A IMPORTÂNCIA DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM LABORATÓRIOS DE CALIBRAÇÃO E ENSAIOS

Douglas Mayoral [1]*; José Antonio Florencio Junior* [2]

[1] Gero Comércio e Serviços Ltda., Cerquilho, Brasil, douglas@gero.com.br
[2] Gero Comércio e Serviços Ltda., Cerquilho, Brasil, junior@gero.com.br

Sumário: O propósito deste trabalho é discutir a importância da gestão de segurança da informação em laboratórios de calibração e ensaios e tratar da necessidade de se estabelecer requisitos mais detalhados que possam ser auditados pelos organismos de acreditação.

Palavras chave: segurança da informação; confidencialidade de dados; integridade, autenticidade e validade legal de documentos eletrônicos.

1. INTRODUÇÃO

O resultado do trabalho dos laboratórios de calibração e ensaios é informação e é por conta dela que o cliente contrata um laboratório. Assim, os laboratórios manipulam instrumentos, dados e outras informações que pertencem ao cliente. Estas informações, bem como o certificado ou relatório, que também passa a pertencer ao cliente são, muitas vezes, confidenciais.

Por outro lado, se observarmos do ponto de vista dos laboratórios, a informação é um ativo e, como qualquer outro ativo, tem um valor e uma importância estratégica.

Tanto em um caso quanto no outro temos como elemento chave a informação, a qual se encontra em diversos meios e mídias, bem como se torna de conhecimento das pessoas que lidam com ela.

Além disso, há a crescente e irreversível demanda por certificados em meio eletrônico, devido à inviabilidade de se administrar um grande número de instrumentos por meio de documentos em papel.

Os requisitos atuais da norma ISO IEC 17025 passam levemente pelo tema, não chegando a ter a profundidade necessária para direcionar políticas e procedimentos que garantam a gestão da segurança da informação dentro de um nível apropriado às atividades de calibração e ensaios.

2. OBJETIVO

O objetivo deste trabalho é discutir a importância da definição de requisitos de gestão da segurança da informação para laboratórios de calibração e ensaios.

3. ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NOS LABORATÓRIOS DE CALIBRAÇÃO E ENSAIOS

3.1. Definição do Nível de Segurança

Inicialmente devemos levar em consideração a necessidade da definição do nível de segurança a ser atendido, ou seja, do nível de segurança que a organização se propõe a atender ou que tenha se comprometido com o cliente em atender.

Para que isso seja feito de maneira coerente entre os laboratórios, é necessário que a norma ou o acreditador defina níveis para os sistemas de segurança da informação, por exemplo:

- Nível mínimo –apenas controles imprescindíveis para que os laboratórios sejam acreditados;
- Nível médio – adequado à manipulação de informação por meios eletrônicos e para o envio de certificados de calibração em ensaio no formato digital;
- Nível alto – no qual a estrutura e controles do laboratório permitiriam alto grau de confiabilidade e confidencialidade.

Também devemos levar em conta que talvez determinadas calibrações e ensaios somente atinjam o nível adequado, em termos de segurança de informação, se realizado pelo pessoal próprio do cliente, sendo que terceiros não seriam “seguros”. Com isso, teríamos ainda outro nível, apenas disponível para calibrações e ensaios realizados internamente e com pessoal próprio do detentor da informação sigilosa (por exemplo, em pesquisa e desenvolvimento).

Para definir o nível de segurança desejado, primeiramente o laboratório deve levantar as exigências (e) de seus clientes, os compromissos já assumidos e a realizar uma análise de riscos. Com base nestas informações a (e) direção da organização juntamente com a gerência do laboratório podem fazer uma análise crítica e definir o nível de segurança desejado.

3.2 Análise de Risco

A análise de risco é fundamental para o correto planejamento das diretrizes, recursos e controles do sistema de segurança da informação. Assim, deve ser dedicada a ela especial atenção, de modo que seja adotada a melhor prática possível, considerando as características e limitações do laboratório.

