Segurança da Informação e Comunicações - Análise ambiental de um Órgão Público: Estrutura metodológica para implementação de Controles de Segurança aplicados a ativos de informação

Domingos Savio Evandro da Silva
é servidor da Agência Nacional de Aviação Civil (ANAC) como Especialista em Regulação de Aviação Civil.

Melina Zaban
é servidora da Agência Nacional de Aviação Civil (ANAC) como Especialista em Regulação de Aviação Civil.

RESUMO

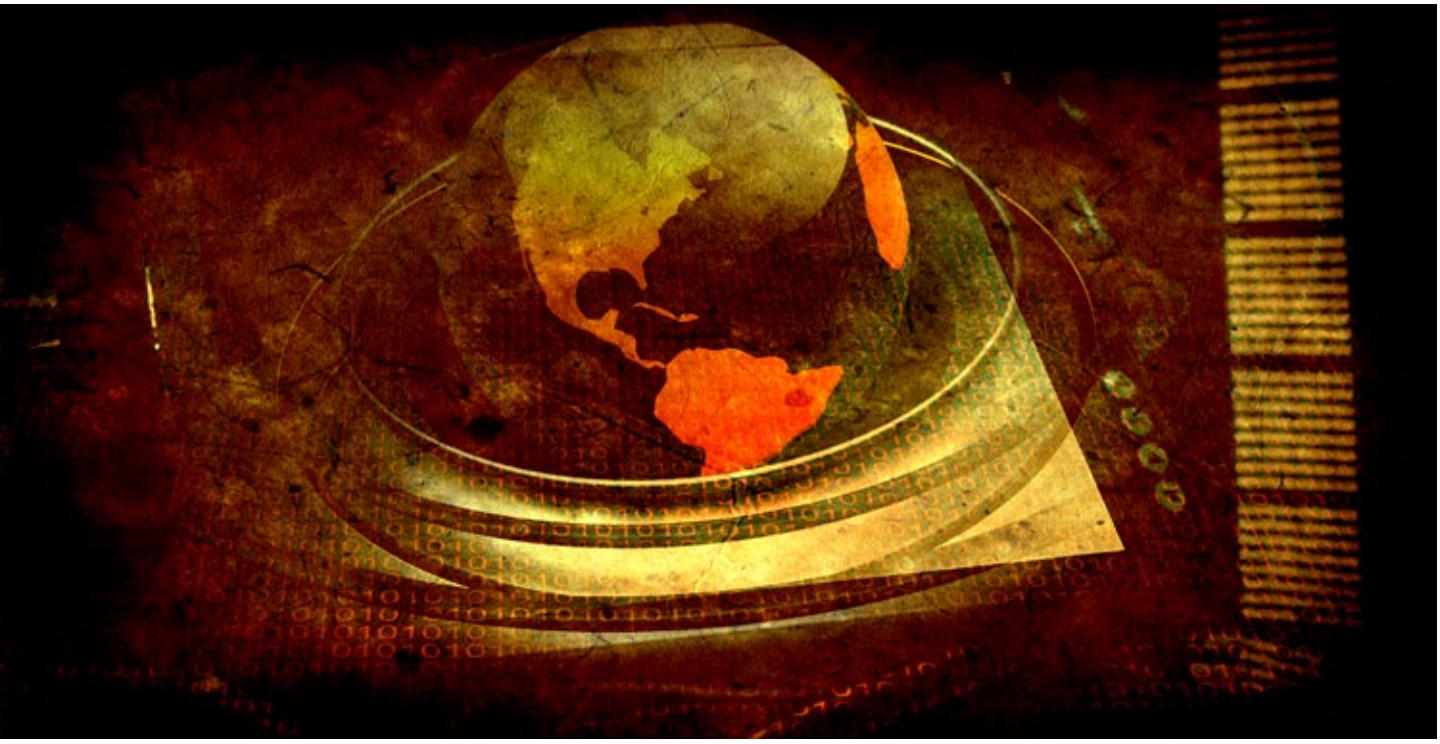
Na sociedade atual, a informação assume uma função estratégica na formulação de políticas organizacionais com vista à obtenção de resultados econômicos favoráveis, a utilização eficiente dos recursos de informação tem sido uma constante. Este artigo se propõe analisar, em uma instituição pública, alguns ativos de informação que necessitam ser protegidos contra eventuais ameaças, bem como verificar a atual estrutura de segurança ambiental dessa instituição na qual estes ativos estão inseridos, exemplificando alguns riscos e controles físicos associados que possam ser tratados por planos de contingências.

