Gestão de Incidentes de Segurança da Informação - Coleta de evidências

Controle

Incidente de SI → Ação de Acompanhamento contra pessoa/organização → Envolvendo ação legal (civil ou criminal) → **Evidências coletadas, armazenadas e apresentadas em conformidade com as normas da jurisdição pertinente.**

"Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), convém que evidências sejam coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição(ões) pertinente(s)."

Diretrizes para implementação

Convém que sejam elaborados e respeitados procedimentos internos para a coleta e apresentação de evidências com propósito de ação disciplinar.

Características das evidências:

a) **admissibilidade** da evidência: se a evidência pode ser ou não utilizada na corte;

b) **importância** da evidência: qualidade e inteireza da evidência.

Para obter a **admissibilidade**: convém que sistemas de informação estejam de acordo com qualquer norma ou código de prática publicado para produção de evidência admissível.

Convém que o **valor da evidência** esteja de acordo com algum requisito aplicável. Para obter o valor da evidência, convém que a qualidade e a inteireza dos controles usados para proteger as evidências sejam demonstradas por uma trilha forte de evidência.

Trilha forte de evidência:

a) **para documentos em papel**: o original é mantido de forma segura, com um registro da pessoa que o encontrou, do local e data em que foi encontrado e quem testemunhou a descoberta; convém que qualquer investigação assegure que os originais não foram adulterados;

b) **para informação em mídia eletrônica:** convém que imagens espelho ou cópias (dependendo de requisitos aplicáveis) de quaisquer mídias removíveis, discos rígidos ou em memórias sejam providenciadas para assegurar disponibilidade; convém que seja mantido registro das ações tomadas durante a cópia e de quem testemunhou; convém que a mídia original que contém a informação e o registro seja mantido de forma segura e intocável.

Convém que qualquer trabalho forense seja somente realizado em cópias do material de evidência; que a integridade de todo material de evidência seja preservada; que o processo de cópia de todo material de evidência seja supervisionado por pessoas confiáveis e que as informações sobre a data, local, pessoas, ferramentas e programas envolvidos no processo de cópia sejam registradas.

Informações adicionais

- ✓ Existe o perigo de que a evidência seja destruída intencional ou acidentalmente antes que seja percebida a seriedade do incidente. É conveniente envolver um advogado ou a polícia tão logo seja constatada a possibilidade de processo jurídico e obter consultoria sobre as evidências necessárias.
- ✓ Convém assegurar que a organização seja devidamente autorizada para coletar as informações requeridas como evidências que ultrapassem seus limites organizacionais/jurisdicionais.
- ✓ Convém que os requisitos de diferentes jurisdições sejam também considerados para maximizar as possibilidades de admissão da evidência em todas as jurisdições relevantes.

Gestão da Continuidade do Negócio – Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação

Controle

Interrupção ou falha de processos críticos → Plano de continuidade → **Assegurar disponibilidade da informação no nível requerido e na escala de tempo requerida.**

"Convém que os planos sejam desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio."

Diretrizes para implementação

Planejamento da continuidade de negócios deve considerar:

a) identificação e concordância de todas as responsabilidades e procedimentos da continuidade do negócio;

b) identificação da perda aceitável de informações e serviços;

c) implementação dos procedimentos que permitam a recuperação e restauração das operações do negócio e da disponibilidade da informação nos prazos necessários; atenção especial precisa ser dada à avaliação de dependências externas ao negócio e de contratos existentes;

d) procedimentos operacionais que permitam a conclusão de restauração e recuperação que estejam pendentes;

e) documentação dos processos e procedimentos acordados;

f) educação adequada de pessoas nos procedimentos e processos definidos, incluindo o gerenciamento de crise;

g) teste e atualização dos planos.

Convém que o processo de planejamento foque os objetivos requeridos do negócio. Convém identificar os serviços e recursos que facilitam isso, prevendo a contemplação de pessoal e recursos em geral, além da tecnologia de informação, assim como o procedimento de recuperação dos recursos de processamento das informações.

Convém que o plano de continuidade do negócio trate as vulnerabilidades da organização, que pode conter informações sensíveis e que necessitem de proteção adequada.

Convém que cópias do plano de continuidade do negócio sejam guardadas em um ambiente remoto, a uma distância suficiente para escapar de qualquer dano de um desastre no local principal. Convém que o gestor garanta que as cópias dos planos de continuidade do negócio estejam atualizadas e protegidas no mesmo nível de segurança como aplicado no ambiente principal. Convém que outros materiais necessários para a execução do plano de continuidade do negócio também sejam armazenados em local remoto.

Convém que, se os ambientes alternativos temporários forem usados, o nível de controles de segurança implementados nestes locais seja equivalente ao ambiente principal.

Informações adicionais

Convém que seja destacado que as atividades e os planos de gerenciamento de crise (ver 14.1.3 f)) possam ser diferentes de gestão de continuidade de negócios, isto é, uma crise pode acontecer e ser suprida através dos procedimentos normais de gestão.