Dada a sua importância, a análise de risco deve envolver os responsáveis pelas diversas áreas do laboratório, inclusive do responsável pela segurança patrimonial e, é claro, do pessoal de TI.

3.3 Política de Segurança da Informação

3.3.1 Geral

É fundamental que seja definida, divulgada e implantada uma política de segurança de informação.

A política de segurança da informação deve ser muito mais ampla e detalhada do que a política do sistema de gestão da qualidade. Isso para explicitar, tanto para clientes quanto internamente, o nível de segurança que a organização se compromete a atender, como também para:

- Deixar clara a importância das sistemáticas e procedimentos que serão adotados;
- Estabelecer os acordos de confidencialidade e termos de responsabilidade;
- Declarar comprometimento com requisitos estatutários, legais ou contratuais;
- Para dar amparo legal a ações que possam ser necessárias para tratar desvios;
- Para definir as diretrizes e sistemáticas para atingir o nível pretendido;
- Para definir diretrizes e relação às partes externas à organização.

A política de segurança da informação deve estabelecer diretrizes para implantação dos controles e das ações de conscientização e treinamento necessários. Deve também abordar o uso de software, normas e de outros materiais com direitos autorais, assim como o uso da rede de informática para fins ilícitos como pirataria, pedofilia etc.

Além disso, a política de segurança da informação deve dar diretrizes e servir de referência para a conscientização das pessoas quanto às conseqüências e ações disciplinares decorrente de mau uso dos recursos ou de ações que ponham em risco o sistema de segurança da informação ou informações restritas.

Aprendendo com o que acontece na implementação de outros sistemas de gestão, os laboratórios devem tomar cuidado para elaborar uma política que realmente seja compatível com suas características e atenda suas necessidades. Uma política publicada e não praticada provavelmente trará resultados piores para o laboratório e para sua imagem que do que a inexistência de uma política.

3.3.2 Estabelecimento de Responsabilidades

Como existe muita informação em meio eletrônico a responsabilidade pela segurança da informação tende a ser direcionada para o setor de TI. Mas na verdade segurança da informação envolve todas as áreas e todos os níveis de uma organização. Para que a política de segurança da informação seja implementada é necessário estabelecer os responsáveis por cada ativo importante levantado no inventário de informações e as responsabilidades para a proteção destes ativos.

3.3.3 Análise Crítica da Política de Segurança da Informação

Devido à velocidade das mudanças de requisitos, processos e tecnologias é normal que diretrizes, definições e controles se tornem obsoletos. Por isso, além da análise inicial, deve ser prevista uma análise crítica periódica da política de segurança da informação. Para realizar esta análise o laboratório precisará:

- Revisar o inventário de informações;
- Verificar a alteração da legislação e de requisitos internos, regulamentares ou contratuais;
- Realizar nova análise de risco;
- Consolidar dados sobre auditorias e incidentes de segurança da informação.

A análise crítica poderá resultar em novas definições de metas e objetivos e na necessidade de novos recursos ou controles.

3.3.4 A Direção da organização, do laboratório e a Segurança da Informação

Toda política a ser adotada por uma organização depende de que a Direção entenda sua necessidade e importância, concorde com ela e queira que a mesma seja implantada. Qualquer projeto a ser implementado que dependa de uma política de gestão e não conte com o comprometimento da Direção está fadado ao fracasso.

Para que a Política de Segurança da Informação seja realmente implementada, a Direção da organização precisa estar comprometida com ela, fornecer os recursos e, tão importante quanto, dar o apoio político necessário para vencer as resistências em todos os níveis.

3.4 Classificação da Informação

A informação deve ser classificada para receber um nível adequado de proteção e para que os esforços, recursos e limitações sejam proporcionais ao valor da informação, ao risco estimado e aos compromissos assumidos. Para isso, devemos levar em consideração o nível de segurança que a organização se propõe a atender ou que tenha se comprometido com o cliente em atender.

