

**BOAS PRÁTICAS TECNOLÓGICAS NA AUDITORIA DE SISTEMAS
ALTERNATIVOS DE CONTROLE DE JORNADA DE TRABALHO PARA
AVALIAÇÃO DE CONFORMIDADE COM REGULAMENTAÇÕES BRASILEIRAS¹**

***GOOD TECHNOLOGICAL PRACTICES IN AUDIT OF ALTERNATIVE WORK SHIFT
CONTROL SYSTEMS FOR ASSESSMENT OF CONFORMITY WITH BRAZILIAN
REGULATIONS***

***BUENAS PRÁCTICAS TECNOLÓGICAS EN AUDITORÍA DE SISTEMAS
ALTERNATIVOS DE CONTROL DE TURNO DE TRABAJO PARA LA EVALUACIÓN
DE LA CONFORMIDAD CON LAS NORMAS DE BRASIL***

Alessandro Santiago Santos, Pesquisador do Instituto de Pesquisas Tecnológicas (IPT) do Estado de São Paulo, Doutorando em Engenharia e Mestre em Ciência da Computação pela Universidade de São Paulo (USP). Endereço Profissional: Av. Prof. Almeida Prado 532 Cid. Universitária - Butantã. São Paulo/SP –Brasil, CEP 05508-901, Telefone: +55 (11) 3767-4000. URL da Homepage: <http://www.ipt.br>. E-mail: alesan@ipt.br

Leandro Avanço, Pesquisador do Instituto de Pesquisas Tecnológicas (IPT) do Estado de São Paulo, Mestre em Engenharia da Computação pelo IPT. Endereço Profissional: Av. Prof. Almeida Prado 532 Cid. Universitária - Butantã. São Paulo/SP –Brasil, CEP 05508-901, Telefone: +55 (11) 3767-4000. URL da Homepage: <http://www.ipt.br>. E-mail: lavanco@ipt.br

Maria Cristina Machado Domingues, Pesquisadora do Instituto de Pesquisas Tecnológicas (IPT) do Estado de São Paulo, Mestre em Engenharia da Computação pelo IPT. Endereço Profissional: Av. Prof. Almeida Prado 532 Cid. Universitária - Butantã. São Paulo/SP –Brasil, CEP 05508-901, Telefone: +55 (11) 3767-4000. URL da Homepage: <http://www.ipt.br>. E-mail: cmachado@ipt.br

Denis Bruno Viríssimo, Pesquisador do Instituto de Pesquisas Tecnológicas (IPT) do Estado de São Paulo, Mestre em Engenharia da Computação pelo IPT. Endereço Profissional: Av. Prof. Almeida Prado 532 Cid. Universitária - Butantã. São Paulo/SP –Brasil, CEP 05508-901, Telefone: +55 (11) 3767-4000. URL da Homepage: <http://www.ipt.br>. E-mail: denisbv@ipt.br

RESUMO

O Ministério do Trabalho e Emprego (MTE) elaborou duas Portarias que objetivam disciplinar o registro eletrônico de ponto de empregados, a fim de minimizar os problemas decorrentes do controle de jornada de trabalho. A Portaria 1.510 instituiu o equipamento de Registro Eletrônico de Ponto (REP), que é um *hardware* com inteligência fiscal embarcada. No entanto, a Portaria 373 permitiu o uso de Sistemas Alternativos de Controle de Jornada, os quais poderiam ser baseados em *software*. Contudo, esse sistema deve atender a uma série de exigências para apresentar conformidade legal com a regulamentação do MTE. Assim, as

¹ Artigo submetido em 13/08/2014, revisado em 28/09/2014, aceito em 19/10/2015 e divulgado em 30/06/2016 pelo Editor João Carlos Hipólito Bernardes do Nascimento, após *double blind review*.

empresas devem incorporar mecanismos de auditoria de sistemas para avaliar o cumprimento dessas exigências. Este artigo apresenta uma metodologia de verificação de conformidade de tais sistemas, destacando o diagnóstico padrão e vulnerabilidades encontradas através de estudos de casos. Dentre as contribuições deste artigo está a apresentação das boas práticas e mecanismos tecnológicos que minimizam os riscos de não conformidade com as regulamentações brasileiras.

Palavras-chave: MTE, Auditoria de Sistemas, Controle de Ponto, Segurança de Informação, REP, sincronismo de relógio.

ABSTRACT

The Brazilian Department of Labour and Employment (MTE) created two regulations that aim to regulate the electronic registration of employees working time which with the use of ICT targets to minimize the problems arising from disputes over these records. The Regulation No. 1510 introduced the special equipment Electronic Timekeeping (REP), which is a hardware embedding fiscal intelligence. However, the Regulation No. 373 allowed the use of alternative systems for working time, which could be software-based. However, alternative REP systems must meet a series of requirements to legal compliance. The companies using these systems should incorporate mechanisms of systems auditing to verify compliance with these regulations. This paper presents a methodology for compliance assurance that highlights the design patterns and vulnerabilities founded in case studies. Among the main findings are best practices and technological mechanisms that minimize the risks of non-compliance with Brazilian regulations.

Keywords: MTE; Systems Auditing; Information Security; Human Resources; REP; Timekeeping Systems.

RESUMEN

El Ministerio de Trabajo y Empleo ha redactado dos reglamentos para la regulación del registro electrónico del tiempo de trabajo con el fin de minimizar los problemas derivados del control de la jornada de trabajo. El Reglamento 1.510 estableció el equipo de Registro Electrónico de Punto (REP), que es un hardware integrado de inteligencia fiscal. Sin embargo, el Reglamento 373 permitió el uso de Sistemas Alternativos de Control de la Jornada de Trabajo, que podrían ser basados en software. No obstante, este software debe cumplir una serie de exigencias para presentar el cumplimiento legal. Por lo tanto, las empresas deben incorporar estos factores a su gestión de riesgos, imponiendo mecanismos de auditoría que requieren sistemas para evaluar estos nuevos factores. Este trabajo presenta una metodología de verificación, destacando el diagnóstico convencional y vulnerabilidades encontradas en estudios de caso. Entre los aportes de este trabajo está la presentación de buenas prácticas y mecanismos tecnológicos que reduzcan al mínimo los riesgos de incumplimiento de la normativa brasileña.

Palabras clave: Auditoría de Sistemas; Control de Punto; Seguridad de la Información; REP; sincronización de reloj.

1 INTRODUÇÃO

O desenvolvimento do governo eletrônico vem se intensificando e acompanhando as tendências das Tecnologias da Informação e Comunicação (TIC) que agregam valor e melhoram a eficiência do poder público. Nesse sentido, um dos focos de uso dessas tecnologias é a melhoria da fiscalização da aplicação das leis e regulamentos que regem as relações de trabalho entre empresas e seus empregados.

O Ministério do Trabalho e Emprego (MTE) identificou que a automação dos processos de registro eletrônico de ponto poderia melhorar o controle e a segurança sobre o registro de horas trabalhadas, minimizando as divergências e processos trabalhistas envolvendo remuneração dessas horas. Segundo o Ministério do Trabalho e Emprego (MTE), a quantidade de processos trabalhistas, por ano, atinge por volta de 2 Milhões (90% se referem a Horas Extras não pagas), sendo esta a principal causa das disputas registradas nas varas trabalhistas. Ao deixar de registrar o trabalho adicional de seus empregados, e com base no Relatório Anual de Informações Sociais (RAIS), os cálculos revelam que a sonegação à Previdência Social pode chegar a R\$ 4,1 bilhões, e mais R\$ 1,6 bilhão ao Fundo de Garantia do Tempo de Serviço (FGTS)(MTE, 2010).

A ideia de um relógio eletrônico de ponto já existia. No entanto, os relógios de ponto eletrônico automatizavam os processos corporativos, mas não tinham uma inteligência fiscal embarcada e, ao automatizar processos corporativos, nem sempre estavam em acordo com todas as regulamentações trabalhistas.

Internacionalmente, existem relatos de decisões determinando o pagamento de horas extras quando os apontamentos não são bem documentados ou registrados pelos empregadores. O Congresso dos Estados Unidos aprovou a *Fair Labor Standards Act (FLSA)*, em 1938, que determina, na Seção 11 (c), que os empregadores são obrigados a manter registros precisos sobre a jornada de trabalho dos empregados. A Seção 16 (b) da Lei permite que os funcionários reivindiquem horas extras efetivamente comprovadamente trabalhadas quando o empregador não apresenta seus registros de jornada (UNITED STATES SUPREME COURT, 1946; GROSSMAN, 1978).