Palavras-chave: Contingência, Gestão da Informação; Segurança da Informação; Risco.

1. INTRODUÇÃO

A segurança da informação exige que as organizações implementem e mantenham uma adequada estrutura de controles físicos, de forma a garantir que os ativos de informação sejam protegidos contra as ameaças que possam danificá-los ou inutilizá-los, com risco de prejuízos por vezes imensuráveis.

Este artigo se propõe analisar a atual estrutura de segurança física e ambiental de uma determinada instituição pública e examinar, por meio de observa-



ção, alguns dos ativos de informação que necessitam ser resguardados e protegidos contra eventuais ameaças. Também apresenta alguns exemplos de riscos com uma breve análise dos seus efeitos na instituição e dos controles físicos associados.

2. ESTRUTURA ORGANIZACIONAL

A instituição analisada se refere a um típico órgão público federal, o qual é constituído por agentes públicos, servidores públicos, funcionários terceirizados e de cargos de confiança.

Na sua estrutura orgânica, além dos setores responsáveis pela gestão administrativa, financeira e patrimonial que são essenciais para o funcionamento, há também várias unidades que são responsáveis pelos diversos atendimentos ao público em geral, e que representam as atividades prioritárias para cumprimento das finalidades regimentais do órgão.

Para a realização das atividades organizacionais, são utilizados recursos financeiros subsidiados que devem ser administrados por um núcleo de controle especializado, uma vez que a execução das despesas deve ser previamente aprovada e os resultados mensurados e monitorados, gerando informações que serão utilizadas para tomada de decisões.

O tráfego de pessoas pelos recintos da organização é intenso, seja pela quantidade de serviços que são prestados ao público de determinado segmento da sociedade, seja pelos meios de acesso às instalações prediais compartilhados com outras entidades, o que aumenta a necessidade de se manter um sistema de gestão da informação e de segurança da informação e comunicações em níveis adequados.

3. RISCOS ASSOCIADOS

Com base na observação dos ativos de informação que compõem o acervo patrimonial da instituição, podem-se elencar alguns mais relevantes de forma a exemplificar as ameaças específicas envolvidas, bem como proceder à análise dos riscos e do grau de avaliação, conforme tabela 1.

