UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS

CIÊNCIAS ECONÔMICAS

MBA EM ADMINISTRAÇÃO DA TECNOLOGIA DA INFORMAÇÃO.

FLÁVIO GIUSTI

CONTROLES PARA AUTORIA E IRRETRATABILIDADE NO SISTEMA DE ERP DA EMPRESA VINHOS SALTON S.A.

BENTO GONÇALVES - RS

2010

FLÁVIO GIUSTI

CONTROLES PARA AUTORIA E IRRETRATABILIDADE NO SISTEMA DE ERP DA EMPRESA VINHOS SALTON S.A.

Trabalho de conclusão apresentado à Universidade do Vale do Rio dos Sinos como requisito para conclusão a MBA em Administração da Tecnologia da Informação

Orientador: Prof. MSc. Candido Fonseca da Silva.

BENTO GONÇALVES - RS

2010

RESUMO

Este trabalho trata sobre um aspecto da auditoria de sistema que é a geração de *logs*[1] em sistemas de informação.

Com base na Norma Brasileira NBR ISO/IEC 27.002, que orienta as boas práticas em tecnologia da informação, o trabalho aborda os pontos de controle de *logs* e quais informações devem ser coletadas para ter registros que apontem a autoria e fortaleçam o não repúdio das informações manipuladas no sistema de informação pelos seus usuários.

O trabalho apresenta uma grade de avaliação contendo quesitos abordados na norma e que podem ser aplicados a um sistema de informação, para medir o nível de conformidade do mesmo com a Norma Brasileira NBR ISO/IEC 27.002.

[1] São arquivos gerados automaticamente por aplicações e que registram as suas atividades.

SUMÁRIO

1 INTRODUÇÃO

A política de segurança utilizada nas empresas tem o objetivo de comunicar ao usuário, de forma clara, como os recursos da tecnologia da informação deverão ser utilizados corretamente. Informa, também, como as informações deverão ser manuseadas e que as mesmas pertencem à empresa, devendo ser mantidas de forma adequada a cada momento da realidade da empresa. Essa política imputa responsabilidades, direitos e deveres às pessoas que têm contato com as informações.

Com base na Norma Brasileira ABNT NBR ISO/IEC 27.0002, este trabalho pretende definir os pontos chaves de controle e descrever os registros de *logs*[2] que serão usados em auditorias de sistema, visando atribuir autoria e irretratabilidade no manuseio dos dados do sistema de ERP, criando assim uma grade de quesitos para avaliação dos registros de controle de sistema.

Acredita-se que este trabalho permitirá: (1) Analisar a forma de geração dos registros de auditoria gerados pelo atual sistema de ERP da empresa Vinhos Salton S.A.; (2) Avaliar a conformidade do atual sistema ERP, mediante o registro de auditoria por ele gerado,

[2] São arquivos gerados automaticamente por aplicações e que registram as suas atividades.

confrontando a grade de avaliação dos registros de controle de sistema; (3) Propor melhorias para os registros de auditoria do futuro ERP da Empresa que está em fase de implantação.

1.1 Definição do problema

Quando uma empresa é vítima de fraude, ela está em situação delicada, devendo tomar de imediato as providências corretas; contudo, essa empresa deve ter conhecimento profundo sobre como foi a metodologia da ação da fraude para, assim, poder traçar uma estratégia para não só recuperar os recursos perdidos, mas também para evitar a ocorrência de futuros incidentes similares.

Entre outras providências, saber quem e de que modo agem aqueles que estão lesando a empresa é uma tarefa árdua e demorada, fruto de um trabalho minucioso e que deve ser preciso para evitar injustiças e mais prejuízos.

Atualmente no ERP da empresa Vinhos Salton S.A., para fins auditoria interna do sistema, a geração de informações dos logs somente são coletados um ponto de controle único que registra todas as atividades dos usuários nas ferramentas do ERP.

Segundo as boas práticas da norma ISO/IEC 27.002, os sistemas devem gerar registros que possibilitem auditoria. Mas em que pontos eles podem ser implementados? Qual o objetivo de cada controle? Ele será de utilidade para revelar a autoria dos registros?

Mais especificamente, em caso da empresa ser vítima de fraude envolvendo recursos da empresa, é possível revelar os autores dos registros fraudulentos, eventualmente

registrados no ERP, após a auditoria do sistema? Quais os procedimentos que podem ser implementados para garantir a autoria e irretratabilidade por parte dos usuários envolvidos?

Atualmente, mesmo existindo na empresa procedimentos e controles de segurança para suporte a auditoria de sistema, tem-se a convicção de que tais procedimentos e controles podem ser aprimorados, permitindo respostas aos questionamentos do parágrafo anterior.

1.2.1 Objetivo Geral

Propor, à luz da Norma ISO/IEC 27.002, controles sobre a utilização de ERP, mediante o registro das operações (registros de *logs)* que garantam a autoria dos dados manipulados de forma irretratável.

Descrever em que ponto do ERP os controles devem gerar dados para que uma auditoria de Sistema ou uma perícia forense tenham registros suficientes para determinar os autores e esclarecer como e onde foram efetuadas as operações que lesaram a empresa.

1.2.2 Objetivos Específicos

Efetuar análise da norma ISO/IEC 27.002 e levantar quais os controles devem ser implementados no ERP, para que uma auditoria de sistema (ou perícia forense) tenha as informações necessárias para atribuir a autoria de operações realizadas no ERP.

Elaborar uma grade de requisitos de controles, para servir como base para avaliar os registros de *log* gerado por um sistema de ERP, para garantir a autoria e irretratabilidade dos registros.