O MTE, em 21 de agosto de 2009, resolveu disciplinar o registro eletrônico de ponto e a utilização do Sistema de Registro Eletrônico de Ponto, por meio da Portaria 1.510(BRASIL, 2009). O elemento central desta Portaria é um equipamento chamado de Registrador Eletrônico de Ponto (REP), que concentra a inteligência fiscal para disciplinar o registro. O REP é assim definido, segundo o Artigo 3º da Portaria 1.510 do MTE:

Equipamento de automação utilizado exclusivamente para o registro de jornada de trabalho e com capacidade para emitir documentos fiscais e realizar controles de natureza fiscal, referentes à entrada e à saída de empregados nos locais de trabalho.

A Portaria MTE 1.510/2009 definiu que Sistema de Registro Eletrônico de Ponto - SREP - é o conjunto de equipamentos e programas informatizados e destinados à anotação por meio eletrônico da entrada e saída dos trabalhadores das empresas, e este deve utilizar o REP no local da prestação do serviço, de forma obrigatória, vedados outros meios de registro. O elemento principal é o REP, sendo de forma resumida, caracterizada pelos seus principais requisitos:

- Ter como finalidade exclusiva a marcação de ponto;
- Possuir memória das marcações de ponto que não possa ser alterada ou apagada;

- Emitir comprovante a cada marcação efetuada pelo trabalhador;
- Não possuir mecanismo que permita marcações automáticas ou restrições às marcações;
- Manter o relógio atualizado por no mínimo 1.440 horas (em caso de falta de energia) e não atrasar por mais de 1 minuto ao ano.

Os requisitos importantes para o empregador, segundo o MTE, são a utilização do REP; a geração dos dados originais na forma do Arquivo-Fonte de Dados (AFD) salvo em Pen-drive; a emissão da Relação Instantânea de Marcações com as marcações efetuadas nas 24h (vinte e quatro horas) precedentes, dentre outros.

Este equipamento atende a maioria das empresas que realizam a gestão eletrônica de jornada de trabalho, sendo obrigatório o uso do REP nestas situações. A Portaria nº 388, de 25 de agosto de 2014 delegou ao INMETRO as atividades de planejar, desenvolver e implementar o Programa de Avaliação da Conformidade dos Registradores de Ponto Eletrônico - REP, no âmbito do Sistema Brasileiro de Normalização, Metrologia e Qualidade Industrial –Sinmetro. Este criou o regulamento técnico de qualidade pela Portaria n.º 595, de 05 de dezembro de 2013, o qual deve ser usado pelos fabricantes na elaboração de seus produtos, para posterior venda aos empregadores.

Algumas empresas possuem a gestão de jornada de trabalho embarcada em sistemas computacionais complexos, que incorporam aplicações corporativas voltadas às questões de negócio da empresa. A incorporação de um mecanismo como o REP poderia ser um retrocesso tecnológico e geraria uma dificuldade operacional que poderia comprometer a gestão do negócio. Uma alternativa foi a iniciativa do Governo em instituir a Portaria nº 373, de 25 de fevereiro de 2011, que dispõe sobre a possibilidade de adoção, pelos empregadores, de sistemas alternativos de controle de jornada de trabalho (BRASIL, 2011), desde que:

- Sejam autorizados por Convenção ou Acordo Coletivo de Trabalho;
- Haja o cumprimento integral, pelo empregado, da jornada de trabalho contratual, convencionada ou acordada, vigente no estabelecimento;
- Seja disponibilizado ao empregado, até o momento do pagamento da remuneração referente ao período em que está sendo aferida a frequência, qualquer ocorrência que ocasione alteração de sua remuneração em virtude da adoção de sistema alternativo.

Os sistemas alternativos eletrônicos de marcação de pontos não devem admitir restrições à marcação do ponto; marcação automática do ponto; exigência de autorização prévia para marcação de sobre jornada e alteração ou eliminação dos dados registrados pelo empregado. Além disso, a fiscalização deve ter acesso aos sistemas alternativos eletrônicos no local de trabalho, sendo possível identificar o empregador e empregado nesse sistema; e possibilitar através da central de dados, a extração eletrônica e impressa do registro fiel das marcações realizadas pelo empregado.

Essas duas Portarias geraram alguns impasses no mercado, pois incorporaram algumas vulnerabilidades em um processo já estabelecido, que instituía o controle por *hardware* com inteligência fiscal embarcada, que tem um processo rigoroso de homologação por empresas credenciadas pelo MTE. O processo como um todo poderia ser substituído por soluções baseadas em *software*, que podem ser desenvolvidas por terceiros ou até pelos empregadores. Assim, como poderia ser possível garantir todas as premissas do processo anterior, que ainda é válido, sem um controle equivalente?

Nesse contexto, existe a possibilidade de perdas decorrentes de multas, penalidades ou indenizações resultantes de ações de órgãos de supervisão e controle, bem como perdas decorrentes de decisão desfavorável em processos judiciais ou administrativos (COSO, 2007). As empresas devem se prevenir e incluir este novo rol de regulamentações em sua Gestão de Riscos. Este artigo vem esclarecer quais são os principais pontos ao observarmos sistemas alternativos de controle de jornada, apresentar boas práticas a serem seguidas, apontar as vulnerabilidades desse modelo, e propor recomendações necessárias para que sistemas alternativos consigam minimizar riscos de não conformidade com as regulamentações nacionais.

2 METODOLOGIA DE AVALIAÇÃO

A auditoria de sistemas auxilia na segurança dos sistemas de informação, identificando possíveis problemas e estabelece medidas preventivas para maior segurança desses sistemas. Sua realização é imprescindível nas organizações e concluiu-se que através dela tem-se uma visão abrangente em relação ao sistema de informação, podendo assim apontar suas falhas, seus erros, mau uso e fraudes por parte de usuários e fontes diversas (GARCIA et al., 2013).

A Metodologia de avaliação de sistemas alternativos de controle de jornada deve ser pautada para a resolução das principais vulnerabilidades de sistemas de *software*. Nesse sentido, três abordagens devem ser exploradas: avaliação das vulnerabilidades funcionais, de gestão, e sincronismo automático de hora.

As vulnerabilidades funcionais de *software* podem ser avaliadas por técnicas de testes abordadas pela Engenharia de *Software*, enquanto as vulnerabilidades de processo e gestão são verificadas por procedimentos de Segurança da Informação. Por fim, as vulnerabilidades no sincronismo de hora são avaliadas pelos mecanismos tecnológicos de controle incorporados aos sistemas.

2.1 VERIFICAÇÕES FUNCIONAIS DE *SOFTWARE*

De acordo com as metodologias de teste de *software* abordadas pela Engenharia de *Software*, estas são classificadas em dois grupos: teste de caixa branca e teste de caixa preta. (PRESSMAN, 2011).

O teste de caixa branca, chamado de teste estrutural, utiliza o código fonte para avaliar as questões funcionais do *software*. O teste de caixa preta, chamado de teste funcional, enfoca o domínio da informação dos *softwares*, originando casos de teste utilizando os dados de entrada e o resultado esperado (dados de saída). Como o Sistema de Ponto Eletrônico é regido por funcionalidades que devem atender a legislação, e não necessariamente ligadas à estrutura do Sistema, os testes de caixa preta são suficientes para análise e mitigação dos riscos.

Os testes de caixa preta podem ser de dois tipos: estáticos ou dinâmicos. O estático é feito a partir de documentação e modelos; o dinâmico é feito em algo que possa ser executado nos sistemas prontos. Os planos de testes são elaborados e aplicados no sistema que está em funcionamento, por isso a técnica utilizada foi a de testes dinâmicos.

Utilizando testes de caixa preta dinâmicos é impossível abranger todas as possibilidades de execução e afirmar com certeza que os testes garantem o funcionamento esperado do *software* (SOMMERVILLE, 2011). Entretanto, se o teste for corretamente realizado, poderá fornecer bons indícios sobre a conformidade e qualidade dos sistemas.

Os planos de teste são elaborados com base na Norma IEEE 829 *Standard for Software Testing Documentation* (IEEE COMPUTER SOCIETY, 1998) e o seu conteúdo segue a seguinte estrutura:

- Identificação do teste – breve definição do teste;
- Descrição do teste – passo-a-passo de como realizar o teste;
- Dados de Entrada – informações que o testador deverá fornecer ao sistema;
- Resultado Esperado – o comportamento que o sistema deve apresentar;
- Registro do caso de teste – tipo de teste, neste caso Teste de Caixa Preta;
- Levantado por – responsáveis por realizar os testes;
- Data – data da execução do teste;
- Descrição do resultado obtido – descrição do comportamento apresentado pelo sistema e verificação se o resultado esperado foi alcançado.