Sendo assim, a informação deve ser classificada com base no nível de segurança escolhido, na análise de riscos e na política de segurança da informação, sendo compatível com estes. Usualmente as classificações são:

- Secreta – informação que devem ficar restritas a um pequeno grupo de pessoas, pois tem um

grande dano potencial atrelado ao seu acesso indevido;

- Confidencial – informação que deve ficar dentro do âmbito da organização, apresenta potencial para danos, caso tornada pública;
- Interna – informação que deve ficar dentro do âmbito da organização, porém apresenta baixo potencial para danos, caso tornada pública;
- Pública – informação que pode ou deve ser tornada pública.

O laboratório deve analisar do risco associado às informações antes de classificá-las. A realização da classificação da informação deverá ser feita em conjunto com o responsável pelo ativo.

Deve ser definido um período para realização de uma revisão da classificação das informações para garantir que contínua adequada.

3.5. Proteção da Informação

3.5.1 Geral

O foco do sistema de segurança da informação é a proteção da informação, ou seja, garantir sua autoria, integridade, disponibilidade e confidencialidade. Para cada tipo de informação, um ou outro dos aspectos citados pode ser mais relevante, mas de uma maneira geral podemos dizer que as principais necessidades em termos de proteção são:

- Proteção de dados e privacidade de informações pessoais;
- Salvaguarda de registros organizacionais;
- Direitos de propriedade intelectual;
- Uso adequado, proteção da informação de propriedade do cliente.

A fim de proteger as informações os laboratórios normalmente utilizam as tradicionais ferramentas: controle de acesso físico, backup, antivírus, firewall e senhas para acesso à rede, e-mails e documentos. Porém, normalmente serão necessários outras políticas, procedimentos e controles para atingir este objetivo, os quais devem cobrir de forma consistente a abrangência do fluxo de informações. Isto significa que deve ser considerado o trabalho nas instalações do cliente, o uso e transito de mídias (inclusive papel), as conexões sem fio, o acesso remoto etc. Especial atenção deve ser dada à formulação de política e controles para trocas de informação por e-mail e mensagens instantâneas.

Da mesma forma que temos que tratar o fluxo de informações que saem das instalações do laboratório, também temos que nos preocupar com as pessoas que entram nele. Neste sentido é importante definir uma política para o acesso de visitantes às instalações físicas e à rede. Estes visitantes podem ser clientes, avaliadores, prestadores de serviços entre outros e suas atividades no laboratório estão atreladas a um determinado risco, que deve ser avaliado e tratado.

Os procedimentos e controles para proteção da informação deverão ser planejados em duas linhas complementares:

- Prevenção: tentar evitar que aconteça;
- Recuperação: voltar ao funcionamento normal após um incidente.

Eles serão definidos em função da análise de riscos de segurança da informação, do nível de segurança requerido e da Política de Segurança da Informação. Mas é importante termos em mente que nem todos os controles são aplicáveis ou praticáveis em todas as organizações.

A implementação das políticas, controles e procedimentos passa necessariamente pela conscientização e treinamento das pessoas envolvidas. Porém, os especialistas em segurança consideram “pessoas” como o elo mais fraco da segurança. Isso significa que, quanto menos a segurança das informações dependerem das pessoas, tanto melhor. Por exemplo, se não houver alguma limitação no processo, é provável que alguém escolha a senha “1234” ou outra igualmente fácil de ser descoberta. Daí o uso cada vez mais popular de dispositivos geradores de senha, como os tokens.

Por isso, para aumentar a segurança, o laboratório deverá assegurar que funcionários, fornecedores e terceiros conheçam entendam suas responsabilidades e estejam de acordo com seus papeis e reduzir risco de furto ou roubo fraude ou mau uso de recursos. Mas também precisará tomar medidas para limitar as pessoas de, intencionalmente ou não, afetarem negativamente a segurança.