Tabela 1: Avaliação dos riscos

Id.	Ativo	Ameaça específica	Vulnerabilidade	Risco - R	Probabilidade	Impacto	Nível Risco
A1	Área de atividades Arquivísticas	Acesso não autorizado	Ausência de sistema de controle de acesso	R1 - Perda de integridade da informação.	Alta	Gravíssimo	Muito alto
A2	Equipamento de informática registrador de documentos oficiais	Cópia indevida das informações armazenadas, pela empresa contratada pela instituição.	Permite que a empresa acesse a informação sem o devido controle.	R2 - Perda de confidencialidadeda informação.	Muito Alta	Grave	Muito Alto
A3	Sistema de Gestão Documental	Interrupção de conexão com o servidor.	Ausência de rotina de acionamento de redundância.	R3 - Perda de disponibilidade da informação.	Muito Baixo	Crítico	Baixo
A3	Sistema de Gestão Documental	Servidor não suportar a demanda de acessos ao sistema.	Limitação de acessos ao servidor.	R4 - Perda de disponibilidade da informação.	Média	Baixo	Baixo
A3	Sistema de Gestão Documental	Visualização não autorizada de documento.	O sistema possui apenas dois níveis de restrição de acesso a documentos, não abrangendo todos os casos.	R5 - Perda de confidencialidade	Muito Alta	Gravíssimo	Muito Alto
A4	Impressora	Obtenção, por pessoas não autorizadas, de informação armazenada na memória da impressora.	Ausência de rotinas para limpeza de memória ou descarte do dispositivo de armazenamento de informações da impressora.	R6 - Perda de confidencialidade da informação.	Muito Alta	Grave	Muito Alto
A5	Notebooks	Furto.	Armazenamento de informações críticas no notebook.	R7 - Perda de confidencialidade da informação.	Média	Gravíssimo	Muito alto
A6	Desktops	Visualização não autorizada de informações críticas ao negócio.	Sistema operacional acessível à ausência do usuário-proprietário.	R8 - Perda de confidencialidade	Alta	Crítico	Alto
A7	Documentos físicos	Visualização não autorizada de documento.	Não há mecanismos de controle de acesso a documentos físicos.	R9 - Perda de confidencialidade	Muito Alta	Gravíssimo	Muito Alto

Fonte: os autores

O quadro 1 mostra a matriz de risco, na qual é apresentada a relação da probabilidade de ocorrência de um evento com o nível de impacto nos recursos de informação ou funcionalidades dos ativos da informação.

Neste contexto, foram aplicadas as seguintes definições:

Probabilidade

Muito baixa: Muito improvável de ocorrer – (0% a 10%);
Baixa: Improvável de ocorrer – (10,1% a 30%);
Média: Ocorre ocasionalmente – (30,1% a 70%);
Alta: Provável de ocorrer – (70,1% a 90%);
Muito alta: Ocorre frequentemente – (90,1% a 100%).

Impacto

Desprezível: Os danos são insignificantes para a organização;
Baixo: A organização consegue reparar os danos com os próprios recursos;
Crítico: A recuperação dos danos exige recursos não previstos pela organização;
Grave: Danos que prejudiquem a imagem do órgão ou geram algum incidente de difícil reparação;
Gravíssimo: Dano ou perda irreparável da imagem do órgão ou da funcionalidade dos recursos.

Para um sistema de gerenciamento de informações devem ser estabelecidos adequados processos de

Quadro 1: Nível de risco

		Probabilidade				
		Muito Baixa	Baixa	Média	Alta	Muito Alta
Impacto	Gravíssimo	Risco Alto	Risco Alto	Risco Muito Alto	Risco Muito Alto	Risco Muito Alto
	Grave	Risco Médio	Risco Médio	Risco Alto	Risco Alto	Risco Muito Alto
	Crítico	Risco Baixo	Risco Médio	Risco Médio	Risco Alto	Risco Alto
	Baixo	Risco Muito Baixo	Risco Baixo	Risco Baixo	Risco Médio	Risco Médio
	Desprezível	Risco Muito Baixo	Risco Muito Baixo	Risco Muito Baixo	Risco Muito Baixo	Risco Muito Baixo

Quadro 2:
Definição de prioridades

		Eficácia das Ações de controle				
		Forte	Satisfatória	Insatisfatória	Fraca	Inexistente
Ranking do Risco	Risco Muito Alto	Prioridade Alta	Prioridade Alta	Prioridade Muito Alta	Prioridade Muito Alta	Prioridade Muito Alta
	Risco Alto	Prioridade Média	Prioridade Média	Prioridade Alta	Prioridade Alta	Prioridade Muito Alta
	Risco Médio	Prioridade Baixa	Prioridade Média	Prioridade Média	Prioridade Alta	Prioridade Alta
	Risco Baixo	Prioridade Muito Baixa	Prioridade Baixa	Prioridade Baixa	Prioridade Média	Prioridade Média
	Risco Muito Baixo	Prioridade Muito Baixa	Prioridade Muito Baixa	Prioridade Muito Baixa	Prioridade Muito Baixa	Prioridade Muito Baixa

identificação e controle dos riscos nos quais "são identificados os riscos, que se dá por meio do levantamento das ameaças e vulnerabilidades que os documentos estão suscetíveis e o impacto resultante caso uma ameaça explore alguma vulnerabilidade". (PORTELA, T.N.O; SILVA, N.P. 2011).