O plano de teste deve ser executado e os resultados anotados para futuro confronto do resultado verificado com o resultado esperado. A análise dessa comparação irá definir o nível de risco ou não conformidade do Sistema Alternativo frente às vulnerabilidades funcionais de *software*.

2.2 VERIFICAÇÕES DA SEGURANÇA DA INFORMAÇÃO

As verificações de processo e gestão envolvem a forma como são tratados os sistemas computacionais, como é a gestão de recursos humanos que tem acesso à infraestrutura de TI, e quais são os mecanismos tecnológicos de proteção dos dados.

Os recursos de segurança previstos na Portaria 1.510 são implementados no *hardware* do REP. Como os recursos de segurança dos Sistemas Alternativos são implementados via *software*, devem ser utilizadas as normas internacionais do grupo ISO 27000, que estabelecem critérios de verificação dos mecanismos de segurança instituídos (ABNT, 2006).

A ABNT traduziu a norma ISO/IEC 27001:2006 sem modificações, intitulado-a como ABNT NBR ISO/IEC 27001:2006. Em sua introdução geral menciona que foi preparada para prover um modelo com objetivo de estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A sua especificação e implementação são influenciadas pelas necessidades e objetivos, requisitos de segurança, processos empregados, tamanho e estrutura da organização. É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização; por exemplo, uma situação simples requer uma solução de SGSI simples.

A ABNT NBR ISO/IEC 27001 exige que a organização “realize análises críticas regulares da eficácia do SGSI levando em consideração os resultados da eficácia das medições” e que “meça a eficácia dos controles para verificar se os requisitos de segurança da informação foram alcançados”. Esta também exige que a organização “defina como medir a eficácia dos controles ou grupo de controles selecionados e especifique como essas medidas devem ser usadas para avaliar a eficácia dos controles para produzir resultados comparáveis e reproduzíveis”.

A ABNT NBR ISO/IEC 27001 adota o ciclo denominado PDCA (*Plan, Do, Check, Act*) para estruturar todos os processos envolvidos em um SGSI. O PDCA é uma ferramenta gerencial que possibilita a melhoria contínua de processos e a solução de problemas (Figura 1).

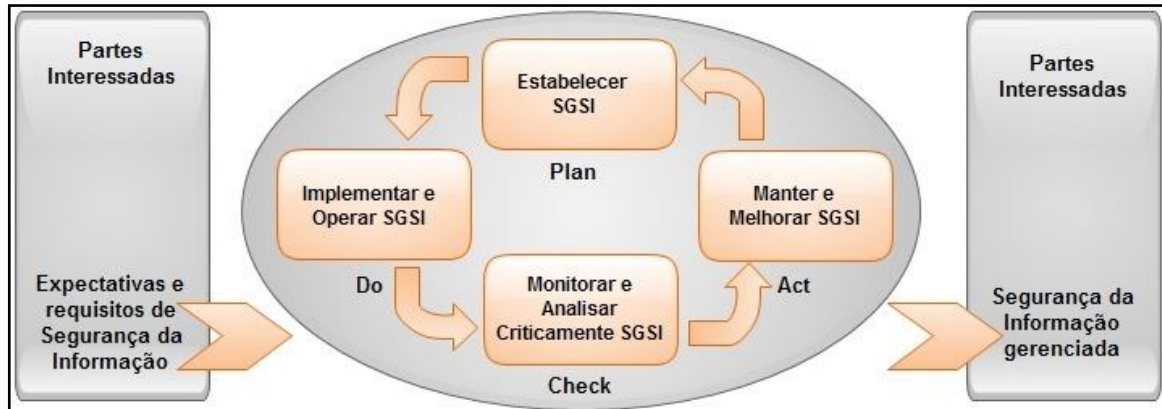


Figura 1: Modelo PDCA aplicado aos processos do SGSI.

Fonte: ABNT (2006).

As verificações para avaliar o Sistema Alternativo devem incluir os procedimentos e políticas de segurança, controles e gerenciamento de riscos baseados na norma ISO 27001, que cubram pelo menos:

- Política da Segurança da Informação;
- Infraestrutura da Segurança da Informação;
- Responsabilidade pelos ativos;
- Áreas seguras (Segurança Física);
- Procedimentos e responsabilidades operacionais (Gerenciamento);
- Cópias de segurança;
- Monitoramento;
- Requisitos de negócio para controle de acesso;
- Gerenciamento de acesso do usuário;
- Controles de acesso à rede;
- Aspectos da gestão da continuidade de negócio, relativos à segurança da informação;
- Conformidade com normas e políticas de segurança da informação e conformidade técnica;
- Considerações quanto à auditoria de sistemas da informação;
- Requisitos para aquisição de tempo (sincronismo de relógio).

Sendo assim, cada item de verificação da lista apresentada da ISO 27001 é aplicado no sistema alternativo e registrado para ser confrontado com o que é regido pela norma. Uma análise posterior determina quais são os pontos de melhoria para a conformidade com as regulamentações.

2.3 VERIFICAÇÕES DO CONTROLE DE HORA

O registro da hora de jornada é uma informação sensível, que ao ser manipulada indevidamente poderá ocasionar uma não conformidade ou prejuízo ao Sistema Alternativo. Assim, uma análise para identificar quais são os recursos tecnológicos empregados no controle de hora é determinante para o nível de confiança destes recursos.

Os mecanismos podem variar em complexidade e efetividade. A maneira mais simples é a configuração de hora manual, a qual promove um alto nível de incerteza. Seja pela imprecisão do lançamento manual ou pela falta de *logs* de alteração de hora, que não são comuns neste modelo. A maneira mais complexa envolve o sincronismo de horário dos equipamentos envolvidos com fontes confiáveis ou um carimbador de tempo (ON, 2007).

A arquitetura para sincronismo de tempo pode ser dividida em diversos níveis, conforme Figura 2. No nível 1, a configuração de tempo é efetuada manualmente em todos os

servidores e equipamentos, o operador do sistema necessita acessar todos os equipamentos e efetuar o ajuste do relógio. No nível 2, os equipamentos possuem o serviço de sincronismo do relógio configurado para obter a hora de um servidor interno de tempo, no entanto, este servidor ainda é configurado manualmente pelo operador do sistema. No nível 3, o servidor interno de tempo é configurado para obter automaticamente a hora de uma fonte externa confiável. E por fim, no nível 4, o servidor interno de tempo é configurado para obter a hora de um carimbador de tempo homologado conforme a Hora Legal Brasileira, que pode estar localizado na empresa ou ser acessado pela internet.

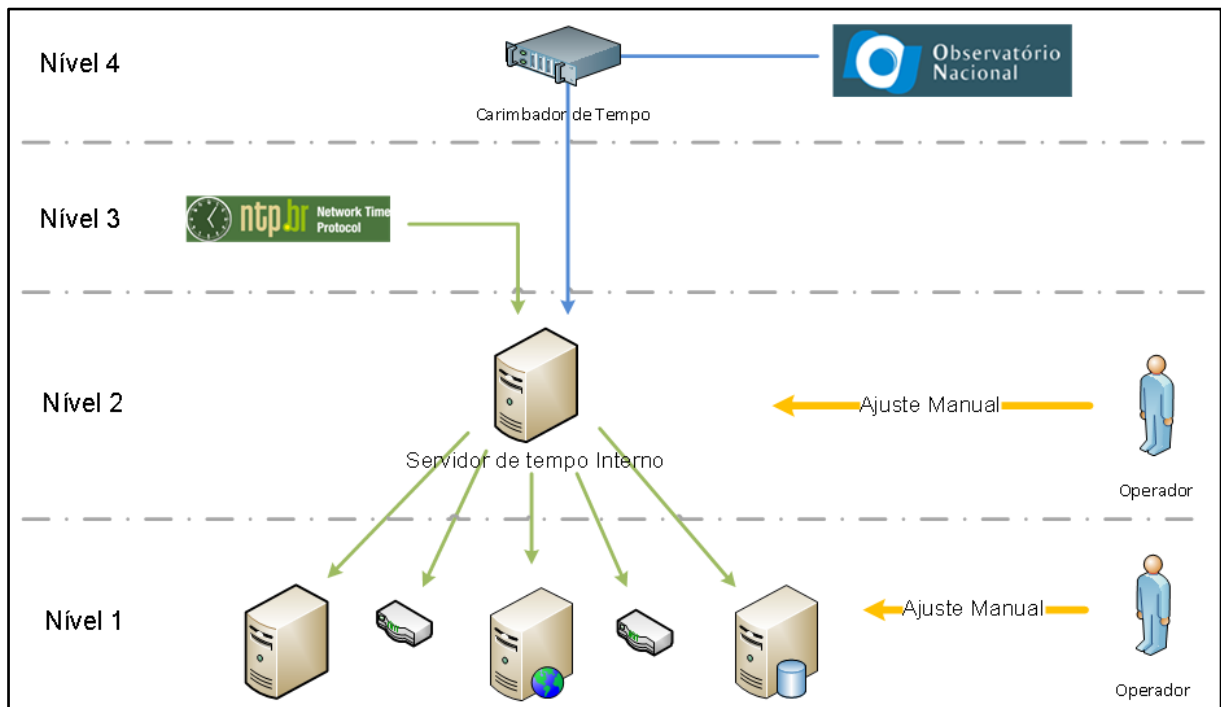


Figura 2: Níveis de arquitetura para sincronismo de tempo.