Avaliar os controles de *logs* do atual ERP da vinícola Salton S.A., utilizando a grade de requisitos de controles.

Propor um cronograma de implementação no ERP que será implantado com o objetivo de assegurar a autoria e irretratabilidade nos dados do ERP da vinícola Salton S.A., tornando os controles uma fonte de informação para a auditoria de sistema ou subsidiar processos judiciais que venham a ser instaurados.

1.3 Justificativa

A auditoria em sistemas de informação tem como objeto de análise o sistema e os documentos nele registrados, mas as análises do Sistema podem ser feitas de forma mais completa se houver um efetivo registro de eventos relevantes.

Segundo a norma ISO/IEC 27.002, o próprio sistema deve gerar registros para futura auditoria. O procedimento de manter os registros para auditoria em determinados pontos chaves do Sistema de ERP é decisivo para a identificação dos autores de eventuais fraudes naqueles sistemas.

Definir os pontos de controle e como os registros devem ser feitos pode variar de empresa ou sistema. Porém, em qualquer caso, devem ser registradas, em uma linha de tempo, as atividades dos usuários do sistema, de forma a subsidiar futuras auditorias de sistema. Sem estes registros, a auditoria fica restrita à situação atual do sistema e documentos nele registrados. Com os registros históricos é possível determinar qual usuário, como e aonde ocorreram os fatos que são relevantes na auditoria.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Fraude

Art. 1º Código Penal Brasileiro - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal. (Redação dada pela Lei nº 7.209, de 11.7.1984)

Os crimes no Brasil estão definidos pelo Código Penal brasileiro, Decreto-Lei numero 2.848 de 7 de Dezembro de 1940. Apesar da lei ser do século passado, ela vem sendo atualizada, por exigência da evolução social e suas relações. Os representantes do poder legislativo votam projetos de leis que o renovam, para atender a todos os interesses da sociedade.

Os advogados e juízes enquadram os crimes no código penal pelos resultados do ato cometido, mesmo que ele ao ser executado, tenha feito uso de meio eletrônico ou informatizado. Mas os crimes de informática são analisados, caracterizados e equiparados a outros crimes dentro do código penal mesmo não havendo sua definição na lei. O Direito

considera os meios de processamento de dados informatizados como meio e não como fim.

O envio de e-mails que ferem a honra de uma pessoa não está definido no Código Penal Brasileiro, mas os advogados e juízes equiparam a crimes contra a honra (Capitulo V do Código Penal).

[*C.Penal*]

2.2 Autoria criminal

O Código Penal define a autoria de um crime em seu título II artigo 13, onde descreve a relação da causalidade. “O resultado, de que depende a existência do crime, somente é imputável a quem lhe deu causa. Considera-se causa a ação ou omissão sem a qual o resultado não teria ocorrido. (Redação dada pela Lei nº 7.209, de 11.7.1984)”

Para se definir o autor de um crime o código penal orienta que, primeiramente, tem-se que verificar se a ação está prevista como crime, determinar o resultado do crime e quem lhe deu causa.

A Norma ISO/IEC 27.002 no item 13.2.3 “Coleta de evidências” orienta que é boa pratica gerar registros para futuros processos jurídicos.

No âmbito dos sistemas as empresas implantam, e utilizam, sistemas de ERP para melhor controlar seus ativos. É de grande importância registrar em *logs*: (1) eventos que determinam a autoria de registros em seu sistema de ERP, (2) os usuários que têm acesso a informação e (3) os registros relativos a estas operações. Os documentos resultantes devem

ser guardados adequadamente para serem analisados nas auditorias de sistema que forem realizadas ou que possam vir a ocorrer.

[*C.Penal*]

2.3 Arquivos de *logs*

São arquivos gerados automaticamente por aplicações e que registram as suas atividades. Estes registros são preciosos no processo de auditoria de sistemas e podem ser de diversos tipos:

Usuários: podem conter informações de *login* e *logout* válidos e de tentativas; hora do evento; dispositivo usado;

Sistemas: registra as ações efetuadas pelo sistema operacional, como erros, status, modificações e atualizações do sistema; desligamentos; e reset sofrido;

Rede: requisições de início de serviço; equipamento envolvido; trafegam e conexões usadas; duração; e período da conexão;

Aplicação: informações sobre erros de ferramentas; e serviços;

Processos: registros de início e fim de processos; quantidade processada; duração e recursos consumidos;

Sistema de arquivos: mudanças de privilégio de arquivos; arquivos abertos; criados; excluídos e copiados.

[*FERREIRA 2006*]

2.4 ERP - Enterprise Resource Planning ou planejamento dos recursos da empresa.

É o nome que as empresas desenvolvedoras de software usam para denominar um sistema completo para administrar todos os setores e recursos da empresa , englobando as áreas de planejamento de necessidades de materiais e planejamento dos recursos de manufaturas, dando um melhor utilização para todos os ativos da empresa.

[*ERNESTO 2007*]

2.5 Auditoria de sistemas – Controle de operações e de uso de recursos tecnológicos

Aspectos a serem observados para minimizar problemas de segurança operacional em sistemas:

a) Processo sistemático de análise de logs, para acompanhamento do uso de computadores;

b) Verificação diária da geração de logs, para detectar possíveis problemas em sua geração;

c) Existência de controle de acesso, adequado de usuários a arquivos e programas do ambiente de produção;

d) Realização de análise e registro de utilização de recursos computacionais, por parte de usuários para futura otimização;

e) Existência de algum sistema que possibilite a gerência avaliar se a utilização dos recursos computacionais é adequada às atividades operacionais;

f) Existência de algum sistema que apure os custos dos recursos computacionais;

g) Existência de cronograma de utilização diária, semanal, quinzenal, mensal e anual do uso dos recursos computacionais;

h) Registro de análise dos recursos, perante o cronograma e quantidade de dados a processar, a fim de identificar possíveis sobrecargas e inviabilizar as operações da empresa;

i) Registro de controle de programas em execução na área de produção, para evitar o uso de programas extra-oficiais no sistema de informação.

