valor ao negócio na economia digital requer uma abordagem ágil. As soluções Micro Focus permitem integrar o poder de DevOps em ambientes de TI Híbrida – permitindo a entrada de inovações na velocidade das demandas de negócio. Agora velocidade e qualidade podem andar de mãos dadas.

**www.microfocus.com/pt-br/trend/enterprise-devops**

MICRO FOCUS®