Gestão de Riscos: Identificação de Ameaças (ISO 27005 / BS 7799:3)

O processo de gestão de riscos definido pela BS 7799:3 (2006) tem como objetivo prover uma organização na compreensão dos riscos operacionais existentes, a fim de permitir uma decisão mais efetiva quanto aos controles necessários associados aos riscos mensurados.

A norma em si não trata de identificação de ameaças, apenas o conceito.

Ameaça - Ação que pode afetar a segurança de bens corporativos e causar a destruição, divulgação, modificação de dados e / ou impedir o funcionamento de um sistema. Exemplo: hackers; crackers; agentes naturais; vândalos;

Ainda:

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização [ISO/IEC 13335-1:2004]

Se a banca examinadora quis dizer realmente “Ameaças” as ISO/IEC 13335-1 e -3 fazem tratamento das mesmas dentro da análise de riscos.

Método de análise de tipo de riscos

A análise de riscos tem os seguintes estágios:

- Identificação dos bens e seus valores;
- Avaliação das ameaças;
- Avaliação das vulnerabilidades;
- Avaliação das medidas de segurança existentes ou planejadas;
- Avaliação dos riscos.

A avaliação dos riscos é uma combinação dos impactos causados por incidentes e o nível das ameaças e vulnerabilidades levantadas. Os riscos são em função dos:

- valores dos bens;
- as ameaças;
- a facilidade de exploração das vulnerabilidades pelas ameaças;
- as medidas de segurança, que podem reduzir as vulnerabilidades.

O objetivo da análise de risco é identificar os riscos aos quais os sistemas estão expostos, a fim de selecionar as mais apropriadas medidas de segurança. Para avaliar os riscos diversos aspectos devem ser considerados, incluindo o impacto e a freqüência com que eles ocorrem.

O impacto pode ser avaliado de modo quantitativo ou qualitativo, ou até mesmo de uma combinação de ambos. Para avaliar a freqüência com que o risco ocorre, deve ser estabelecido um período de tempo durante o qual os bens necessitam estar protegidos. A probabilidade de uma ameaça ocorrer é afetada pelos seguintes itens:

- **A atratividade** do bem;
- **A facilidade de conversão do bem em recompensa**;
- **As capacidades técnicas do agente ameaçador**;
- **A freqüência** da ameaça;
- **A susceptibilidade da vulnerabilidade às ameaças**.

A avaliação das ameaças e das vulnerabilidades são classificadas em ALTA, MÉDIA, BAIXA, geralmente feitas através de questionários feitos aos funcionários técnicos, pessoal, inspeções nos locais e revisões de documentação. Feito isso, pode-se medir o risco. Para cada bem, as vulnerabilidades relevantes e suas correspondentes ameaças são consideradas. Se existe uma vulnerabilidade sem ameaça, ou ameaça sem vulnerabilidade, então não há risco algum.

* **Risco** - combinação da probabilidade de um evento e de suas conseqüências [ABNT ISO/IEC Guia 73:2005].

Classificação da informação

Objetivo: Assegurar que a informação receba um nível adequado de proteção.

Convém que a informação seja classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação.

A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Convém que um sistema de classificação da informação seja usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento.

7.2.1 Recomendações para classificação

Controle

Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.

Diretrizes para implementação

Convém que a classificação da informação e seus respectivos controles de proteção levem em consideração as necessidades de compartilhamento ou restrição de informações e os respectivos impactos nos negócios, associados com tais necessidades.

Convém que as diretrizes para classificação incluam convenções para classificação inicial e reclassificação ao longo do tempo, de acordo com algumas políticas de controle de acesso predeterminadas (ver 11.1.1)

Convém que seja de responsabilidade do proprietário do ativo (ver 7.1.2) definir a classificação de um ativo, analisando-o criticamente a intervalos regulares, e assegurar que ele está atualizado e no nível apropriado.

Convém que a classificação leve em consideração a agregação do efeito mencionado em 10.7.2.

Convém que cuidados sejam tomados com a quantidade de categorias de classificação e com os benefícios obtidos pelo seu uso. Esquemas excessivamente complexos podem tornar o uso incômodo e ser inviáveis economicamente ou impraticáveis. Convém que atenção especial seja dada na interpretação dos rótulos de classificação sobre documentos de outras organizações, que podem ter definições diferentes para rótulos iguais ou semelhantes aos usados.

Informações adicionais

O nível de proteção pode ser avaliado analisando a confidencialidade, a integridade e a disponibilidade da informação, bem como quaisquer outros requisitos que sejam considerados.

A informação freqüentemente deixa de ser sensível ou crítica após um certo período de tempo, por exemplo quando a informação se torna pública. Convém que estes aspectos sejam levados em consideração, pois uma classificação superestimada pode levar à implementação de custos desnecessários, resultando em despesas adicionais.

Considerar, conjuntamente, documentos com requisitos de segurança similares, quando da atribuição dos níveis de classificação, pode ajudar a simplificar a tarefa de classificação.