Fonte: Elaboração própria.

2.4 VALIDAÇÃO E EXPERIMENTAÇÃO METODOLÓGICA POR ANÁLISE DE ESTUDOS DE CASOS

Para esclarecer quais os principais pontos a serem observados nos sistemas alternativos de controle de jornada, a metodologia proposta foi aplicada em diversos casos. Observou-se que a validação e experimentação poderiam ser analisadas por setores ou ramos de atividades, pois as características operacionais, o perfil de gestão de RH, arquitetura computacional tinham semelhanças fundamentais. Como os sistemas alternativos de ponto são executados por mecanismos computacionais, a arquitetura do sistema é o principal elemento a ser investigado para o levantamento de vulnerabilidades e elaboração de diagnósticos, assim como para proposição de boas práticas e mitigação de riscos.

A metodologia proposta foi testada em seis grandes companhias e foram agrupadas em três perfis de casos, que representam três ramos de atividades:

- Bancário;
- *Call Center*;
- Prestação de serviços.

De forma resumida, cada empresa possui uma entrada de marcação distinta. Na empresa do setor bancário, o funcionário registra o ponto em uma estação de trabalho; na do

setor de *Call Center*, o funcionário registra o ponto ao se *logar* no sistema de atendimento pelo aparelho telefônico; e na empresa prestadora de serviços, o funcionário registra o ponto em um dispositivo móvel, pois geralmente suas atividades são realizadas fora das dependências da empresa.

Devido às necessidades e diferenças presentes nos ramos de atividade, cada um dos sistemas alternativos avaliados apresenta um fluxo particular. Além disso, diferentes recursos técnicos e mecanismos foram empregados para a adequação do sistema aos requisitos do REP. Os itens, a seguir, descrevem a arquitetura do sistema alternativo para controle de jornada de trabalho em cada um dos estudos de caso.

2.4.1 Estudo de caso A – Empresa do Setor bancário

O registro é efetuado em um terminal de caixa ou em uma estação de trabalho. Dentro de um intervalo de tempo definido, o sistema envia as informações armazenadas para a base de dados do Mainframe (DB2). O Mainframe envia estas informações, em arquivo sequencial, para uma base de dados de baixa plataforma e os dados são disponibilizados no portal WEB. A Figura 3 apresenta a arquitetura do sistema.

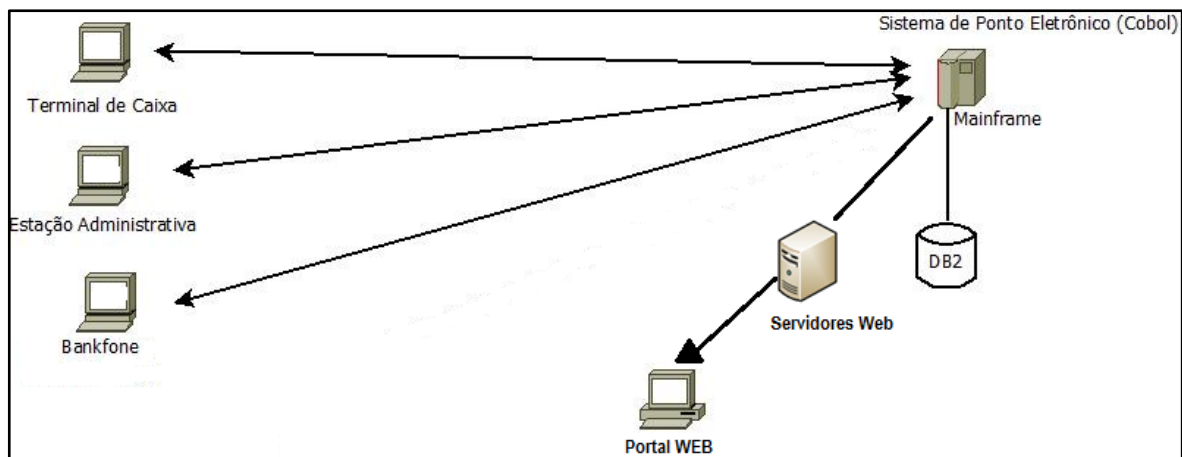


Figura 3: Processo de Marcação de Ponto no Setor bancário.
Fonte: Elaboração própria.

2.4.2 Estudo de caso B – Empresa de Setor de *Call Center*

A infraestrutura da empresa do Setor de *Call Center* baseia-se nos componentes apresentados na Figura 4. Os dados registrados no aparelho telefônico são armazenados no sistema gerenciador de chamadas (*Call Management System - CMS*), que possui uma base própria e que também é utilizado para registrar *logouts* e pausas no atendimento. Os registros de cada gerenciador são transferidos para uma base de dados. Após a transferência, as informações são encaminhadas ao ambiente secundário, composto pelo sistema para controle de jornada.

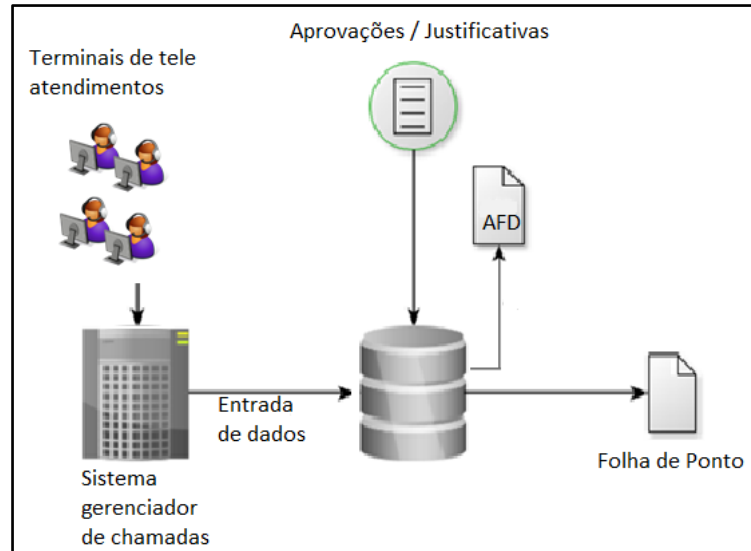


Figura 4: Arquitetura do Sistema de Call Center.
Fonte: Elaboração própria.

2.4.3 Estudo de caso C – Empresa do setor de prestação de serviços

Por se tratar de uma empresa que atende seus clientes *on-site*, os funcionários da manutenção utilizam um dispositivo móvel para realizar o registro do ponto sem a necessidade de se deslocar até a empresa. Este dispositivo possui uma base local para armazenar os dados de registro de ponto. Conforme a disponibilidade da conexão de dados, as informações de marcação são transferidas para uma base de dados central, que fica relacionada a um sistema de *Customer Relationship Management* (CRM). Ao mesmo tempo, as informações de marcação são enviadas para o funcionário por um e-mail gerado automaticamente pelo sistema. A Figura 5 apresenta o esquema da arquitetura deste sistema de controle de jornada.