[*SCHIMIDT 2006*]

2.6 Auditoria de Sistema – Medidas que amenizam a ocorrência de ameaças em geral

As medidas complementares à segurança da informação e que tendem a minimizar a ocorrência de falhas são:

a) Definição de responsabilidade do usuário: delimitar a área e a função, atribuindo tarefas e autoridade a sua alçada;

b) Treinamento do usuário: para mostrar os recursos a ele conferidos e para a melhor operação, minimizar erros e renovar conhecimentos;

c) Adequação da capacidade do pessoal: em cada etapa do trabalho avaliar se o usuário tem o conhecimento a ele exigido, realocar pessoas ou treinar se necessário.

d) Segregação de Função: não atribuir à mesma pessoa atividades conflitantes, como requisitar e comprar o recurso.

e) Rotação de responsabilidade: Promover dentro de um determinado tempo, a troca de pessoas com funções de alto grau de risco. Um rodízio de pessoas nesta alçada evita a criação de núcleos informais, que podem desvirtuar as operações da empresa.

[*SCHIMIDT 2006*]

2.7 Forense Computacional

A Forense Computacional é um processo de investigação que obedece a métodos científicos e sistemáticos de análise de provas, para reconstituir ações executadas em ativos de tecnologia computacional de armazenamento de informações.

Algumas das técnicas utilizadas na elaboração de peças da forense computacional são:

a) Coleta dos dados: recolher de forma a preservar as características originais das provas, identificar a origem e catalogar as mesmas.

b) Exame dos Dados: Analisar as provas coletadas de forma a não adulteradas e extrair delas informações relevantes à investigação das ações em questão.

c) Analise das Informações: Analisar as informações extraídas e responder as perguntas que motivaram a investigação.

d) Interpretação dos Resultados: Relatar de forma clara e sem dúvidas quais os resultados obtidos e descrever os procedimentos adotados.

Após a análise e se a interpretação ainda precisa de subsídios uma nova coleta de dados pode ser feia, examinada avaliada até chegar o resultado final da investigação.

[*PEREIRA 2007*]

2.8 Norma NBR ISO/IEC 27.002

Existe uma orientação precisa de como implementar um sistema de gestão da segurança da informação, desde dezembro de 2000 quando a parte 1 da norma BS 7799 tornou-se norma oficial da ISO sob código ISO/IEC 17799, hoje, após varias revisões, renomeada como norma ISO/IEC 27.002.

Abaixo, algumas das orientações (melhores práticas) previstas na norma:

a) Registro de Auditoria: Orienta que o próprio sistema produza registros para posterior auditoria de segurança.

b) Proteção das informações dos registros (*log*): Após a geração estes registros devem ser mantidos e protegidos contra alteração para futura analisem.

c) Registro de Usuários: Orienta a ter um procedimento a ser seguido para registro e controle de usuários que tem acesso a informações.

d) Gerenciamento de Senha do Usuário: Orienta como controles podem ser implementados para que os usuários tenham uma senha particular e forte para garanti acesso somente para usuários habilitados.

e) Responsabilidade dos usuários: Orienta como atribuir à responsabilidade da confidencialidade das senhas e das informações liberadas a mesma, através de acordes de confidencialidade firmado entre empresa e usuário.

f) Controle ao Acesso ao Sistema: Mostra maneiras de controlar o acesso a fim de permitir somente o acesso a informação somente a usuários autorizados.

g) Identificação de Usuários: Orienta a centralização do cadastro de usuários e a correta validação do mesmo.

h) Coleta de Evidências: Orienta que o próprio sistema gere informações para futura auditoria de forma a dirimir dúvidas inclusive em âmbito judicial.

[*ISO/IEC 27.002*]

3 METODOLOGIA

3.1 Pesquisa bibliográfica

Determinar quais os controles necessários para atribuir autoria e irretratabilidade nos dados manipulado no ERP, buscando as melhores práticas, segundo a norma ISO/IEC 27.002, de forma a gerar registros fiéis à verdade, para serem usados em auditorias de sistemas e perícia forense e para atender a processos judiciais a serem, eventualmente, instaurados.

3.2 Determinar os itens de avaliação dos registros de controle.

Elaborar uma tabela, contendo os quesitos entendidos como necessários para determinar a autoria e irretratabilidade de informações no sistema de ERP, que atendam as necessidades de auditoria de sistemas e perícias forenses.

3.3 Avaliar o ERP atual da Empresa Vinhos Salton.

Aplicar a tabela obtida no item anterior aos itens considerados como necessários para um efetivo registro das atividades dos usuários no ERP da Empresa Vinhos Salton.

3.4 Cronograma de mudanças para o novo ERP

Documentar as mudanças a serem implementadas no novo ERP da empresa Salton, para que se tenha um efetivo registro das atividades dos usuários no sistema de ERP, com a finalidade de garantir a autoria e irretratabilidade nas informações contidas no sistema.

4 CONTROLES PARA AUTORIA E IRRETRATABILIDADE EM ERP

Este capítulo propõe a introdução de controles em ambiente ERP, para possibilitar a determinação de autoria e irretratabilidade. Tais pontos de controle introduzidos em pontos chave, com orientação das normas ISO/IEC 27.002 poderão ser decisivos para evitar e até mesmo comprovar fraudes.

