NF-e 4.0 e ERP: o que muda para as empresas depois do dia 2 de julho?

Robinson Idalgo (*)

Dia 02 de julho de 2018. Esse é o seu prazo final para adotar de vez a NF-e 4.0

O novo formato da nota fiscal eletrônica já está disponibilizado para uso desde 2017, junto com a sua versão anterior, a NF-e 3.10. O Governo permitiu a utilização dos dois formatos para que os comerciantes e os desenvolvedores de soluções de emissão de NF tivessem tempo hábil para adequar os programas e se adaptarem ao novo modelo. Se você usa uma solução fiscal que esteja atualizada com as exigências governamentais, certamente já está apto a utilizar a nova versão 4.0.

Com o prazo chegando ao fim, a versão 3.10 para de funcionar e apenas a 4.0 passa a ser aceita. Na prática, isso significa que os emissores terão mais algumas informações para preencher no documento, mas nada que cause muita dor de cabeça, principalmente para quem já trabalha com uma boa solução de ERP.

A Nota Fiscal Eletrônica no Brasil começou a valer em 2006 e foi recebida com certa desconfiança. Hoje, sua emissão já virou rotina, com mais de 17 bilhões de notas emitidas por mais de 1 milhão de emissores, segundo o site oficial da NF-e.

Depois do dia 2 de julho de 2018, apenas a versão 4.0 será aceita pela Secretaria da Fazenda. O arquivo XML que passa a ser gerado terá um novo layout, definido pela Nota Técnica 2016.002 em novembro de 2016 e atualizado em abril de 2017.

Entre as principais mudanças, podemos destacar a adoção do protocolo TLS 1.2 ou superior, ficando proibida a utilização do protocolo SSL. Essa mudança chega para garantir mais segurança durante o processo de envio da Nota Fiscal, já que o protocolo SSL apresenta algumas vulnerabilidades. Também temos algumas modificações nas regras de validação, para atender os novos campos ou controles.

Em relação ao seu conteúdo, talvez a principal mudança seja referente ao campo especial do Fundo de Combate à Pobreza (FCP), que recebe recursos do ICMS. No novo layout, temos campos relativos ao FCP para operações internas ou interestaduais, com ou sem a substituição tributária. O valor devido, de acordo com o percentual do imposto recolhido, deve ser identificado nos campos pré-determinados. Também recebem novos campos a base do cálculo e a ocorrência de retenção aplicada ao FCP.

Outra mudança importante fica por conta do campo indicador da forma de pagamento, que passa a integrar o Grupo de Informações de Pagamento. Antes ele se restringia a informar se o pagamento aconteceu à vista ou a prazo, mas agora é preciso informar também qual o meio de pagamento utilizado: dinheiro, cheque, cartões de débito ou crédito, vale alimentação, entre outros.

Para as empresas, outras novidades significativas da NF-e 4.0 são: a possibilidade de preencher "operação presencial, fora do estabelecimento" no campo "Indicador de Presença" (isso ocorre no caso de venda ambulante); a Nf passa também a aceitar duas novas modalidades de frete: o transporte próprio por conta do remetente e transporte próprio por conta do destinatário.

O novo layout passa a contar com o "Grupo de Rastreabilidade de Produto", que permite o rastreamento de itens sujeitos a regulações sanitárias, como bebidas, itens odontológicos ou defensivos agrícolas. As empresas que trabalham com medicamentos devem informar na NF-e o código da ANVISA (Agência Nacional de Vigilância Sanitária) em um campo específico do documento.

Como você pode ver, a evolução da NF-e 3.10 para a NF-e 4.0 é na verdade uma série de mudanças técnicas, mas que não devem atrapalhar a rotina das empresas. Se sua organização já possui um ERP de qualidade, que acompanha todas as novidades e demandas da Secretaria da Fazenda, e que cumpre com o seu papel de acompanhar seus clientes e oferecer sempre o melhor serviço, certamente já está preparado para as novidades da NF-e 4.0. A mudança da Nota Fiscal Eletrônica chega para acompanhar a evolução da nossa economia e os ERPs atuais já estão preparados para este momento.