Assim devem ser implementadas algumas ações e controles de segurança capazes de mitigar ou eliminar o risco, seguindo uma ordem de prioridade.

Segundo PORTELA *et* SILVA (2011), o tratamento dos riscos deve ser iniciado pelo risco que tem a maior probabilidade de acontecer e que cause impacto relevante ao negócio.

No quadro 2, apresenta-se uma definição da escala de prioridades que auxiliam na implementação de ações, possibilitando eficiência na alocação de recursos para a organização.

4. PLANO DE AÇÕES

A seleção de controles de segurança da informação, tal como descrito na ISO/IEC 27002 (ABNT, 2005) depende das decisões da organização, baseada nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização e convém que também esteja sujeito a todas as legislações e regulamentações nacionais e internacionais relevantes. (SILVA, E.M. 2011a).

Ainda, segundo SILVA (2011a) estes controles não devem ser independentes, é preciso que façam parte da Política de Segurança da Informação e Comunicações - PoSIC para que possam obedecer às regras de acesso e ao provimento dos dispositivos de acompanhamento e monitoria.

4.1 PLANO DE ADMINISTRAÇÃO DE CRISE - PAC

Dentro da política de segurança, devem ser definidos planos organizacionais para fazer frente a eventuais incidentes, tal qual o Plano de Administração de Crises - PAC, que define detalhadamente o funcionamento das equipes antes, durante e depois da ocorrência do incidente. Tem como objetivo definir os procedimentos a serem executados até o retorno normal das atividades. (SILVA, E.M. 2011).

4.2 PLANO DE RECUPERAÇÃO DE DESASTRES - PRD

Todas as entidades estão sujeitas à perda de ativos de informações pelas vulnerabilidades inerentes aos próprios negócios que podem ser aproveitados pelas ameaças externas e internas. Portanto, "faz-se necessário garantir a continuidade de processos e informações importantes da empresa, no menor espaço de tempo possível, evitando ou minimizando os impactos de um incidente". (OLIVEIRA et SILVA SAVIO, 2011).

Neste contexto, tem-se o PRD que abrange a recuperação e restauração das funcionalidades dos ativos humanos, operacionais, tecnológicos e que suportam o negócio. Tem como objetivo restabelecer o ambiente às condições originais de operação.

Na tabela 2, apresenta-se um esboço das ações a serem executadas como parte integrante do PAC, considerando o risco associado aos ativos de informação, conforme descrito na tabela 1.