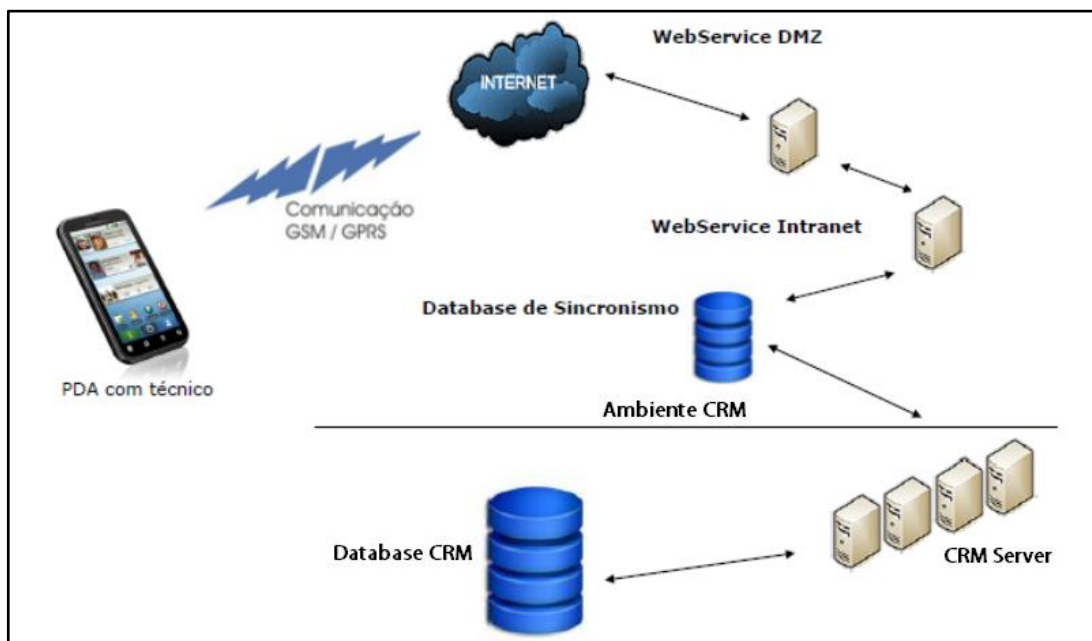


Figura 5: Arquitetura de Marcação Móvel de Ponto.
Fonte: Elaboração própria.

3 VULNERABILIDADESE DIAGNÓSTICOS

Os sistemas alternativos de controle de jornada de trabalho estão pautados no atendimento dos requisitos elencados na Portaria 373, assim como da Portaria 1.510, que tem um relacionamento direto com os requisitos da Portaria 373. Nesta seção, são apresentadas as vulnerabilidades essenciais de não conformidades com as referidas Portarias, além do diagnóstico, encontradas em cada um dos estudos de casos.

3.1 ARQUITETURA CONCEITUAL PADRÃO

Ao analisar os estudos de caso foi possível observar que sistemas alternativos de controle de jornada apresentam uma arquitetura padrão em várias camadas que, em engenharia de *software*, é definida como sistemas de N camadas (FOWLER, 2003). A Figura 6 sintetiza a ideia geral da arquitetura padrão de sistemas alternativos.

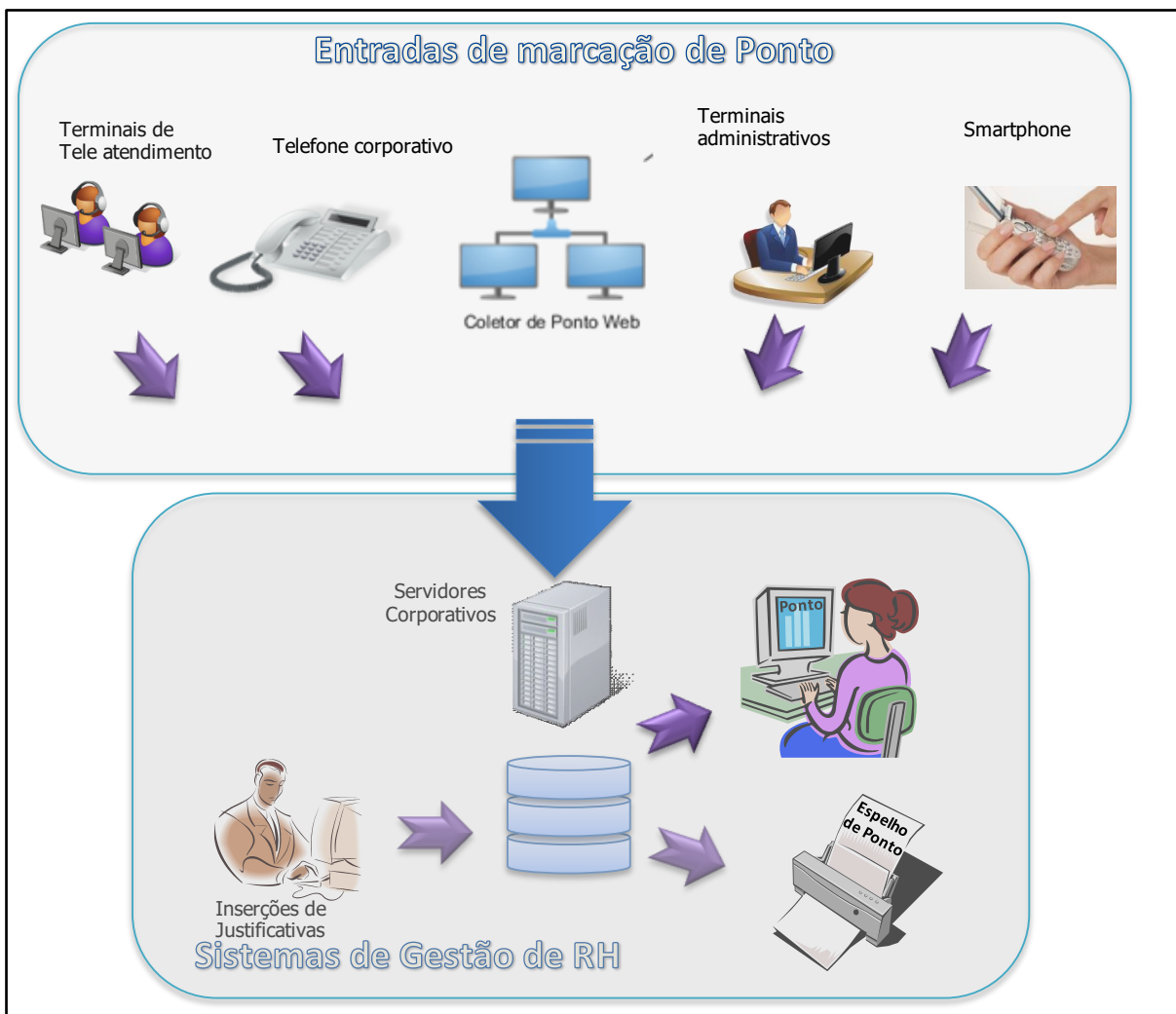


Figura 6: Modelo arquitetural padrão para Sistemas alternativos de controle de jornada.

Fonte: Elaboração própria.

Uma vez que o sistema estudado possa ser enquadrado na arquitetura conceitual padrão apresentado na figura 6, é possível identificar pontos estratégicos de verificação na busca de vulnerabilidades e evidências de não conformidade. Desta forma, nas próximas seções são apresentados estes pontos.

3.2 VULNERABILIDADES DE SISTEMAS ALTERNATIVOS

As vulnerabilidades decorrem da falta de mecanismos de controle sobre os requisitos das Portarias, ou de fragilidades na gestão de pessoas, infraestrutura e processos. Desta forma, as vulnerabilidades estão apresentadas em dois grupos fundamentais: vulnerabilidades funcionais e de gestão.

As vulnerabilidades funcionais são vulnerabilidades de *software* e estão relacionadas, principalmente, ao não atendimento dos requisitos elencados na Portaria 1.510 e Portaria 373, podendo ocorrer na implementação ou na utilização do sistema alternativo. A **Erro! Fonte de referência não encontrada.** apresenta os pontos vulneráveis de *software*.

Tabela 1 – Vulnerabilidade funcionais de sistemas alternativos

1.	Ausência de exclusividade para marcação de ponto
2.	Possibilidade de manipulação das marcações
3.	Falta de emissão de comprovante de marcação
4.	Existência de mecanismo de marcação automática
5.	Baixo controle da Hora de marcação
6.	Constantes mudanças no código fonte

Fonte: Elaboração própria.

As vulnerabilidades de gestão ocorrem nos processos e nos ambientes de tecnologia da informação, no qual o sistema de controle de jornada está inserido. Neste sentido, é importante analisar os pontos de verificação que envolvem três grupos de controle: Pessoas, Infraestrutura e Procedimentos operacionais. O Quadro resume os principais pontos vulneráveis a respeito da gestão operacional.