Fechando o ciclo de melhoria, o laboratório precisará estabelecer ferramentas de monitoramento e auditoria, ferramentas e sistemáticas de análise e tomar ações preventivas e corretivas para melhoria do sistema. Adicionalmente, o laboratório poderá tomar ações preventivas analisando incidentes sofridos por outras organizações e acompanhando a evolução tecnológica tanto das ameaças quanto das ferramentas de segurança.

3.5.2 Uso de senhas e ferramentas de criptografia

O uso de senhas faz parte de nosso cotidiano e, é claro, tem singular importância para a segurança da informação. Assim como o uso adequado das senhas pode ser de grande valor, seu uso incorreto pode deixar as informações do laboratório totalmente expostas.

Outro elemento de suma importância para a proteção dos dados é a criptografia. Certamente agrega valor para o laboratório a definição de sistemáticas para seleção e uso de ferramentas adequadas de criptografia. Conforme sistematizado pelo laboratório, estas ferramentas poderão ser utilizadas para guarda, assinatura e envio de documentos. Entre estas ferramentas destacamos a assinatura digital e os certificados digitais, que discutiremos mais à frente, e podem ter um papel fundamental no aumento da confiabilidade e da agilidade das relações entre o INMETRO, o laboratório e o cliente.

No intuito de extrair o máximo de benefício destes elementos para a segurança da informação, o laboratório

precisará definir processos para gerenciar as senhas, as chaves criptográficas e os certificados digitais. Os processos deverão controlar a adequação das senhas, a distribuição chaves e os incidentes com chaves e senhas. Também deverão controlar a validade dos certificados e senhas.

3.6. Pessoal

Provavelmente o pessoal interno seja principal fator de risco à segurança da informação de qualquer organização.

É comum o uso de "termo de confidencialidade" como forma de comprometer as pessoas com necessidade de se proteger a informação. E é realmente importante a aplicação deste documento, principalmente como ferramenta de conscientização e para dar amparo legal caso necessário uma ação disciplinar. Porém, perda, dano ou vazamento de informação pode ser causado por ações que vão além do que normalmente é previsto em um termo de confidencialidade como, entre outras:

- Uso indevido da Internet;
- Impressão não autorizada de documentos ou descarte inadequado dos mesmos;
- Restrição insuficiente de acesso de clientes durante auditorias ou visitas técnicas;
- Trafego de informações em trabalho externo ao laboratório,
- Terceirização ou subcontratação.

É necessário o desdobramento da política de segurança da informação citada anteriormente, em outras políticas e sistemáticas como:

- Política para uso de recursos de informática;
- Procedimento para seleção, contratação, demissão e mudança de função;
- Definição de um processo disciplinar formal.

Também é importante que o laboratório tenha procedimentos para contratação, demissão, mudança de cargo e função que considerem:

- Descrição de cargo definindo claramente o papel referente a segurança da informação;
- Conscientização, educação e treinamento: uso adequado dos recursos, cumprimento da política de segurança da informação e outras políticas pertinentes;
- Termo de responsabilidade de guarda e uso de senhas;
- Termo de responsabilidade no uso de ativos (recursos, informações, acessos etc);
- Conscientização de que a validade dos acordos de confidencialidade as responsabilidades com relação à segurança da informação se estendem fora da organização, do horário de trabalho e do período de contratação;
- Situações nas quais cabe devolução de ativos, retirada ou atribuição de privilégios e direitos de acesso etc.

3.7. Validade de Certificados em Meios Eletrônicos

3.7.1 Assinatura Digital

Existe uma demanda crescente por certificados em formato digital. Isso ocorre devido a inviabilidade de se controlar um número grande de instrumentos utilizando documentos em papel ou de se redigitar informações em planilhas ou sistemas de controle.

A validade jurídica de certificados em meios eletrônicos depende de que os mesmos possuam uma assinatura eletrônica conforme os requisitos legais determinados pelos países envolvidos. No Brasil, a validade das assinaturas eletrônicas depende da conformidade com a medida provisória MP 2.200-2 e aos processos criados em decorrência dela.

