Estudo de Caso de Segurança da Informação

Extrato de Entrevista realizada na Empresa *ACME corporation*.

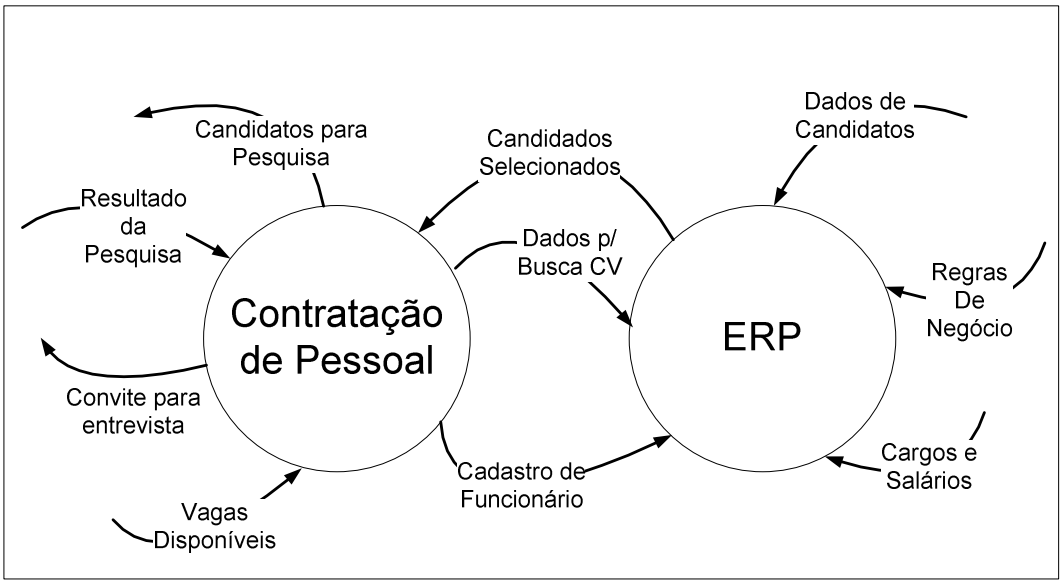
Entre os Processos de Negócio`(PN), dois foram evidenciados como de risco relevante:

A. Contratação de Pessoal - A empresa mantém um cadastro permanente de CV pela internet. Uma *Intranet* atende a todos os setores da empresa, através de uma rede local. Havendo vagas disponíveis, os CV são pesquisados através de uma transação disponível no ERP da empresa, que seleciona os CV em ordem priorizada através de inteligência artificial. Os CV selecionados tem os dados pessoais do candidato pesquisados por outra empresa, que investigará e atestará a idoneidade do candidato para a vaga. A solicitação desta pesquisa é feita por email, com requisito de sigilo. O candidato então é convidado por telefone para uma entrevista com o gestor do PN. Tendo sido aprovado para a vaga, o mesmo é cadastrado pelo gestor no ERP, para que outros PN possam usá-lo em outras transações já como funcionário da empresa. O gestor declara que a sua função é muito importante, mas permite uma tolerância de até 20 dias de paralisação, intervalo máximo típico de suas férias. No entanto, ressalta que a investigação feita pela empresa é altamente sigilosa, e os dados pessoais descobertos sobre os candidatos devem ser preservados e disponibilizados apenas para alguns usuários específicos, como o Diretor de RH. Relatórios impressos da pesquisa sobre os candidatos, por exemplo, devem ser mantidos em cofre e triturados após sua utilidade. A informação, no entanto, é mantida criptografada no banco de dados. O gestor declarou que, apesar da alta confidencialidade dos dados, o pessoal do setor não possui cultura de Segurança da Informação, temendo um incidente que possa comprometer a imagem da empresa, apesar de jamais ter tido conhecimento da ocorrência de algum.