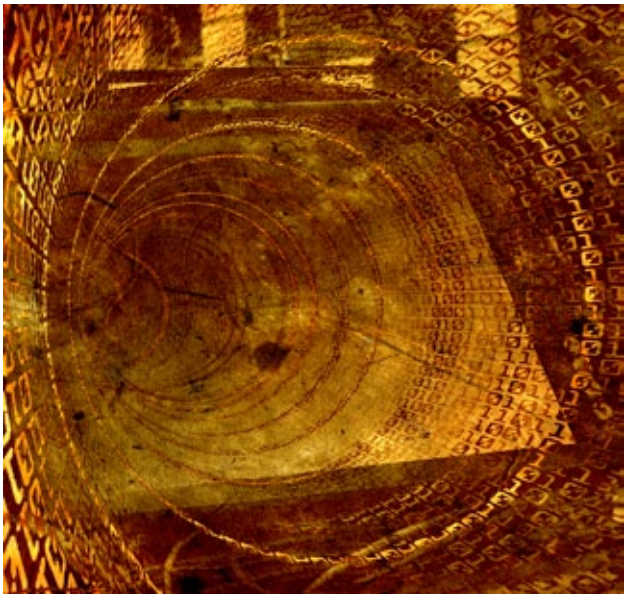


Tabela 2:
Modelo de PAC

Plano de Administração de Crises		
Id.	**Ativo**	**Ações**
R1	A1	1) Acionar a equipe de segurança predial. 2) Verificar se houve dano ao arquivo, acesso às informações confidenciais e alteração de dados arquivados. 3) Informar sobre o incidente e a previsão de reestabelecimento do serviço ao nível hierárquico adequado.
R2	A2	1) Consultar registro de identificação de pessoas que tiveram acesso à sala do equipamento. 2) Verificar registros de acesso lógico e integridade dos dados. 3) Informar sobre o incidente ao nível hierárquico adequado, solicitando abertura de sindicância.
R3	A3	1) Contatar a equipe de suporte de informática. 2) Solicitar a acionamento do sistema para centro de processamento reserva. 3) Verificar o prazo de atendimento no contrato do respectivo fornecedor. 4) Informar sobre o incidente e a previsão de reestabelecimento do serviço ao nível hierárquico adequado.
R4	A3	1) Contatar a equipe de suporte de informática. 2) Solicitar liberação temporária de maior número de acessos simultâneos ao servidor. 3) Verificar o prazo de atendimento. 4) Informar sobre o incidente e a previsão de reestabelecimento do serviço ao nível hierárquico adequado.
R5	A3	1) Identificar informações violadas. 2) Identificar documentos relacionados à informação. 3) Verificar registros de acesso aos documentos violados. 4) Informar sobre o incidente ao nível hierárquico adequado, solicitando abertura de sindicância.
R6	A4	1) Verificar quais as impressoras estão sendo descartadas. 2) Suspender o processo de descarte das impressoras. 3) Informar sobre o incidente ao nível hierárquico adequado, solicitando abertura de sindicância.
R7	A5	1) Verificar se o notebook furtado possuía algum sistema de bloqueio às informações à distância ou de rastreamento. 2) Verificar onde ocorreu o furto, acionando a equipe de segurança predial caso o furto tenha se dado nas dependências da organização. 3) Informar sobre o incidente ao nível hierárquico adequado, solicitando abertura de sindicância e de registro de ocorrência policial.
R8	A6	1) Verificar quais informações críticas estavam disponíveis e acessíveis. 2) Verificar se houve alteração na integridade e permissões de acesso das informações. 3) Informar a equipe de suporte de informática para efetuar procedimentos de segurança adequados. 4) Informar sobre o incidente ao nível hierárquico adequado e às áreas envolvidas sobre o comprometimento de tais informações.
R9	A7	1) Identificar informações violadas. 2) Identificar documentos relacionados à informação. 3) Informar sobre o incidente ao nível hierárquico adequado, solicitando abertura de sindicância.

Fonte: os autores

5. SEGURANÇA ORGÂNICA

Considerando os padrões sugeridos pela ISO/IEC 27.002/2005 é possível efetuar uma análise das variáveis que compõem o conjunto de requisitos referente aos controles físicos necessários a uma adequada gestão da Segurança da informação e Comunicações aplicadas ao ambiente organizacional.