Quadro 1 – Vulnerabilidade de gestão e processos de sistemas alternativos

Vulnerabilidades de gestão e processos	Pessoas	Infraestrutura	Procedimentos
Falta de controle sobre o versionamento e as alterações no código fonte; dificuldade de analisar as implicações de mudanças de equipamentos e novas versões do <i>software</i> . Não há aprovações ou controle de mudança de código que envolve regras sensíveis à conformidade.	X		x
Interrupção da marcação de ponto, perda de dados de marcação de pontos, assim como falhas no armazenamento de informações trabalhistas no período mínimo de 5 anos.		x	x
Dificuldade no rastreamento de falhas operacionais e de segurança	X	x	
Facilidade de manipulação de dados sensíveis por pessoas não autorizadas	X		x
Não há auditoria regular em componentes críticos dos sistemas alternativos	X	x	x

Fonte: Elaboração própria.

3.3 DIAGNÓSTICOS

As análises dos estudos de casos, a partir da aplicação dos planos de teste, constataram que todos os casos apresentam vulnerabilidades de *software*, assim como, após a verificação dos mecanismos e gestão de segurança da informação, também se observaram vulnerabilidades de gestão e processos.

3.3.1 *Software*

Em dois dos sistemas avaliados, a saber, estudos de caso B e C, não há a exclusividade para marcação de ponto: é o caso do dispositivo móvel e do sistema gerenciador de chamadas.

O dispositivo móvel é utilizado para realizar chamadas telefônicas, receber mensagens, acessar Internet, cronometrar a distância e o tempo da chamada até a execução do serviço. O sistema gerenciador de chamadas é usado para atender reclamações dos usuários, transferir chamadas, realizar as pausas, colocar as ligações em espera, gerenciar as filas de atendimento, entre outros.

Foi constatado, também, que não é possível garantir que não haveria manipulação das marcações de ponto. Os registros das marcações de ponto são sempre armazenados em sistemas gerenciadores de banco de dados. Mesmo com políticas de segurança aplicadas no momento, não estaria descartada a possibilidade do responsável ou administrador dos bancos de dados alterarem ou apagarem um registro.

A vulnerabilidade da falta de emissão do comprovante de marcação está presente em todos os sistemas avaliados. Já a existência de mecanismo de marcação automática não foi encontrada em nenhum dos sistemas.

As principais vulnerabilidades encontradas na aquisição de tempo para controle de hora ocorrem por não existir um único ponto confiável para sincronismo de relógio e por ocorrer o ajuste manual do relógio dos servidores e equipamentos.

No estudo de caso havia a falsa impressão de sincronismo de relógio. Um único servidor foi eleito como fonte confiável de tempo, então todos os servidores da instituição foram configurados para obter a hora desse servidor. No entanto, o servidor de sincronismo em questão não possuía a configuração para obter a hora de uma fonte confiável, sendo sua configuração efetuada de forma totalmente manual. Assim, o erro de tempo associado à sincronização manual era propagado para todos servidores da organização.

3.3.2 Gestão e Processos

A gestão de mudança tem o objetivo de agregar confiabilidade a todo processo de Tecnologia da Informação implantado na instituição. Para controle e documentação das mudanças há necessidade de normas e procedimentos que contemplem as áreas de Tecnologia da Informação e demais áreas envolvidas com o Sistema Alternativo de Controle de Jornada. As normas e os procedimentos são documentados e adotados na aquisição, desenvolvimento e transferência de equipamentos e *softwares* do ambiente de desenvolvimento e homologação para o ambiente de produção. Essas práticas devem ser adotadas para garantir o versionamento correto dos códigos fontes dos aplicativos e sistemas e assim melhorar a qualidade dos ambientes de desenvolvimento, homologação e dos sistemas implantados.

Nas análises realizadas no estudo de caso C foram encontrados processos onde o controle de mudanças não é devidamente documentado. As alterações e mudanças de sistemas são efetuadas mediante o registro de um número de controle, no entanto não existe um grupo responsável por avaliar e aprovar as alterações. As áreas envolvidas não são obrigadas a apresentar documentos com todo o detalhe e impactos das alterações a serem efetuadas. Além disso, não são documentadas as medidas de contorno e retorno para o caso de falhas no procedimento de mudança.

A gestão de continuidade do negócio tem como objetivo não permitir que as suas atividades sejam interrompidas e proteger os processos mais críticos ao negócio contra falhas significativas, restabelecendo sua operação no menor tempo possível. O processo de continuidade do negócio possui os riscos mapeados e contempla os requisitos de segurança de tecnologias da informação.

Assim, o Plano de Continuidade do Negócio foi outro processo importante que apresentou vulnerabilidades nos casos estudados. Durante as análises foram encontrados

planos de continuidade do negócio com um grande nível de abordagem dos processos, assim como planos de continuidade mais básicos.

O plano de continuidade mais completo, identificado no estudo de caso A, apresenta redundância local, de instalações, processo e armazenamento das informações. Além disso, existe um *site backup* em uma localidade remota com cópia de todos os sistemas presentes no *site* principal. A rotina de *backup* dos sistemas é efetuada regularmente e todas as cópias são armazenadas em um ambiente externo.

O plano mais básico, identificado no estudo de caso B, apresenta redundância para os sistemas mais críticos como autenticação e banco de dados. Também possui *site backup* para recuperação desses sistemas. A rotina de *backup* é efetuada regularmente e as cópias armazenadas no *site backup*.

Além desses, também foi encontrado ambiente onde é mencionada a implantação do plano de continuidade do negócio, caso do estudo de caso C. No entanto, não foram apresentados documentos ou evidências que comprovem a existência e aplicação efetiva do plano.

A monitoração dos sistemas analisados e dos ativos envolvidos é importante para detectar qualquer anomalia ou atividade não autorizada para o processamento das informações. A monitoração concentra-se em verificar eventos de segurança e registros de *logs* de operação e falhas.

Os sistemas analisados e os sistemas auxiliares e demais equipamentos pertencentes à arquitetura do sistema apresentaram um mecanismo de registros de *logs* de auditoria deficitário. As informações esperadas nos *logs* são: identificação do sistema ou equipamento, detalhe do evento, nível de privacidade, identificação do operador, armazenamento e retenção da informação.

Dos três casos analisados, os estudos de caso A e B apresentaram registros de *logs* parciais, ou seja, nem todas as informações esperadas eram registradas; também foram encontradas situações onde somente alguns sistemas registravam *logs*. O estudo de caso C apresentou a situação mais extrema, devido a nenhum tipo de registro de *log* ser efetuado, para nenhum elemento do sistema.

Ainda sobre os *logs* de auditoria, foi identificada ausência de mecanismos de segurança para garantir a integridade desses *logs*.

O controle de acesso aos ambientes controlados é importante para assegurar que somente pessoas autorizadas tenham esse acesso. Nos ambientes analisados o acesso físico aos ambientes operacionais de TI está devidamente regulamentado por normas internas das três organizações. No entanto, no estudo de caso C foi constatado que o controle de acesso ao local restrito estava em manutenção há um longo período de tempo, sendo substituído por um controle manual de acesso.

As principais vulnerabilidades encontradas na aquisição de tempo para controle de hora ocorrem por não existir um único ponto confiável para sincronismo de relógio e por ocorrer o ajuste manual do relógio dos servidores e equipamentos. Além disso, nenhum controle de registro de mudança de horário foi encontrado.

4. BOAS PRÁTICAS E MITIGAÇÃO DE RISCOS

Com base nos estudos de caso e avaliações realizados, e confrontando-se a regulamentação, foi possível identificar boas práticas para mitigar os riscos de não

conformidade. Estas incluem alguns mecanismos tecnológicos, além de políticas de gestão e controle que podem auxiliar a mitigação dos riscos em sistemas alternativos.

4.1 MECANISMOS TECNOLÓGICOS DE PROTEÇÃO

Em relação à base de dados de marcações, uma alternativa possível seria a construção de uma base primária de dados centralizada, onde ficariam os dados “brutos” e inalterados, estando de acordo com a regulamentação de não alteração dos dados da marcação de ponto. Para o atendimento desta exigência seriam necessárias políticas de segurança concisas, instruindo apenas a possibilidade de inserção e leitura dos dados das marcações, e visando atender a todos os requisitos de segurança impostos à MRP (Memória do REP). A partir desta base de dados seria possível a extração dos arquivos fontes de dados e encaminhamento para os sistemas de gestão de RH.