A assinatura digital, embora também sirva para comprovar a autoria de um documento, é completamente diferente da assinatura que fazemos em papel. É tão diferente que é muito mais simples acreditar que assinatura digital seja a imagem de uma rubrica ou firma colada em um documento digital do que compreender seu conceito atual: um conjunto de operações criptográficas aplicadas a um determinado arquivo, que permite dar a ele garantia de integridade e autenticidade. Os dois elementos são importantes para confiarmos no arquivo: a integridade para garantir que não foi corrompido ou adulterado e a autenticidade para que o destinatário saiba que foi realmente este documento que o signatário que o assinou.

Os mesmos mecanismos criptográficos que permitem a assinatura digital podem ser usados para que o documento seja enviado ao destinatário de forma confidencial.

Para dar confiabilidade e reconhecimento jurídico ao processo de assinatura digital existe o certificado digital e a estrutura de certificação.

O certificado digital é o documento que vai garantir a identidade virtual do signatário. Para ter validade jurídica no Brasil, o certificado digital deve ser assinado por uma autoridade certificadora credenciada pela Autoridade Certificadora Raiz.

3.7.2 Estrutura da certificação digital no Brasil

A Medida Provisória 2.200-2, de 24 de agosto de 2001 instituiu a ICP-Brasil (Infra-estrutura de Chaves Públicas Brasileira). Também criou o Comitê Gestor da ICP-Brasil, a Autoridade Certificadora Raiz Brasileira e definiu as demais entidades que compõem sua estrutura. A partir dessa MP, foram elaborados os regulamentos, Instruções Normativas e outros documentos que regem as entidades integrantes da Infra-estrutura de Chaves Públicas Brasileira.

O modelo de Infra-estrutura adotado pela ICP-Brasil foi o de Certificado com Raiz única, sendo que a autoridade certificadora raiz é o Instituto Nacional de Tecnologia da Informação - ITI. Cabe ao Instituto credenciar os demais

participantes da cadeia, supervisionar e fazer auditoria dos processos.

3.7.3 Entendendo assinatura digital

A assinatura digital utiliza recursos de criptografia para garantir a integridade e autenticidade de documentos eletrônicos, podendo também ser utilizada para enviar arquivos a um determinado destinatário com confidencialidade. Os principais recurso utilizados são:

- Função hash: produz um resumo do arquivo original. O objetivo da função hash é que cada arquivo possua um resumo único, ou seja, por menor que seja a diferença entre dois arquivos, a função hash deve gerar resumos diferentes para cada um deles. Isso é fundamental para garantir que um arquivo não foi corrompido ou adulterado.

Chave assimétrica: um par de códigos relacionados denominados chave pública e chave privada. A criptografia feita com a chave pública pode ser decifrada com a chave privada. Da mesma maneira, a criptografia feita com a chave privada pode ser desfeita com a chave pública. Porém elas são complementares, nenhuma delas pode reverter a própria criptografia.

É claro que tanto a função hash como as chaves não são perfeitas. Existem organizações nacionais e internacionais que tratam de garantir o uso das tecnologias mais seguras e atualizadas nas estruturas de chaves públicas.

Para assinar um documento, utilizamos um software que aplica a função hash para gerar um resumo do arquivo. Este resumo é então criptografado com a chave privada do autor e anexado ao arquivo original (vide figura 1).

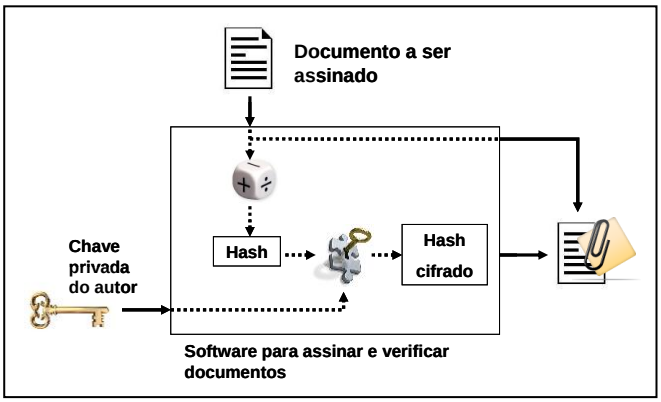

Figura 1 – Assinatura de documento

Para verificar a assinatura o destinatário precisa ter a chave pública do autor, para isso ele deve receber seu documento de identidade eletrônico, o certificado digital, do qual trataremos adiante.