Para o controle dos ativos de informação identificados, foran sugeridas a criação e a implementação de controles de acesso físico. Desta forma, as áreas classificadas como sensíveis devem ser protegidas por controles de entrada apropriados, para garantir que apenas o pessoal autorizado tenha acesso a elas, devendo ser considerado que:

a. Visitantes nas áreas de segurança devem ser supervisionados ou conduzidos pela segurança e as datas e horários de sua entrada e saída devem ser registrados.
b. O acesso a informações sensíveis deve ser controlado e restringido apenas ao pessoal autorizado. Controles de autenticação com sistema de identificação, como cartões magnéticos, devem ser usados para autorizar e validar todos os acessos.
c. Todo o pessoal deve ser obrigado a usar alguma forma visível de identificação e deve ser encorajado a questionar estranhos desacompanhados e qualquer um que não esteja usando identificação visível.
d. Os materiais recebidos devem ser inspecionados quanto a possíveis perigos antes de serem transferidos do depósito para o local de uso.

Da mesma forma foi sugerida a implementação de uma política de treinamento, uma vez que a coopera-

Tabela 3:
Controles de segurança e compatibilidade com os ativos de informação identificados

Controle ISO/IEC	Controle existente ou sugerido	Ativo
7.1.2	É necessário implementar controle de acesso físico de forma que contemple os controles sugeridos pela norma ABNT 27002. Há controle de acesso por meio de catraca, do edifício, e recepcionistas nas portarias. Não há nenhuma restrição de trânsito interno, ainda que os setores possuam portas e restrição de horário de expediente definido.	A1 e A7
7.1.5	O acesso a uma área de entrega e carregamento a partir do exterior do prédio deve ficar restrito ao pessoal identificado e autorizado. Necessidade de as portas externas de uma área de entrega e carregamento serem protegidas enquanto as portas internas estiverem abertas.	Todos
7.2.4	Periodicamente é realizada a manutenção preventiva dos equipamentos (notebooks, computadores e impressoras). Faz-se necessário elaborar e implementar um processo de gestão de capacidade, o monitoramento dos recursos e sistemas é feito de forma informal e não periódica.	A2 a A6
7.2.6	É necessária a elaboração de norma para Segurança Orgânica (Física e Ambiental) que contemple a seção 9.2.6 - Reutilização e alienação segura de equipamentos (ABNT 27002), para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.	A2 a A6
7.3.1	Faz-se necessário uma política de treinamento para sensibilização e conscientização de assuntos relacionados à Segurança da Informação e Comunicações e cuidados que devem ser tomados pelos usuários.	Todos

Fonte: os autores adaptado de ISO/IEC 27002/2005

ção dos usuários autorizados é essencial para a eficácia da segurança, pois todos devem ser conscientizados de suas responsabilidades quanto à manutenção de controles eficazes de acesso, particularmente ao uso de senhas e à segurança do equipamento.

6. CONCLUSÃO

Com base na observação dos ativos de informação que compõem o acervo patrimonial da instituição, pôde-se verificar a relevância da utilização de normas e metodologias para implementar uma estrutura de segurança que contemple, entre outros aspectos, o inventário dos Ativos de informação e a análise dos riscos associados.

Após a verificação da conformidade dos ativos com os controles físicos existentes, procedeu-se à priorização das ações de segurança de acordo com o nível de risco avaliado, o que auxilia na gestão dos recursos que devem ser alocados nestas ações.

Com estes procedimentos, foi apresentado um modelo de Plano de Administração de Crises - PAC, com detalhamento das ações que devem ser seguidas em caso de ocorrência de algum incidente, incluindo o funcionamento das equipes antes, durante e depois dessa ocorrência.

Com esse instrumento, torna-se possível elaborar o Plano de Recuperação de Desastres - PRD, com o intuito de abranger a recuperação e restauração das funcionalidades dos ativos elencados anteriormente, uma vez que este plano objetiva restabelecer o ambiente às condições originais de operação.

Por fim, verificou-se que os controles de segurança física a serem aperfeiçoados devem levar em consideração as características definidas na ISO/IEC 27.002/2005, com vista a fornecer razoável garantia de que o ambiente esteja protegido contra as ameaças existentes, o que propiciará à instituição estudada uma melhor gestão dos recursos de informação.