Quanto à emissão do comprovante de marcação de ponto, uma alternativa seria a adoção de comprovante digital via mecanismos *on-line*, legalmente válidos, para a garantia da integridade do registro. Para assegurar validade digital equivalente ao papel impresso, poderia ser usado um Certificado Digital, documento eletrônico que contém dados do funcionário e da empresa com comprovação mútua de autenticidade.

Para garantir a hora correta de efetivação do registro do ponto, uma alternativa confiável e legalmente válida seria a utilização do Carimbo de Tempo, emitido por uma entidade externa credenciada. Esse Carimbo de Tempo garantiria a data e hora da assinatura digital da marcação, em sincronia com a hora legal brasileira. Um sistema alternativo de marcação de ponto poderia enviar um e-mail contendo os dados da marcação, do empregado, do empregador, e da data e hora com o Carimbo de Tempo.

Para o sincronismo de relógio, as instituições devem adotar a estratégia de aquisição de tempo centralizada, ao menos com as configurações sugeridas no nível 3 e, preferencialmente, com as configurações no nível 4, conforme **Erro! Fonte de referência não encontrada.** Um servidor de aplicação pode abrigar o serviço de tempo ou um servidor dedicado pode ser utilizado. Os demais servidores e equipamentos devem ser configurados com o serviço NTP (*Network Time Protocol* – Protocolo para Tempo em Rede), que é um protocolo para sincronização dos relógios dos computadores baseado no protocolo UDP. Este serviço permite a sincronização do relógio de um conjunto de computadores em redes de dados com latência variável sem afetar a precisão do relógio: para este caso, o uso do NTP.br é recomendado. O projeto NTP.br surgiu de um convênio com o Observatório Nacional (ON) e o Comitê Gestor da Internet no Brasil, o qual oferece uma fonte confiável e gratuita para o sincronismo de hora. Para situações onde é necessária a hora certificada, o Observatório Nacional oferece o serviço de hora com carimbador de tempo. Um equipamento homologado pelo ON deve ser utilizado como fonte da hora, ou seja, a aplicação solicitaria ao carimbador o registro de hora.

Em termos arquiteturais deve haver uma separação lógica entre os componentes que recebem a informação primária (Bruta), e a parte que realiza a gestão de RH. A portaria 1.510 define dois componentes que representam esta separação, o REP e o SREP. Sendo assim, é conveniente que o sistema alternativo também tenha dois níveis conceituais, criando uma separação lógica entre as informações primárias, submetidas a um rígido controle técnico que evite a sua alteração, e as cópias desses dados enviados para o sistema de gestão de RH, o qual tem níveis de exigência de conformidade diferentes.

O Auditor Fiscal do MTE necessita ter, durante sua inspeção no local de trabalho, acesso a arquivos e relatórios que ele extrairia do REP. Isto é, o Arquivo-Fonte de Dados – AFD (copiado em Pen-drive) e a emissão da Relação Instantânea de Marcações– RIM, com as

marcações efetuadas nas 24h precedentes. Assim, a fonte desses documentos deve ser a base primária. Adicionalmente, O "Programa de Tratamento de Registro de Ponto" deve gerar o relatório "Espelho de Ponto Eletrônico", o Arquivo Fonte de Dados Tratados - AFDT e o Arquivo de Controle de Jornada para Efeitos Fiscais – ACJEFA(BRASIL, 2009).

A Figura 7 sintetiza alteração da proposta de arquitetura padrão apresentada na Figura 6, para mitigar os riscos e facilitar a comprovação de conformidade.

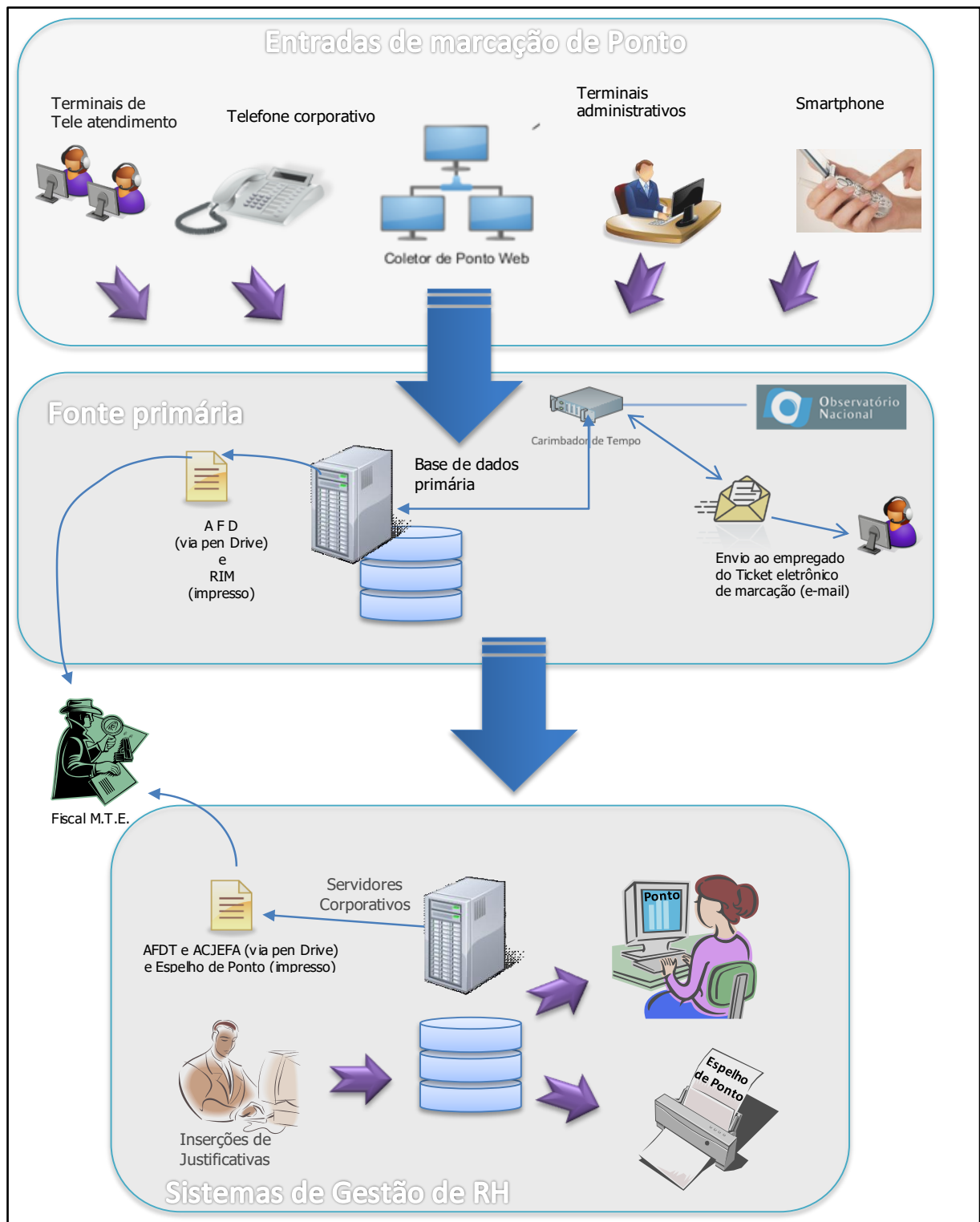


Figura 7: Novo modelo arquitetural padrão para sistemas alternativos.

Fonte: Elaboração própria.

4.2 POLÍTICAS DE GESTÃO E PROCESSOS

Nos casos apresentados foram observadas como boas práticas a implantação de programas de auditoria periódica sobre os processos de recursos humanos e sobre os sistemas de tecnologia da informação que interagem com os sistemas alternativos de controle de jornada.

O planejamento de auditorias deve contemplar auditorias internas, executadas por equipes dedicadas a esta atividade, e auditorias externas, executadas por empresas contratadas e que possuam reconhecimento público sobre os trabalhos de auditoria realizados. As equipes de auditoria interna não devem responder hierarquicamente às equipes de recursos humanos, tecnologia da informação e segurança da informação. Devem estar submetidas a níveis hierárquicos superiores, que garantam a sua imparcialidade quanto aos resultados levantados. É desejável que as auditorias, sejam internas ou externas, ocorram a cada dois anos ou menos, e que o calendário seja divulgado e cumprido. Com isso, espera-se garantir a qualidade na execução dos processos envolvidos.