Quando o destinatário vai verificar a assinatura o software:

- gera um resumo do arquivo recebido usando a função hash (da mesma forma que na assinatura)
- decifra o resumo anexo utilizando a chave pública do autor.
- Depois disso compara os dois resumos se forem iguais, nenhum dos dois arquivos foi alterado (vide figura 2).

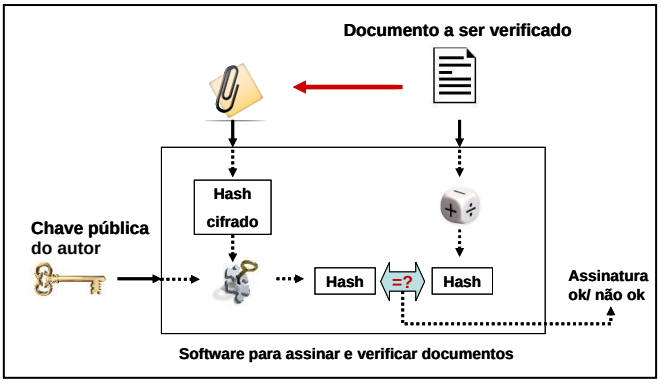

Figura 2 – Verificação da Assinatura

Caso o arquivo original tenha sido alterado (adulterado ou corrompido), ele produzirá um hash diferente do gerado pelo arquivo original, isso será percebido pelo software e a assinatura não será validada.

Outra possibilidade é a pessoa que adulterar o arquivo gerar um novo resumo (utilizando a função hash). Como ele não possui a chave privada do autor, não conseguirá gerar um resumo criptografado idêntico, novamente a assinatura não será validada.

Numa terceira hipótese, uma pessoa adultera o arquivo, gera uma assinatura usando uma chave privada que não é a do autor do arquivo original e envia a chave pública correspondente. Neste caso o software vai decifrar o resumo que vem anexo com o arquivo e notar que é idêntico ao resumo gerado pela função hash. Porém, haverá inconsistência no certificado digital e a assinatura novamente não será validada.

3.7.4 Certificados Digitais

Neste contexto "certificados digitais" não se refere a certificados de calibração ou ensaio, mas sim à identidade virtual do autor.

Os Certificados Digitais são compostos por um par de chaves (Chave Pública e Privativa) e a assinatura de uma terceira parte confiável - a Autoridade Certificadora – AC. A chave provada fica instalada no computador do autor ou em dispositivos como tokens. Já a chave pública é disponibilizada para o destinatário por meio do certificado digital.

Para o destinatário ter certeza que a chave pública pertence mesmo ao autor e é válida, o software consulta a AC. Continuando a cadeia de credibilidade, a AC deve ser credenciada pela Autoridade Certificadora Raiz.

O Brasil optou pelo modelo de certificação que prevê uma única certificadora raiz. O Instituto Nacional de Tecnologia da Informação - ITI foi estabelecido como Autoridade Certificadora Raiz. Cabe ao ITI credenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

O modelo de certificação adotado seguiu critérios internacionais para permitir o estabelecimento de acordos de reconhecimento mútuo da certificação digital, como ocorreu,

por exemplo, no Mercosul. Na XXXI reunião do Grupo, realizada em Córdoba, na Argentina onde ocorreu a aprovação da Normativa Mercosul sobre Certificação Digital.

3.7.5 Assinatura digital Aumentando a Confiabilidade da RBC

Como acontece em outras áreas, também existe quem falsifique certificados de calibração da RBC.