Propõe-se um sistema de controle desdobrado em 4 partes; (1) Gerenciamento de usuários e Senhas de acesso ao ERP; (2) Controle de autenticação de acesso ao ERP; (3) Controle de ferramentas acessadas no ERP; (4) Controle de manipulação de dados das ferramentas do ERP.

O gerenciamento de usuários e senhas de acesso ao ERP registra todas as alterações de senhas, tem a finalidade de identificar o autor e comprovar que o usuário tem a posse de dados de acesso exclusivos somente conhecidos por ele. O registro efetuado pelo controle de autenticação de entrada ao ERP tem o objetivo de registrar quais usuários estão utilizando o ERP. O controle de acesso às ferramentas do ERP tem a finalidade de registrar quais as ferramentas usuário fez acesso. O controle de manipulação de dados das ferramentas do ERP tem a finalidade de registrar as atividades do usuário dentro das ferramentas do ERP.

Os registros efetuados pelo ERP nos controles de logs citados acima serão utilizados em processos administrativos internos ou em perícias para fornecer dados para determinar a autoria, o esclarecimento de fraudes ou atividades não autorizadas, revelando como, onde, e qual a proporção destes atos.

4.1 Gerenciamento de usuários e senhas de acesso ao ERP

O meio mais comum para a autenticação de usuários é a utilização de senha de acesso. Para tornar esse controle mais forte, a norma ISO/IEC 27.002 sugere vários procedimentos importantes para que o usuário tenha acesso a recursos de informação da empresa, dentro do ERP, todas as atividades relativas ao gerenciamento do usuário e senhas utilizadas por ele devem estar devidamente registradas.

4.1.1 Cadastro de Usuário e senha de acesso ao ERP

Para utilização de senhas individuais no cadastramento de um usuário é necessário atribuir uma senha temporária, com validade restrita. Posteriormente, o próprio usuário deve fazer a alteração da senha, informando a senha temporária e cadastrando uma senha forte contendo letras e números. Desta forma atribuímos ao usuário uma senha forte e particular, somente conhecida por ele.

O cadastro de senha controla também a data de expiração da mesma, obrigando o usuário a realizar a troca de senha temporária pela individual e após forçar a troca de senha em períodos pré-determinados, sem a reutilização de senhas. Este procedimento evita o uso da senha por pessoas que tiveram acesso, de forma indevida aos dados do usuário. Lembrando que a nova senha de ser individual e somente conhecida pelo usuário.

4.1.2 Registro do Gerenciamento de Usuários e senhas de acesso ao ERP

Todos os registros de alteração de senha devem ser gravados em *log;* a gravação deverá conter: os dados como usuário; senha anterior e nova; discriminação do dispositivo de acesso; horário do evento; entre outros. Além destes também deverão ser registradas as mudanças efetuadas com sucesso e as tentativas de troca não efetivadas, utilizando técnicas de criptografia para ocultar a senha, e ter mecanismos que assegurem que os registros sejam protegidos contra alteração indevida.

4.2 Controle de autenticação de acesso ao ERP

No momento que o operador solicitar acesso ao ERP e efetuar a digitação de seu nome de usuário e senha, o sistema não deve mostrar o conteúdo informado no campo da senha, após efetuar a consulta com os dados de acesso, mostrando as mensagens de forma adequada, autenticando o usuário.

Nos casos onde houver erro de digitação na solicitação de autenticação, recomenda-se que seja disparado um temporizador, que será multiplicado pelo número de tentativas de digitação. Este procedimento estimula a digitação correta e cria dificuldades para a possível utilização de programas de quebra de senha.

Todas as tentativas de digitação de usuário e senha devem ser registradas em *log*, mencionando o local físico do dispositivo de acesso, horário da tentativa e os dados informados. Estes registros devem ter um tratamento especial referente ao campo senha, onde técnicas de criptografia são utilizadas para que seu conteúdo não seja acessado por pessoas não autorizadas; e protegidos contra alterações indevidas.

O sistema de controle de autenticação de usuários deve ser alimentado com informações em casos de troca de função ou desligamento de funcionário. Na troca de cargo, recomenda-se que o usuário tenha sua senha bloqueada até a definição de um novo menu; e na demissão, a realização do imediato bloqueio do acesso do usuário.

4.2.1 Registro do controle de autenticação do ERP

Em todas as autenticações feitas no ERP devem ser registradas em *log*: os dados do usuário; senha utilizada; descriminação do dispositivo de acesso; horário do evento. Além das autenticações bem sucedidas, o controle deve também registrar as tentativas não efetivadas, utilizando técnicas de criptografia para ocultar a senha, e ter mecanismos que assegurem que os registros sejam protegidos contra alteração indevida.

4.3 Controles de ferramentas acessadas no ERP

Os registros deste controle disponibilizam informações sobre que ferramentas o usuário faz uso. Juntamente com os demais controles, este controle de ferramentas confirma a utilização da ferramenta. Serve também para verificar se ferramentas autorizadas ao usuário estão alinhadas com a política de segurança e segregação de função, fazendo registro de quem executou a ferramenta utilizada em que momento e qual o dispositivo.

4.3.1 Interface de acesso personalizada do usuário

Se um usuário autenticado tem acesso ao sistema, através dos controles de segregação de funções, pode-se liberar a ele somente as ferramentas compatíveis com sua função na empresa.

Cabe ao controle de utilitários do ERP após a validação de usuário e senha:

a) Disponibilizar interface de fácil navegação e habilitar somente as ferramentas autorizadas a seu uso.

b) Controlar também horário de acesso e tempo utilização da ferramenta e efetuar a desconexão em caso de inatividade ou horário incompatível de operação.