(*) É fundador da SoftUp – empresa brasileira criadora do sistema de gestão* (ERP) grátis. Mais informações no site: www.sistemagratis.com.br.

A identidade é o novo perímetro

A figura do hacker encapuzado, vasculhando o computador na calada da noite, buscando falhas em sistemas está no imaginário de cada nós. Porém, mais fácil do que investigar brechas é ter acesso às informações de uma empresa diretamente, certo? Pois quantos de nós já entregamos nas mãos de cibercriminosos nossas credenciais corporativas?

Eduardo Bernuy (*)

Isso mesmo. Cada vez que não trocamos as nossas senhas nos períodos em que nos é exigido, usamos nosso e-mail corporativo para criar uma conta em um aplicativo ou realizar uma compra em um e-commerce, ou mesmo clicamos em um e-mail sem refletir muito a respeito, mesmo notando que ele tem algo que foge ao padrão da empresa, estamos entregando nas mãos de criminosos as nossas credenciais corporativas e facilitando seu acesso às informações dos locais onde trabalhamos.

A partir de brechas, os hackers passam a conhecer um pouco mais sobre a empresa, estudar sua cultura e criar e-mails falsos, justamente incentivando o clique para disseminar vírus, derrubar sistemas, entre muitas outras possiblidades. Tudo o que eles precisavam era de uma brecha que nós mesmos demos. Além disso, nem é preciso ser um "hacker profissional" para provocar estragos: qualquer pessoa, mesmo com pouco conhecimento de tecnologia, pode ter acesso, na deep web, a um verdadeiro cardápios de cibercrimes, escolher o que desejar e usar as credenciais corporativas para disseminar ataques cada vez mais sofisticados. Trata-se do "CaaS – Cybercrime as a service" e, com ele, a propagação de ataques de sequestro de dados (Ramsonware), com poder de parar toda uma operação, a popularização do Cryptojacking, motivados pelo crescimento das criptomoedas, e que podem detonar o poder computacional de empresas, entre outros tipos.

Com as credenciais, os criminosos podem acessar redes remotamente, dados armazenados na nuvem ou orquestrar um ataque maior, com forte poder de destruição. A Computerworld lembra do case Shamoon 2 que causou três grandes ondas de ataques na Arábia Saudita, utilizando uma combinação de ferramentas legítimas e scripts para promover reconhecimento de rede, roubo de credenciais e entregar um trojan de capacidade altamente destrutiva, o Disttrack.

Grandes vazamentos vieram a público recentemente – Uber, Facebook, Netshoes – mas o problema é muito maior do que se imagina. Relatório da consultoria Javelin Strategy e Research, divulgado recentemente, mostra que o número de vítimas que tiveram seus dados vazados cresceu 16% somente nos EUA, chegando a 15 milhões, sendo que entre eles, desde indivíduos até grandes corporações. Outro exemplo conhecido é da operadora de telefonia móvel Swisscom: os dados pessoais de um em cada dez residentes na Suíça estavam comprometidos.

Em 2016, o roubo de identidade já era considerado o principal crime de violação de dados do mundo. Segundo o Relatório do Breach Level Index1, 1792 violações de dados comprometeram quase 1,4 bilhão de registros de dados do mundo inteiro de 2016, um aumento de 86% em relação ao ano anterior.

O Brasil, por sua vez, já é considerado polo do cibercrime mundial, ao lado de Índia, Coreia do Norte e Vietnã, alvo número um e a principal fonte de ataques na América Latina, segundo estudo recente da McAfee e a CSIS. Mas uma característica peculiar dos crimes cibernéticos aqui é que 54% deles são originários do próprio país, demonstrando que temos um ecossistema de cibercrime diferente do resto do mundo. Será que não estamos contribuindo para este cenário ao negligenciar nossa identidade corporativa?