Em geral, a classificação dada à informação é uma maneira de determinar como esta informação vai ser tratada e protegida.

7.2.2 Rótulos e tratamento da informação

Controle

Convém que um conjunto apropriado de procedimentos para rotulação e tratamento da informação seja definido e implementado de acordo com o esquema de classificação adotado pela organização.

Diretrizes para implementação

Os procedimentos para rotulação da informação precisam abranger tanto os ativos de informação no formato físico quanto no eletrônico.

Convém que as saídas de sistemas que contêm informações classificadas como sensíveis ou críticas tenham o rótulo apropriado da classificação da informação (na saída). Convém que o rótulo reflita a classificação de acordo com as regras estabelecidas em 7.2.1. Itens que devem ser considerados incluem relatórios impressos, telas, mídias magnéticas (fitas, discos, CD), mensagens eletrônicas e transferências de arquivos.

Convém que sejam definidos, para cada nível de classificação, procedimentos para o tratamento da informação que contemplem o processamento seguro, a armazenagem, a transmissão, a reclassificação e a destruição. Convém que isto também inclua os procedimentos para a cadeia de custódia e registros de qualquer evento de segurança relevante.

Convém que acordos com outras organizações, que incluam o compartilhamento de informações, considerem procedimentos para identificar a classificação daquela informação e para interpretar os rótulos de classificação de outras organizacões.

Informações adicionais

A rotulação e o tratamento seguro da classificação da informação é um requisito-chave para os procedimentos de compartilhamento da informação. Os rótulos físicos são uma forma usual de

rotulação. Entretanto, alguns ativos de informação, como documentos em forma eletrônica, não podem ser fisicamente rotulados, sendo necessário usar um rótulo eletrônico. Por exemplo, a notificação do rótulo pode aparecer na tela ou no display.

Onde a aplicação do rótulo não for possível, outras formas de definir a classificação da informação podem ser usadas, por exemplo, por meio de procedimentos ou metadados.

Papéis e responsabilidades

Controle

Convém que papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros sejam definidos e documentados de acordo com a política de segurança da informação da organização.

Diretrizes para implementação

Convém que os papéis e responsabilidades pela segurança da informação incluam requisitos para:

a) implementar e agir de acordo com as políticas de segurança da informação da organização (ver 5.1);

b) proteger ativos contra acesso não autorizado, divulgação, modificação, destruição ou interferência;

c) executar processos ou atividades particulares de segurança da informação;

d) assegurar que a responsabilidade é atribuída à pessoa para tomada de ações;

e) relatar eventos potenciais ou reais de segurança da informação ou outros riscos de segurança para a organização.

Convém que papéis e responsabilidades de segurança da informação sejam definidos e claramente comunicados aos candidatos a cargos, durante o processo de pré-contratação.

Informações adicionais

Descrições de cargos podem ser usadas para documentar responsabilidades e papéis pela segurança da informação. Convém que papéis e responsabilidades pela segurança da informação para pessoas que não estão engajadas por meio do processo de contratação da organização, como, por exemplo, através de uma organização terceirizada, sejam claramente definidos e comunicados.

Segurança Física e Operacional

Segurança da Informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de *Segurança Informática* ou *Segurança de Computadores* está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

O suporte para as recomendações de segurança pode ser encontrado em:

- Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infra-estrutura (que garante a existência da informação)que a suporta.

Existem mecanismos de segurança que apóiam os controles físicos:

Portas / trancas / paredes / blindagem / guardas / etc ..

- Controles lógicos: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

Existem mecanismos de segurança que apóiam os controles lógicos:

- *Mecanismos de criptografia*. Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.
- *Assinatura digital*. Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade do documento associado, mas não a sua confidencialidade.
- *Mecanismos de garantia da integridade da informação*. Usando funções de "Hashing" ou de checagem, consistindo na adição.
- *Mecanismos de controle de acesso*. Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.
- *Mecanismos de certificação*. Atesta a validade de um documento.
- *Integridade*. Medida em que um serviço/informação é genuino, isto é, esta protegido contra a personificação por intrusos.

- *Honeypot*: É o nome dado a um software, cuja função é detectar ou de impedir a ação de um cracker, de um spammer, ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.

Nível de Segurança

Depois de identificado o potencial de ataque, as organizações têm que decidir o nível de segurança a estabelecer para uma rede ou sistema os recursos físicos e lógicos a necessitar de proteção. No nível de segurança devem ser quantificados os custos associados aos ataques e os associados à implementação de mecanismos de proteção para minimizar a probabilidade de ocorrência de um ataque.

Segurança física

Considera as ameaças físicas como incêndios, desabamentos, relâmpagos, alagamento, acesso indevido de pessoas, forma inadequada de tratamento e manuseamento do material.

Segurança lógica

Atenta contra ameaças ocasionadas por vírus, acessos remotos à rede, *backup* desatualizados, violação de senhas, etc.