4.3.2 Registro de ferramentas utilizadas

Todos os acessos às ferramentas do ERP utilizados pelo usuário devem ser registrados em *log*, mencionando o usuário, descritivo da ferramenta, dispositivo de acesso utilizado, horário de entrada e saída da ferramenta. Estes registros devem ser armazenados de forma adequada e possuir controles que inibam alterações indevidas.

4.4 Controles de Manipulação de dados das ferramentas do ERP

O registro do controle de manipulação de dados das ferramentas do ERP tem a finalidade de armazenar informações referentes às operações efetuadas pelo usuário no dado manipulado na ferramenta do ERP. Quais os dados inseridos, alterados ou excluídos; e usuário que efetuou a manipulação.

Os registros dos dados manipulados podem ser o mais importante, mas eles isoladamente somente informam as mudanças nos dados. Para um perito forense o registro de controles tem um valor maior se forem segregados e seu conteúdo narrar, de forma cronológica, as operações. A seqüência da geração de registro de auditoria, a independência dos demais controles, o conteúdo das informações, de como o usuário teve acesso a ferramenta, como se autenticou e se a senha é forte e conhecida por somente o usuário, irá formar uma estrutura lógica de como e por quem o ERP foi manipulado.

4.4.1 Registros de manipulação de dados do ERP

A empresa deve eleger quais ferramentas do ERP farão parte deste controle. Em princípio, ferramentas que manipulam ativos da empresa devem fazer parte deste controle, registrando em *log* a manipulação de dados, pois no futuro será de grande valia para a coleta de evidências.

Escolhida a ferramenta, toda a informação cadastrada, alterada ou excluída deve ser registrado em *log*. Este registro deve conter as seguintes informações, usuário, terminal de acesso utilizado, ferramenta do ERP utilizada, nome do arquivo, registro e conteúdo anterior em caso de exclusão ou alteração e conteúdo atual em caso de cadastramento ou alteração.

5 RESULTADOS OBTIDOS

Com o objetivo de gerar registros de forma a subsidiar a auditoria de sistemas de ERP, descreve-se abaixo: (1) Os controles necessários para atribuir autoria e fortalecer a irretratabilidade de usuários. (2) O ponto chave onde deve ser implementado. (3) A finalidade de cada controle.

Controle de *log*	**Ponto chave de Coleta**	**Finalidade do Controle**
Gerenciamento de usuários e senhas	Cadastramento e alterações de senhas	Comprovar a autoria e fortalecer a irretratabilidade do usuário
Controle autenticação ERP	No ato de solicitação de autenticação	Comprovar a entrada no ERP do usuário com senha
Controle de ferramentas do ERP	No ato de solicitação de ferramentas	Comprovar a carga da ferramenta do usuário
Controle de Manipulação de Dados do ERP	Na Ferramenta após toda atualização no Banco de Dados	Comprovar a manipulação do dado em questão feita pelo usuário

No Apêndice A, são descritos os quesitos que podem ser utilizados para avaliar sistemas de ERP no que diz respeito à geração de registros para auditoria de sistema que tem o objetivo de revelar autoria de ações de usuários no ERP avaliado.

No Apêndice B, é mostrada a confrontação entre os quesitos de avaliação com os controles de log do atual ERP. São apontados os pontos fortes do atual controle, e pontos fracos que podem ser implementados no novo ERP da empresa Vinhos Salton S.A.

Para cada quesito de avaliação foi indicada a referência na norma ISO/IEC 27.002 onde se encontra a orientação correta de implementação do controle.

No Apêndice C, o autor deste trabalho sugere um cronograma de melhorias para implementação dos controles de auditoria que poderão atribuir autoria e fortalecer a irretratabilidade dos usuários do ERP da empresa usada como estudo de caso.

É fundamental a implantação de todos os controles descritos no item 4, uma vez que:

(1) Os registros de *logs* da forma descritos geram subsídios para atribuir autoria e irretratabilidade das operações realizadas no ERP pelos usuários do sistema.

(2) A obediência à seqüência de utilização dos usuários no sistema de ERP e registro destas ações na ordem cronológica de eventos é de grande valia em auditoria do sistema ou pericias forenses que podem ser abastecidas com base nos registros; tais fatos aumentam a credibilidade da informação, em caso de litígios judiciais, atribuindo autoria das informações e seu conteúdo.

(3) A responsabilidade atribuída ao usuário pela correta utilização do ERP, quando inserido no contexto de usuários utilizando senhas fortes e de conhecimento pessoal, aliado ao controle de autenticação do sistema, ferramenta acessada e os dados manipulados no ERP, resulta em um registro correto das informações no sistema, com um grau elevado de segurança.

6 CONCLUSÃO

Acredita-se que os objetivos descritos neste trabalho (itens 1.2.1 e 1.2.2) foram obtidos de forma satisfatória.

Os quesitos propostos na planilha do apêndice A podem ser implementados na sua totalidade ou parcialidade, em sistemas de ERP. A geração de registros das ações dos usuários pode ser ajustada a cada sistema ou empresa; ela pode ser feita de forma simples, com apenas a geração dos dados em arquivo de *logs* ou de forma sofisticada com controle de inatividade da ferramenta conexão e promover a desconexão do usuário.

A Avaliação realizada no apêndice B revela que é possível melhorar os registros de auditoria gerados no sistema de ERP da empresa usada como estudo de caso.

No apêndice C tem-se um cronograma de implementação de melhorias simples em pontos chaves do ERP que está sendo implantado na Empresa alvo.

O maior benefício que a empresa poderá ter ao adotar os controles mencionados neste trabalho é tornar o usuário do sistema como responsável pelos dados por ele, usuário, manipulados.