Assim, não adianta apenas trabalharmos com as seguranças do perímetro, com firewalls e outros métodos cada vez mais inteligentes e rebuscados se entregarmos nosso crachá diretamente nas mãos dos criminosos. A reflexão fica para cada um de nós e a lição, no mundo do cibercrime é que a identidade definitivamente se tornou o novo perímetro e todo cuidado é pouco.

Sobre Eduardo Bernuy - Diretor de operações - Redbelt

(*) É um dos fundadores da Redbelt (2009) e responsável pela coordenação de projetos e soluções relacionadas à cibersegurança.

Entenda o impacto de ignorar o ROI dos seus produtos de segurança digital

As empresas estão investindo cada vez mais em segurança. Segundo o Gartner, em 2018, as organizações vão gastar US$ 96 bilhões em produtos e serviços de segurança, mas será que esses investimentos vão de fato ajudar a reduzir o impacto das ameaças? Infelizmente, em muitos casos, não é isso que acontece.

No Brasil, a ascensão dos ataques cibernéticos tem impulsionado os investimentos em segurança da informação. O país, segundo um estudo divulgado pelo IDC no início deste ano, é alvo de parte significativa dos ataques cibernéticos e, junto de Argentina e México, é um dos países com maior número de ataques detectados por ano. A evolução dos ransomwares é um dos fatores que levou a um aumento de 10% a 12% dos orçamentos dedicados à segurança.

De acordo com o estudo do IDC, a maioria das empresas brasileiras está investindo, principalmente em soluções antimalware e servidores de segurança para pontos terminais, bem como em áreas relacionadas à segurança móvel e em firewall. Apesar de o investimento na adoção de novas tecnologias de segurança ser um passo importante, existe uma grande controvérsia relacionada ao ROI de algumas dessas ferramentas em determinados ambientes.

Por incrível que pareça, mesmo que boa parte dos líderes de segurança contem com alguns indicadores chaves de performance para monitorar e medir as atividades da sua área, não contam com um processo ou uma abordagem para medir a efetividade dos controles de segurança, o que pode levar a uma série de equívocos e a um ambiente lotado de soluções que pouco agregam valor, tornando a infraestrutura de TI ainda mais difícil de gerir e proteger.

Um estudo divulgado pela Varonis no último ano confirma isso, revelando que 76% dos profissionais de segurança creditam o nível de maturidade de sua estratégia de segurança a investimentos em ferramentas individuais. Investir em uma estratégia de soluções pontuais de segurança, no entanto, pode até mitigar algumas ameaças específicas, mas, sem que haja um uso mais tático, o ROI desses produtos acabar sendo baixo.

Os benefícios de calcular o ROI do ambiente de segurança

Uma das maneiras de garantir um maior ROI na infraestrutura de produtos de segurança é contar com uma abordagem baseada em métricas, focada em justificar investimentos. Dados recentes mostram que poucas empresas calculam o ROI de seus controles de segurança.

O cálculo do ROI e o oferecimento de métricas relevantes vão dar ao líder de segurança a possibilidade de enfrentar a difícil posição de ter de explicar que a causa de uma violação de dados foi a falta de um controle específico que foi cortado do budget, por exemplo.

Ao incorporar mais análise de dados e evidências empíricas, por meio da análise de incidentes de segurança e ameaças combatidas no cotidiano – acompanhadas do impacto que teriam se não tivessem sido detidas –, é possível demonstrar a efetividade dos programas de segurança. Mais do que apenas juntar dados de invasões, é essencial relatar o valor obtido na linguagem dos executivos, ressaltando o que a empresa poderia ter perdido em termos de negócio, como perda de propriedade intelectual, roadmaps de produtos e informações sensíveis de clientes e funcionários, e danos permanentes à reputação.