O uso de assinaturas digitais nos certificados em meio eletrônico garante a integridade, autoria e dá amparo legal aos mesmos.

Apenas para relembrar, a assinatura digital não significa análise do conteúdo, o conteúdo deve ser analisado pelo signatário autorizado do laboratório. A assinatura digital irá garantir que foi o signatário que assinou e que o conteúdo não foi alterado.

Porém, benefícios ainda maiores ocorreriam caso o INMETRO entrasse na cadeia hierárquica da infra-estrutura de chaves públicas do Brasil. Isto porque a assinatura somente seria disponibilizada aos signatários.

Neste cenário, os certificados de calibração e ensaios em formato eletrônico seriam mais confiáveis que os em papel, pois falsificações como alteração de data de calibração, nome do laboratório emissor e até mesmo conteúdo poderiam ser coibidas. Também coibiria a emissão de certificados com logo da acreditação por empresas não acreditadas.

3.8 Incidentes com segurança da informação

Todo o sistema deve ser voltado para proteger as informações, porém nenhum sistema está livre de incidentes de segurança da informação. As organizações estão sujeitas a diversas situações que podem exceder sua capacidade de preparação ou controle. São exemplos de incidentes em segurança da informação:

- Eventos climáticos, como inundações;
- Descumprimento à política de segurança da informação;
- Perda ou roubo de computadores, mídias ou documentos;
- Tentativas de ganhar acesso não autorizado a sistemas ou dados, ataques eletrônicos ao sistema de informações;
- Alterações não autorizadas de documentos ou sistemas;

O laboratório deve estar preparado para se recuperar em caso de incidentes de segurança da informação e a aprender com ele.

Neste sentido, a norma ABNT NBR ISO IEC 27002 recomenda adoção da gestão da continuidade do negócio, que é uma prática que define a políticas e processos para uma organização se preparar para responder aos incidentes, a fim de dar continuidade às suas operações num nível predefinido como aceitável.

4. CONCLUSÃO

Considerando o valor estratégico da informação, tanto para os laboratórios de calibração e ensaios quanto para seus clientes, percebemos a importância de manipular e guardar a mesma de forma segura.

De mesma maneira que um sistema de gestão da qualidade ajuda uma organização a manter um nível de qualidade adequado e impulsiona a melhoria contínua, um sistema de gestão da segurança da informação aumenta a confiança em que esta organização trate adequadamente este importante e delicado ativo.

Mas temos que levar em conta também que um sistema de segurança da informação deve ser estruturado sem sobrecarregar ou inviabilizar os laboratórios, mas ainda assim garantindo sua confiabilidade.

Com o exposto, podemos perceber que não é uma tarefa simples o estabelecimento de um modelo, porém a definição de regras para um sistema de gestão da segurança da informação voltado a laboratórios de calibração e ensaio terá grande valor para manutenção e ampliação da confiança que o mercado tem nos laboratórios acreditados.

Também podemos concluir que a utilização de certificados de calibração e ensaios com assinatura digital podem torná-los mais confiáveis que os certificados em papel.

AGRADECIMENTOS

Quero agradecer à Direção da Gero Comércio e Serviços Ltda. que incentivou e colaborou de várias formas com este trabalho.

REFERÊNCIAS

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - **ABNT NBR ISO IEC 17025:2005** – Requisitos gerais para competência de laboratórios de ensaio e calibração. Rio de Janeiro, 2005.

[2] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - **ABNT NBR ISO IEC 2700:2006**– Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, 2006.

[3] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - **ABNT NBR ISO IEC 27002:2005** – Tecnologia da Informação – Técnicas de segurança – Código de prática para gestão da segurança da informação. Rio de Janeiro, 2005.

[4] BRASIL. Medida provisória n.º 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Acessado em 10/03/2011 em http://www.iti.gov.br/twiki/bin/view/Certificacao/MedidaProvisoria