Por fim, recomenda-se fortemente formalizar essa responsabilidade por meio de inserção de cláusulas de confidencialidade, nos contratos firmados entre a empresa e o colaborador que terá acesso à informação, evidenciando esse comprometimento.

REFERÊNCIAS

[*ERNESTO 2007*] HABERKORN, ERNESTO . Um bate-papo sobre gestão empresarial com ERP – São Paulo, Saraiva 2007 cap. 1 pag 14

[*FERREIRA 2006*] FERREIRA, FERNANDO NICOLAU FREITAS E ARAUJO, MARCIO TADEU, Politica de Segurança da informação: guia pratico para elaboração e implementação. Rio de Janeiro: editora Ciência moderna LTDA 2006.

[*SCHIMIDT 2006*] SCHMIDT, PAULO . Fundamentos de auditoria de sistemas. São Paulo: Atlas, 2006.

[*PEREIRA 2007*] PEREIRA E. D. V. et al. *Forense Computacional: fundamentos, tecnologias e desafios atuais*:
Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais – Livro de Minicursos, 2007

[*C.Penal*] Código Penal Brasileiro

Link: WWW.planalto.gov.br/ccivil_03/Decreto_Lei/Del2848compilado.htm acessado em 01/08/2010

[*ISO/IEC 27.002*] NBR ISO/IEC 27002. Tecnologia da Informação: Código de praticas para a gestão da Segurança da informação. Associação Brasileira de Normas Técnicas ABNT.

APÊNDICES

Apêndice A - Planilha de avaliação de quesitos de conformidade com a norma NBR ISO/IEC 27.002 em registros de *log* do sistema de ERP

Apêndice B - Planilha de avaliação de quesitos de conformidade com a norma NBR ISO/IEC 27.002 em registros de *log* do sistema de ERP. Da Empresa Vinhos Salton S.A. (Sistema atual banco de dados Dataflex) em 31/07/2010

Apêndice C - Cronograma de implementações dos registros de *log* do ERP a ser implantado no ano de 2010 utilizando o banco de dados Oracle

Apêndice A - Planilha de avaliação de quesitos de conformidade com a norma NBR ISO/IEC 27.002 em registros de log do sistema de ERP.

Item	Descrição do quesito avaliado	Objetivo do quesito	Peso	Nota	item da Norma NBR ISO/IEC 27.002:2005	Justificativa da nota
1.00	**CONTROLE GERENCIAMENTO DE USUÁRIOS E SENHA DE ACESSO AO ERP**			**0 %**		
1.01	Cadastro de usuários e senha centralizado	Centralização de senhas	10		11.5.2 Identificação e autenticação de usuário	
1.02	Alteração da senha efetuada somente pelo usuário	Atribuir autoria	10		11.3.1 Uso de senhas	
1.03	Cadastro de usuário possui controle de usuário ativo	Segurança da Senha	10		11.5.1 Procedimentos seguros de entrada no sistema	
1.04	Registro de alterações da senha	Registro de log	10		13.2.3 Coleta de evidências	
1.05	Registro identifica o usuário e dispositivo utilizado para alteração da senha, data e horário do evento	Registro de log	10		10.10.1 Registros de auditoria	
1.06	Os registros são protegidos contra alteração	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
1.07	O armazenamento do log é adequado	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
1.08	Na digitação da senha mostra informações adequadas	Segurança da Senha	7		11.5.1 Procedimentos seguros de entrada no sistema	
1.09	Aceita cadastro de senhas frágeis	Segurança da Senha	7		11.3.1 Uso de senhas	
1.10	Aceita senhas antigas já utilizadas	Segurança da Senha	7		11.2.3 Gerenciamento de senha do usuário	
1.11	Registro de log de alteração senha usa criptografia para guarda se senhas	Segurança da Senha	7		11.2.3 Gerenciamento de senha do usuário	
1.12	Possibilita o cadastramento da data de bloqueio do usuário.	Segurança de acesso	5		11.2.1 Registro de usuários	
1.13	Possibilita o cadastro de expiração de senha por tempo de utilização	Segurança de acesso	5		11.2.1 Registro de usuários	
1.14	Possibilita o cadastramento de horário de utilização.	Segurança de acesso	5		11.2.1 Registro de usuários	
1.15	Possibilita o cadastro do tempo para termino de cessão usuário por inatividade	Segurança de acesso	5		11.2.1 Registro de usuários	
2.00	**CONTROLE AUTENTICAÇÃO DE ACESSO AO ERP**			**0 %**		
2.01	Registros de autenticação e tentativas de entrada no sistema de ERP	Registro de log	10		13.2.3 Coleta de evidências	
2.02	Registro identifica o usuário e dispositivo utilizado pela solicitação de autenticação, data e horário do evento	Registro de log	10		10.10.1 Registros de auditoria	
2.03	Os registros são protegidos contra alteração	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
2.04	O armazenamento do log é adequado	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
2.05	Verifica status de usuário ativo	Segurança da Senha	10		11.5.1 Procedimentos seguros de entrada no sistema	
2.05	Na digitação da senha mostra informações adequadas	Segurança da Senha	7		11.5.1 Procedimentos seguros de entrada no sistema	
2.06	Ativa temporizador após digitação de senha invalida	Segurança da Senha	7		11.5.1 Procedimentos seguros de entrada no sistema	
2.07	Registro de log de autenticação usa criptografia para guarda se senhas	Segurança da Senha	7		11.2.3 Gerenciamento de senha do usuário	
2.08	Controla a da data de bloqueio do usuário.	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	
2.09	Controla o horário de utilização do usuário	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	
2.10	Controla o tempo de inatividade da cessão	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	
3.00	**CONTROLE DE FERRAMENTAS ACESSADAS NO ERP**			**0 %**		
3.01	Registro de acesso a ferramenta utilizada e tentativa de acesso	Registro de log	10		13.2.3 Coleta de evidências	
3.02	Registro identifica o usuário e dispositivo utilizado pela solicitação da ferramenta, data e horário do evento	Registro de log	10		10.10.1 Registros de auditoria	
3.03	Os registros são protegidos contra alteração	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
3.04	O armazenamento do log é adequado	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
3.05	Na Interface do sistema ERP é oferecido somente as ferramentas autorizadas ao usuário	Segurança de acesso	7		11.2.1 Registro de usuários	
3.06	Controla o horário de execução de ferramentas	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	
3.07	Desconecta por inatividade da ferramenta	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	
4.00	**CONTROLE DE MANIPULAÇÃO DE DADOS DAS FERRAMENTAS DO ERP**			**0 %**		
4.01	Registros de dados manipulados pelo usuário	Registro de log	10		13.2.3 Coleta de evidências	
4.02	Registro identifica o usuário, dispositivo utilizado, data, horário do evento e atividade executada	Registro de log	10		10.10.1 Registros de auditoria	
4.03	Os registros são protegidos contra alteração	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
4.04	O armazenamento do log é adequado	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
4.05	Controla o horário de execução de ferramentas	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	