Além disso, é importante destacar que, muito mais importante do que investir em tecnologias de segurança, é fundamental estar atento ao nível de visibilidade do ambiente. Você sabe onde estão seus dados sensíveis? Sabe se eles estão classificados de forma apropriada? Sabe quem tem acesso a eles? Sem essas informações básicas do que deve ser protegido, é praticamente impossível entender quais são as soluções que vão dar mais suporte à sua estratégia de segurança, o que, consequentemente, vai acabar gerando um ROI preocupante.

(Fonte: Carlos Rodrigues, vice-presidente da Varonis para América Latina).

News @TI

Futuro da IoT e Blockchain são destaques de evento em São Paulo

@Tecnologias como internet das coisas, inteligência artificial e blockchain estão revolucionando a maneira de pensar, interagir e viver em sociedade. As mudanças nos hábitos, comportamentos e os impactos dessa transformação no mercado serão destaques da SGTI 2018 – Semana de Gestão, Tecnologia e Inovação. O evento, que acontece pela primeira vez em São Paulo, será realizado no Centro Universitário UNIBTA, nos dias 4 e 5 de junho.Serão dois dias de palestras, exposições e debates reunindo especialistas do Brasil e do mundo. O principal destaque do evento será a participação do Ph.D. Huseyin Ucar, professor da Universidade da Flórida. O docente apresenta painel sobre a evolução da tecnologia e as projeções para o futuro. Profissionais da IBM, TOTVS e especialistas da USP e do próprio UNIBTA, completam a lista de palestrantes. O evento, voltado para o desenvolvimento de novas práticas, modelos gerenciais e inovações empresariais, tem como objetivo agregar valor ao mercado e potencializar novos negócios na região. O encontro é gratuito, mas para participar das palestras é necessária inscrição prévia, que pode ser realizada pelo site: https://www.sympla.com.br/grupocetec.

Jovens brasileiros criam ferramenta preditiva

@Após cinco meses de muitas pesquisas e análises, jovens colaboradores da GE Celma, em Petrópolis (RJ), unidade da GE Aviation no Brasil, criaram uma ferramenta preditiva pioneira no mundo. Batizada de PATMOS, a inovação é capaz de analisar em milésimos de segundo a performance de 250 parâmetros na montagem de um motor aeronáutico, ou seja, mais de 10 milhões de dados capazes de indicar se determinado motor será aprovado ou não no banco de provas, a etapa final do processo de reparo de motores. O método possibilita detectar digitalmente o problema e corrigi-lo antes de finalizar a montagem do motor e do mesmo ir para o teste. "Com o PATMOS, a expectativa é alcançar 100% de assertividade na previsão dos dados e o número de reprovações pode tender a zero. Este será mais um diferencial competitivo da GE Celma, visto que a empresa já consegue realizar a completa revisão de um motor, incluindo recebimento, desmontagem, limpeza, inspeção, remontagem, testes e expedição, entre 60 e 65 dias. Um recorde no mercado mundial de aviação", diz Rodrigo Araújo, da área de Planejamento de Produção, e um dos idealizadores.

Vendas de televisão tendem a crescer 5% no período da Copa

As datas sazonais aquecem o varejo durante o ano, e na Copa do Mundo não é diferente. Para impulsionar as vendas de TVs no período, por exemplo, muitas lojas e magazines criaram promoções e condições especiais e atraíram a atenção dos consumidores. Segundo Claudio Felisoni, presidente do Instituto Brasileiro de Executivos de Varejo e Mercado de Consumo (IBEVAR), a venda de TVs, motivada especificamente pela Copa, gira historicamente em torno de 5% do total.

O especialista acredita que os fãs do futebol não são mais reféns do aparelho e podem optar por outros produtos como celulares, tablets e laptops. "Em campeonatos passados, o consumidor tinha que ter uma TV para assistir aos jogos, agora pode optar por outros aparelhos", diz Felisoni. Entretanto, o professor explica que consumidores "novidadeiros" tendem a ceder e adquirir novos produtos com frequência, ainda mais em datas especiais, como na Copa. Já pessoas menos propensas a gastar com novidades, normalmente, esperam os preços diminuírem ou ficam de olho nas promoções (www.ibevar.org.br).