B. ERP - O gestor do ERP da empresa é um profissional do setor de TI, que o administra. Como todo ERP, tem uma alta capilaridade, atendendo a quase todos os setores. No que diz respeito a esta análise, o setor executivo insere valores no Plano de Cargos e Salários, usados nas contratações e promoções. O ERP possui um módulo de Inteligência Artificial que infere competências a partir de dados inseridos pelos candidatos em uma interface disponível pela Internet. O gestor é auxiliado por técnicos que customizam o ERP de acordo com as regras de negócio informadas pelo setor executivo da empresa. Devido a sua importância para a sobrevivência da empresa, as metas do setor apontam para uma tolerância à paralisação máxima de 2 horas, a partir do que passam a ser observados prejuízos no faturamento. A base de dados do ERP é administrada em outro PN, pelo DBA. O gestor declarou que há grande instabilidade no fornecimento de energia, sendo constantes as entradas em operação do *No-break*. É também preocupado com a constante presença de fornecedores de produtos e serviços de TI, ao setor, apesar de nunca ter percebido a ocorrência de algum evento de segurança relevante.

Passos na elaboração do PDS:

1. Mapeamento dos PN (baseado exclusivamente no texto)



O mais importante desta fase é observar o foco exclusivo na informação que entra e que sai de cada PN.

2. Elenco de ativos descritos

	PN A	**PN B**
Físicos	Salas, Mobiliário, infra-estrutura de dados e voz, cofre	Salas, Mobiliário, infra-estrutura de dados e voz
Tecnológicos	XXX	ERP (sistema)
Físico-tecnológicos	Computadores, equipamentos de conectividade locais	Computadores, equipamentos de conectividade locais
Humanos	Gestor	Gestor, técnicos

A identificação do tipo de ativo é de grande importância. Um ativo físico-tecnológico, por exemplo, é um ativo que pode sofrer impactos causados por ameaças de natureza física, mas também de natureza tecnológica.

3. Correlação de ativos com ciclo de vida

Ativo		Fase Ciclo	Info
PN A	Salas, mobiliário	Armazenamento	Todas (em forma visível ou audível)
	Cofre	Armazenamento	Resultado da Pesquisa (impressa)
	Infra-estrutura de dados, equipamentos de conectividade locais	Transporte	Todas, exceto o convite para entrevista
	Infra-estrutura de voz	Transporte	Convite para entrevista
	Computadores	Armazenamento	Todas, exceto o convite para entrevista
	Gestor	Manipulação	Todas
	Gestor	Descarte	Qualquer Info impressa referente ao candidato
PNB	Salas, mobiliário	Armazenamento	Todas (em forma visível ou audível)
	Infra-estrutura de dados, equipamentos de conectividade locais	Transporte	Todas
	ERP, Computadores	Armazenamento	Todas
	ERP	Manipulação	Candidatos Selecionados
	Gestor, técnicos	Manipulação	Todas

Essa associação também é de grande importância, por permitir a evidenciação da necessidade de controles diferentes, de acordo com a fase do ciclo de vida. Um ativo que manipula a informação, por exemplo, precisará de um estudo detalhado de controle de acesso, de forma que apenas a manipulação (edição, leitura, deleção) estritamente necessária seja possível.

4. Identificação de ameaças x vulnerabilidades visíveis

Ameaça		Vulnerabilidade
PNA	Candidato com dados expostos (processo judicial)	Funcionário do setor (Tratamento inadequado da informação sigilosa)
	Qualquer	Gestor de PN sem cultura de segurança
PNB	Pane elétrica	Empresa fornecedora de energia de baixa qualidade
	Sabotador	Acesso fácil de estranhos
	Técnico mal-intencionado	Customização do sistema
	Qualquer	Gestor de PN sem cultura de Segurança

Esta observação, ainda superficial e baseada apenas na perspectiva limitada dos respectivos gestores, já aponta algumas ameaças mais evidentes. Mais adiante, com a Análise de Riscos, outras ameaças serão descobertas.