Apêndice B - Planilha de avaliação de quesitos de conformidade com a norma NBR ISO/IEC 27.002 em registros de *log* do sistema de ERP.Da Empresa Vinhos Salton S.A. (Sistema atual banco de dados Dataflex) em 31/07/2010

Item	Descrição do quesito avaliado	Objetivo do quesito	Peso	Nota	item da Norma NBR ISO/IEC 27.002:2005	Justificativa da nota
1.00	**CONTROLE GERENCIAMENTO DE USUÁRIOS E SENHA DE ACESSO AO ERP**			**14,4 %**		
1.01	Cadastro de usuários e senha centralizado	Centralização de senhas	10	10	11.5.2 Identificação e autenticação de usuário	Único em todo ERP
1.02	Alteração da senha efetuada somente pelo usuário	Atribuir autoria	10		11.3.1 Uso de senhas	
1.03	Cadastro de usuário possui controle de usuário ativo	Segurança da Senha	10		11.5.1 Procedimentos seguros de entrada no sistema	
1.04	Registro de alterações da senha	Registro de log	10		13.2.3 Coleta de evidências	
1.05	Registro identifica o usuário e dispositivo utilizado para alteração da senha, data e horário do evento	Registro de log	10		10.10.1 Registros de auditoria	
1.06	Os registros são protegidos contra alteração	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
1.07	O armazenamento do log é adequado	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
1.08	Na digitação da senha mostra informações adequadas	Segurança da Senha	7	7	11.5.1 Procedimentos seguros de entrada no sistema	Display adequado
1.09	Aceita cadastro de senhas frágeis	Segurança da Senha	7		11.3.1 Uso de senhas	
1.10	Aceita senhas antigas já utilizadas	Segurança da Senha	7		11.2.3 Gerenciamento de senha do usuário	
1.11	Registro de log de alteração senha usa criptografia para guarda se senhas	Segurança da Senha	7		11.2.3 Gerenciamento de senha do usuário	
1.12	Possibilita o cadastramento da data de bloqueio do usuário.	Segurança de acesso	5		11.2.1 Registro de usuários	
1.13	Possibilita o cadastro de expiração de senha por tempo de utilização	Segurança de acesso	5		11.2.1 Registro de usuários	
1.14	Possibilita o cadastramento de horário de utilização.	Segurança de acesso	5		11.2.1 Registro de usuários	
1.15	Possibilita o cadastro do tempo para termino de cessão usuário por inatividade	Segurança de acesso	5		11.2.1 Registro de usuários	

2.00	**CONTROLE AUTENTICAÇÃO DE ACESSO AO ERP**			**0 %**		
2.01	Registros de autenticação e tentativas de entrada no sistema de ERP	Registro de log	10		13.2.3 Coleta de evidências	
2.02	Registro identifica o usuário e dispositivo utilizado pela solicitação de autenticação, data e horário do evento	Registro de log	10		10.10.1 Registros de auditoria	
2.03	Os registros são protegidos contra alteração	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
2.04	O armazenamento do log é adequado	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
2.05	Verifica status de usuário ativo	Segurança da Senha	10		11.5.1 Procedimentos seguros de entrada no sistema	
2.05	Na digitação da senha mostra informações adequadas	Segurança da Senha	7		11.5.1 Procedimentos seguros de entrada no sistema	
2.06	Ativa temporizador após digitação de senha invalida	Segurança da Senha	7		11.5.1 Procedimentos seguros de entrada no sistema	
2.07	Registro de log de autenticação usa criptografia para guarda se senhas	Segurança da Senha	7		11.2.3 Gerenciamento de senha do usuário	
2.08	Controla a da data de bloqueio do usuário.	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	
2.09	Controla o horário de utilização do usuário	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	
2.10	Controla o tempo de inatividade da cessão	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	

3.00	**CONTROLE DE FERRAMENTAS ACESSADAS NO ERP**			**0 %**		
3.01	Registro de acesso a ferramenta utilizada e tentativa de acesso	Registro de log	10		13.2.3 Coleta de evidências	
3.02	Registro identifica o usuário e dispositivo utilizado pela solicitação da ferramenta, data e horário do evento	Registro de log	10		10.10.1 Registros de auditoria	
3.03	Os registros são protegidos contra alteração	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
3.04	O armazenamento do log é adequado	Seg. Registros Log	10		10.10.3 Proteção das informações dos registros	
3.05	Na Interface do sistema ERP é oferecido somente as ferramentas autorizadas ao usuário	Segurança de acesso	7		11.2.1 Registro de usuários	
3.06	Controla o horário de execução de ferramentas	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	
3.07	Desconecta por inatividade da ferramenta	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	