Quanto à Segurança da informação, as organizações devem instituir o Sistema de Gestão da Segurança da Informação (SGSI). Este sistema de gestão deve contemplar normas gerais de segurança, responsabilidades e os responsáveis por cada controle de segurança da informação. A gestão da segurança da informação deverá estar subordinada ao mais alto nível hierárquico, de forma que suas deliberações tenham efeito e abranjam toda a organização. O SGSI, ao reger as regras de segurança de toda a organização, deverá especificar detalhadamente as responsabilidades de todos os seus colaboradores sobre a segurança da informação. Preferencialmente, o SGSI pode receber certificação por órgão competente, atestando sua legitimidade.

O processo de gestão de ativos deverá ser implantado. Os ativos da informação devem ser identificados de forma individual, inventariados, protegidos de acessos indevidos, ter a documentação atualizada e os planos de manutenção definidos. As informações deverão ser classificadas de acordo com a confidencialidade e com a proteção necessária, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da Instituição. Os acessos devem ser rastreáveis, a fim de garantir que todas as ações sejam passíveis de auditoria, que possam identificar individualmente o Colaborador, para que este seja responsabilizado por suas ações. Os riscos devem ser identificados por meio de um processo estabelecido de análise de vulnerabilidades, ameaças e impactos sobre os ativos de Informação da Instituição, para que sejam recomendadas as proteções adequadas. Os incidentes de Segurança da Informação da Instituição devem ser reportados à Diretoria de Segurança Corporativa.

A Instituição deve promover a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação.

O processo de Gestão de Mudanças deve ser implantado para garantir o controle de todas as alterações realizadas nas redes e sistemas. As alterações incluem a aquisição de novos equipamentos, a devolução e remanejamento de equipamentos, as alterações de ambiente e o controle de *software* e aplicativos, tais como: instalação, configuração,

atualização de versões e correção de problemas. Toda mudança de sistemas, *softwares* e equipamentos seguem critérios, procedimentos e processos rígidos, para substituir versões anteriores de sistemas, ou mesmo, mudança ou incorporação de *softwares* e equipamentos.

5 CONCLUSÃO

A Portaria 1.510 do Ministério do Trabalho e Emprego incorporou novos requisitos de conformidade à legislação trabalhista brasileira, os quais devem ser adotados pelas empresas em sua gestão de risco, sendo a adoção do Registrador Eletrônico de Ponto a principal recomendação de conformidade com a Portaria.

A metodologia apresentada neste trabalho é focada em grandes empresas que possuem o controle de gestão de jornada embarcada em sistemas computacionais que gerenciam principalmente o negócio, possuem um grande número de funcionários e atividades distribuídas em várias unidades. A incorporação de um mecanismo como o REP poderia ser um retrocesso tecnológico e geraria uma dificuldade operacional que poderia comprometer a gestão do negócio. Se, e somente se, for esse o caso é recomendável adotar sistema alternativo de controle de jornada de trabalho, utilizando as premissas da Portaria nº 373, de 25 de fevereiro de 2011. Estas empresas geralmente possuem sistemas complexos, e já adotam políticas e mecanismos tecnológicos que podem ser adaptados para atendimento da Portaria.

Durante a Fiscalização, o Auditor Fiscal é autônomo nas exigências que ele faz para esclarecer as dúvidas levantadas em suas inspeções. Assim, o sistema alternativo deve fornecer condições equivalentes àquelas que ele encontraria com o REP instalado. Além disso, a empresa deve demonstrar presteza em esclarecer as razões da necessidade do sistema alternativo em uso, e todas as providências tomadas em atendimento da essência das Portarias do MTE, que preveem uma maior disciplina e segurança no registro eletrônico de ponto.

Cada setor apresentado nos estudos de caso possui necessidades adicionais que envolvem outros requisitos em sua gestão de risco, sendo que estas corporações possuem equipes de Auditoria Interna e passam por controle de Auditoria Externa, além de equipe de TI de grande porte que é consistente com o perfil das empresas. Sendo assim, a metodologia empregada para identificar as vulnerabilidades e fundamentar os diagnósticos é a base para a apresentação das boas práticas sugeridas por este artigo. Estas envolvem mudanças nos processos, melhoramento de infraestrutura, alteração de arquitetura e código fonte, criação e inclusão de premissas no gerenciamento de Segurança da Informação e verificação do processo por empresa externa que valide as ações realizadas pela empresa.

REFERÊNCIAS

ABNT. **ABNT NBR ISO/IEC 27001:2006 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos**. Rio de Janeiro, p. p 34. 2006.

BRASIL. Ministério do Trabalho e Emprego. **Portaria nº 1.510 de 21 de agosto, 2009**. Disponível em:

<http://portal.mte.gov.br/data/files/8A7C812D32B088C70132D9A53F537D2C/p_20090921_1510.pdf>. Acesso em: Agosto 2012.

BRASIL. Ministério do Trabalho e Emprego. **Portaria nº 373, de 25 de Fevereiro, 2011**. Disponível em:

<http://portal.mte.gov.br/data/files/8A7C816A2E2A24F3012E6DD66E2F0092/p_20110225_373%20doc.pdf>. Acesso em: Agosto 2012.

COSO. **Gerenciamento de Riscos Riscos Corporativos** - Estrutura Integrada. Committee of Sponsoring Organizations of the Treadway Commission. [S.l.], p. 135. 2007.

DINIZ, V. **A história do uso da tecnologia da informação na gestão pública brasileira através do CONIP**— Congresso de Informática Pública. CONGRESO INTERNACIONAL DEL CLAD SOBRE LA REFORMA DEL ESTADO Y DE LA ADMINISTRACIÓN PÚBLICA. Santiago, Chile: [s.n.]. 2005. p. 10.

FOWLER, M. **Patterns of Enterprise Application Architecture**. 6ª. ed. Boston-USA: Addison-Wesley Professional, 2003. ISBN ISBN: 0-321-12742-0.

GARCIA, et al. **Auditoria de sistema: evidenciando os pontos de auditoria de sistemas de escritórios de assessoria contábil**. 10th International Conference on Information Systems and Technology Management – CONTECSI. São Paulo: [s.n.]. 2013. p. 3676-3704.

GODOY, J. E. P.; NÓBREGA, C.. Memória da Receita Federal. **Site Memória - Receita Federal**, 2012. Disponível em:
<<http://www.receita.fazenda.gov.br/Memoria/irpf/default.asp>>. Acesso em: 10 jan. 2014.

GROSSMAN, J. Fair Labor Standards Act of 1938: maximum struggle for a minimum wage. **Monthly labor review / U.S. Department of Labor, Bureau of Labor Statistics**, v. 101, n. 6, p. 22-30, ago. 1978. ISSN 0098-1818 PMID=10307721.

IEEE COMPUTER SOCIETY. **IEEE Std 829: Standard for Software Teste Documentation**. [S.l.]. 1998.

MTE. Notícias: Empresas brasileiras podem estar deixando de pagar R\$ 20,3 bilhões em horas-extras por ano. **Sistema de Registro Eletrônico de Ponto - SREP**, 05 Março 2010. Disponível em: <<http://portal.mte.gov.br/pontoeletronico/05-03-2010-empresas-brasileiras-podem-estar-deixando-de-pagar-r-20-3-bilhoes-em-horas-extras-por-ano.htm>>. Acesso em: 01 jan. 2014.

ON. Divisão Serviço da Hora (DSHO). **Observatório Nacional**, 2007. Disponível em: <<http://pcdsh01.on.br/>>. Acesso em: 10 Janeiro 2014.

PRESSMAN, R. **Engenharia de Software**. 7ª. ed. São Paulo: McGraw-Hil, 2011.

RECEITA FEDERAL. Notícias: Total de declarações do IRPF/2013 fica dentro das previsões da Receita. **Site da Receita Federal**, Março 2013. Disponível em: <<http://www.receita.fazenda.gov.br/noticias/2013/mar/ProgramaIR2013.htm>>. Acesso em: 17 Janeiro 2014.

SEFAZ-SP. Esclarecimento ao contribuinte sobre o Emissor de Cupom Fiscal. **Nota Fiscal Paulista**, 07 nov. 2007. Disponível em: <<http://www.nfp.fazenda.sp.gov.br/pdf/ecf.pdf>>. Acesso em: 10 jan. 2014.

SOMMERVILLE, I. **Engenharia de Software**. 9ª. ed. São Paulo: Pearson Addison-Wesley, 2011.

UNITED STATES SUPREME COURT. **ANDERSON v. MT. CLEMENS POTTERY CO., 328 U.S. 680 (1946)**. United States Supreme Court. [S.l.]. 1946.