5. CIDAL

Tabela de significado semântico dos índices:

Índice	Nível	Enquadramento
1	**Não Considerável**	A ocorrência de um incidente de segurança (IS) neste PN é absorvida integralmente através de um Plano de Continuidade de baixo custo sem prejuízo algum à atividade produtiva
2	**Relevante**	A ocorrência de um IS no PN em análise demanda ações reativas programadas perceptíveis em outros PN, podendo causar impactos de baixa monta, como pequenos atrasos ou prejuízos financeiros absorvíveis, porém indesejados
3	**Importante**	Um IS no PN em avaliação provoca a redução imediata de sua operacionalidade normal, causando prejuízos diários. Demanda ações reativas emergenciais para que a extensão de seus impactos não afetem outros PN da empresa e metas da empresa
4	**Crítico**	Os impactos de um IS podem ser percebidos em vários PN associados, demandando iniciativas reativas não previstas anteriormente, causando a necessidade de esforços adicionais e redução da capacidade produtiva de toda ou grande parte da empresa. Compromete metas. A ausência ou demora na reação pode transformar o evento em vital.
5	**Vital**	A ocorrência de um IS deste tipo no PN em análise pode atingir toda a empresa e seus parceiros, causando impactos irreversíveis e demandando ações emergenciais que envolvem desde o setor estratégico até o operacional. Se persistente, pode provocar a falência da empresa

Análise CIDAL com justificativas:

PN A	C	I	D	A	L
1			X		
2		X		X	
3	X				X
4					
5					

PN B	C	I	D	A	L
1					
2					X
3					
4	X			X	
5		X	X		

No PN A, a CONFIDENCIALIDADE e a LEGALIDADE são IMPORTANTES, considerando-se como evento mais sensível o comprometimento do relatório de investigação de um candidato. Tal evento poderia gerar processos judiciais desagradáveis para a empresa. A INTEGRIDADE e a AUTENTICIDADE são avaliadas como RELEVANTES, tomando como parâmetro a possibilidade da obtenção de relatórios forjados abonando a contratação de funcionários inidôneos. A DISPONIBILIDADE é NÃO CONSIDERÁVEL, já que o processo tem grande tolerância temporal, permitindo a construção de soluções alternativas.

No PN B, a CONFIDENCIALIDADE e AUTENTICIDADE, são CRÍTICAS, uma vez que o sistema armazena todas as informações estratégicas da empresa, inclusive os dados sigilosos dos funcionários citados no PN A. Um incidente como o vazamento do arquivo de informações sigilosas referentes aos funcionários pode gerar reações em toda a empresa, com grandes e desagradáveis efeitos. A INTEGRIDADE e a DISPONIBILIDADE são VITAIS, já que se trata de um ERP, onde toda a informação necessária para operação da empresa está armazenada. Dados incorretos ou

indisponíveis podem conduzir à não-concretização de negócios ou decisões incorretas, que persistentes podem comprometer a saúde financeira da empresa. A LEGALIDADE é RELEVANTE, imaginando-se a necessidade de observar aspectos legais para a implementação das regras de negócio sem ferir a legislação vigente e aspectos éticos que possam trazer prejuízos à empresa.

Conclusão: PN A - média 2,2 (PN Relevante); PN B - média 4 (PN Crítico)

6. GUT

Tabela para o significado semântico dos índices:

	Gravidade (CIDAL)	Urgência	Tendência
1	Entre 1 - 2,3	Tolerância acima 120h	Não há menção no PN[1]
2	Entre 2,4 - 3,7	Tolerância entre 24 e 120h	Possibilidade de agrava-mento prevista no PN
3	Entre 3,8 - 5	Tolerância inferior 24h	Previsão de incremento previsto no PN

Análise GUT

	Gravidade	Urgência	Tendência	Total
PN1	**1**	**1**	**1**	**1**
PN2	**3**	**3**	**1**	**9**

Prioridade entre os processos: PN2, mais prioritário que o PN1, o que significa que o PN2 é mais sensível, com maior nível de risco que o PN1.

7. BIA

BIA – *Business Impact Analisys*

	Candidato	Sabotador	Pane Elétrica	Técnico	Tolerância
PN2		X	X	X	2 horas
PN1	X				20 dias

O BIA permite a escolha da melhor estratégia para cada PN, iniciando-se sempre pelo mais crítico (de maior risco)

[1] Plano de Negócios - deve sempre ser solicitado e analisado, para captura de informações relevantes para a compreensão da dinâmica da empresa

8. PLCONT

Escolhendo a ameaça "Pane Elétrica" para o PN2

Contingenciando o ativo ERP em caso de Pane Elétrica:

Em função da importância do ativo ERP para a empresa, é razoável a implementação de uma estratégia de contingência do tipo "warm-site", já que a tolerância admissível é de 2 horas. Neste cenário, são implementados os seguintes **controles** para redução do nível de risco:

a) Um sistema de *no-break* de boa qualidade, com plano de manutenção permanente através de contrato com empresa especializada, com capacidade de atender a toda a configuração necessária para operação da parcela "servidor" do ERP;
b) Definição de Estações de Trabalho críticas, que devem ser protegidas através de sistema *no-break* próprio, igualmente mantidos em condições plenas através de contrato de manutenção;
c) Definição de equipamentos de conectividade críticos para a operação do ERP, através das Estações de Trabalho críticas; e
d) É firmado um contrato com uma empresa especializada em geração de energia, com um SLA que garanta atendimento em intervalo de tempo compatível com a autonomia do sistema de *no-break*. Define-se um local adequado para a operação de geradores deste tipo e marca-se o local, para que nunca fique obstruído permanentemente.

Este Plano de Contingência, que junto com os demais comporá o Plano de continuidade dos negócios da empresa, deve ser organizado em três planos:

Plano de Administração da Crise (PAC) – Ao ocorrer uma pane elétrica, os recursos de controle entrarão em ação automaticamente. No entanto, por tratar-se de uma situação indesejada, que reduz a capacidade operacional da empresa, ações contingenciais são necessárias. No que diz respeito ao PAC, são ações cabíveis:

O responsável pela administração desta contingência é o Gestor de TI. Na sua ausência, o funcionário hierarquicamente mais graduado deve assumir as ações deste plano. O gestor de TI da empresa (ou o seu substituto), verifica a característica da interrupção (extensão da interrupção, possíveis razões internas e externas), registra a ocorrência (horário e dados verificados) e determina a um funcionário do setor de TI que comunique ao Diretor de Operações a ocorrência. O gestor de TI verifica a desobstrução do local onde os geradores de emergência contratados eventualmente ficarão operando;

O Plano de Continuidade Operacional (PCO) – Deve focar na tolerância do PN. Para garantia de continuidade do ERP, primeiramente o Gestor de TI deve acionar a empresa conveniada de fornecimento de geradores e colocá-la de sobreaviso para o atendimento da ocorrência em questão. Entra em contato com a empresa de fornecimento de energia e busca informações sobre uma estimativa de retorno. Caso não haja previsão, solicita à empresa de geradores que mande os equipamentos. Caso contrário, aguarda até uma hora de interrupção antes de solicitar os geradores.

Tão logo os geradores cheguem à empresa, o Gestor de TI recebe os técnicos, orienta quanto ao local de instalação, determina seu acionamento imediato e coordena a manobra de entrada em operação do mesmo, até que substitua os no-break da estrutura de contingência;

O Plano de Recuperação de Desastres (PRD) – Tem uma importância fundamental no Plano de Contingências, porque visa a avaliação da eficiência e a eficácia dos controles, de forma a evitar que novas ocorrências reduzam a capacidade operacional do recurso contingenciado. Assim, são eventos importantes no PRD em questão – análise dos parâmetros da ocorrência: tempo de paralisação, razões evidenciadas, e, principalmente, estimativa de prejuízos com a paralisação. Avaliação preliminar do SLA. Encaminhamento para o setor jurídico, visando o ressarcimento dos prejuízos. Na próxima reunião com o comitê Gestor de Segurança da Informação, discutir a viabilidade da reavaliação da autonomia do sistema de no-break de cada um dos componentes, um SLA mais rigoroso com a operadora e um contrato diferenciado com a empresa dos geradores. O objetivo sempre é a manutenção do nível de risco sob controle.