4.00	**CONTROLE DE MANIPULAÇÃO DE DADOS DAS FERRAMENTAS DO ERP**			**80 %**		
4.01	Registros de dados manipulados pelo usuário	Registro de log	10	10	13.2.3 Coleta de evidências	Possui Registros
4.02	Registro identifica o usuário, dispositivo utilizado, data, horário do evento e atividade executada	Registro de log	10	10	10.10.1 Registros de auditoria	Registro completo
4.03	Os registros são protegidos contra alteração	Seg. Registros Log	10	10	10.10.3 Proteção das informações dos registros	Acesso restrito
4.04	O armazenamento do log é adequado	Seg. Registros Log	10	10	10.10.3 Proteção das informações dos registros	Guarda 5 anos
4.05	Controla o horário de execução de ferramentas	Segurança de acesso	5		11.5.1 Procedimentos seguros de entrada no sistema	

RESULTADO DA AVALIAÇÃO

Pontos fortes:

O atual sistema de ERP da Empresa Vinho Salton tem um controle Centralizado de senha.

Possui registros coletados referente a manipulação de dados efetuado pelos usuários nas ferramentas chaves do ERP.

Os registros do item 4.02 identificam os usuários, dispositivo data, horário e atividade executada no ERP.

Os registros têm acesso restrito e protegidos contra alteração, armazenando os últimos 5 anos.

Pontos fracos:

A parte dos registros voltados a determinar o uso de senha de acesso de conhecimento único do usuário, autenticação no ERP e ferramentas acessadas podem ser melhorados:

1) Registrar o histórico de cadastramento e alterações de senha, identificando quando e onde foi alterada a senha.
2) Registrar o histórico de autenticação e tentativas de acesso ao sistema de ERP pelos usuários, identificando dispositivo usado.
3) Registrar o histórico de ferramentas acessadas e tentativas de acesso pelos usuários para levantamento de uso de programas não homologados.

Apêndice C - Cronograma de implementação dos registros de *log* do ERP a ser implantado no ano de 2010.

A implementação dos registros de log do sistema ERP da Totaldata, que utiliza o Banco de Dados Oracle, pode ser implementado em 4 etapas.

Etapa 1: Cadastramento de usuários e senhas de acesso a ser implantada até janeiro 2011.

Nesta etapa prevê as alterações para que os usuários, depois de cadastrados no sistema, efetuem a alteração da senha inicial dada pelo administrador por uma senha de uso pessoal e controlar a validade e complexidade da senha, registrando as operações em arquivo de log.

Alterações necessárias:

a) Criar no cadastramento do usuário a data do término da validade da senha e status de usuário ativo.
b) Cria no cadastro geral do sistema o número de dias para a troca da senha.
c) Criar o arquivo de log para registro de alteração de senha com os campos: usuário, data da alteração, senha anterior (campo protegido com criptografia), senha atual (campo protegido com criptografia), dispositivo usado e hora do evento.
d) Incluir a digitação do campo validade da senha como campo obrigatório de digitação e sugerir 30 dias da data do cadastramento.

Etapa 2: Controle de autenticação de acesso a ser implantada até janeiro 2011.

Nesta etapa prevê as alterações para que o próprio usuário faça a atualização do usuário e senha para a autenticação do sistema.

Alterações necessárias:

a) Criar o arquivo de log para registro de autenticação do sistema com os campos: usuário, senha utilizada (campo protegido com criptografia), dispositivo usado, hora do evento e autenticação efetuada ou não.
b) Na solicitação do usuário e senha, logo após verificação da digitação, examinar a data de validade da senha; se a data de validade for igual ou maior que a data de vencimento solicitar a entrada da nova senha.
c) Verificar antes de liberar o sistema o status de usuário ativo, liberando o sistema somente para usuários ativos e com senha com data de alteração dentro da validade.
d) Na digitação da nova senha, calcular e atualizar a validade da nova senha, somando a data da validade o número de dias para troca da senha registrada no cadastro geral do sistema e registrando na nova data de vencimento da senha para o usuário.
e) Registrar os dados no arquivo de log de registro de alteração de senhas.
f) Registrar os dados no arquivo de log de registro de autenticação do sistema.

Etapa 3: Registro de ferramentas acessadas no sistema a ser implantada até janeiro 2011.

Nesta etapa prevê as alterações para que o sistema registre as ferramentas acessadas pelos usuários.

Alterações necessárias:

a) Criar o arquivo de log para registro de ferramentas acessadas com os campos: usuário, senha atual (campo protegido com criptografia), ferramenta acessada,dispositivo usado e hora do evento.
b) Registrar os dados no arquivo de log de ferramentas acessadas logo após a abertura da ferramenta.

Etapa 4: Registro de manipulação dos dados das ferramentas do sistema a ser implantada até junho 2011.

Nesta etapa prevê as alterações de toda a manipulação da tabela protegida. Inclusão, alteração e exclusão das informações.

Alterações necessárias:

a) Criar o arquivo de log para registro de dados manipulados no banco de dados contendo: usuário, senha atual (campo protegido com criptografia), ferramenta utilizada, campo alterado, conteúdo anterior, conteúdo atual, dispositivo usado e hora do evento.
b) Registrar os dados no arquivo de log de dados manipulados no banco de dados após a atualização do mesmo.