9. PolSeg

Uma Política de Segurança deve ser construída rigorosamente de acordo com este trabalho, de forma a ser um instrumento eficaz, capaz de ser testada, divulgada amplamente através de programas de conscientização e modularizada de acordo com o público-alvo. É dividida em documentos de orientação geral, emitidos pela alta administração. Estas orientações, chamadas de DIRETRIZES, são particularizadas de acordo com os segmentos do setor tático (gerencial), sendo chamadas de NORMAS. Cada norma deve possuir detalhamentos suficientes para uso cotidiano e direto pelos executores das ações operacionais, sendo então denominadas de PROCEDIMENTOS e INSTRUÇÕES. Como exemplos de uma PolSeg da empresa em discussão, pode-se citar:

Durante as entrevistas, foram evidenciadas algumas vulnerabilidades que podem ser minimizadas. Por exemplo, a presença de elementos estranhos à empresa nos setores. Não é interessante apenas uma ordem para a segurança bloquear acessos indevidos, e sim uma política que faça com que TODOS compreendam a importância de preservar as informações corporativas do mundo exterior. Com este objetivo, pode-se propor:

DIRETRIZ – Por ser um recurso de grande importância para a organização, a confidencialidade das informações deve ser preservada de acordo com o seu controle de acesso e seu sigilo..

NORMA – Cada setor deve ter definido o seu controle de acesso, seus perímetros de segurança e regras específicas para acesso (ou não) de público externo. No caso específico do setor de Gestão do ERP, podemos definir: O acesso de elementos estranhos à empresa apenas deverá ser feito nas seguintes condições:

a) Divulgação de produtos e serviços – apenas as quartas e sextas, das 14h às 15hs, mediante agendamento com o Gestor do PN;

b) Manutenção de equipamentos, infra-estrutura e aplicativos – mediante cadastramento e acompanhamento permanente de um funcionário do setor, em data e horário previamente acertado com o Gestor; e
c) Visita de parentes de funcionários ao setor – vedadas.

PROCEDIMENTOS – Para a realização de manutenções no setor, a empresa prestadora deverá enviar os dados dos funcionários previamente (RG, função, tarefa a cumprir). Os dados serão verificados na chegada do prestador de serviços, que será orientado a não circular em nenhum momento pela empresa desacompanhado. Receberá um crachá RFID com permissão de acesso apenas aos setores rigorosamente necessários e aos banheiros. Será notificado que a empresa é monitorada por câmeras e alarmes de acesso a áreas restritas. Será informado que isto ocorrendo, ele será obrigado a retirar-se e a empresa será notificada de seu procedimento. Um colaborador da empresa será indicado pelo gestor para acompanhar o prestador de serviço durante toda a sua permanência na empresa. Após a realização do serviço, o prestador será acompanhado até a portaria pelo colaborador responsável. O registro de sua presença será mantido para eventuais perícias futuras.

10. Análise de Risco

Após a elaboração da primeira versão da Política de Segurança, onde os controles necessários evidenciados são descritos e implementados, dentro da disponibilidade financeira alocada pela empresa, parte-se para a etapa de análise de risco. Nesta etapa, são testadas objetivamente as vulnerabilidades da empresa, através da simulação da ação de ameaças. Pode-se planejar o seguinte:

a) **Auditoria de Conformidade** – Os controles previstos na política de segurança são testados, através de entrevistas verificando se os gestores estão capacitados para a condução dos procedimentos previstos, bem como se conhecem as normas pertinentes aos seus setores e as diretrizes do setor executivo. Os documentos de controle são verificados (planilhas de exercícios de capacitação, históricos de entrada em operação dos PLCONT, registros de incidentes de segurança, registros de testes com os Planos de Contingência, etc.), e todas as discrepâncias são registradas;
b) **Auditoria de Rigidez Física** – São feitas verificações da rigidez dos controles de acesso, da infra-estrutura, dos perímetros de segurança, dos controles de manutenção de hardware (inventários, MTBF, manutenção preventiva), SLAs de prestadoras, contratos de manutenção em vigor, verificação de *gaps* para descrição em relatório;
c) **Auditoria de Rigidez Lógica** – Os Sistemas Operacionais em uso são testados com relação à sua atualização (inclusive os de equipamentos de conectividade). As aplicações são verificadas quanto a vulnerabilidades conhecidas e aleatórias, como por exemplo no transporte de informações sigilosas de forma não criptográfica. Os controles lógicos (Firewall, IDS, antivírus corporativos) são testados e verificados com ferramentas especialistas de ataque; e
d) **Auditoria de Capacitação** – São usadas técnicas de Engenharia Social para verificar o nível de mentalidade de segurança entre os colaboradores da empresa; são evidenciadas as principais deficiências de forma

genérica, sem apontar nomes, para sugestão de estratégias na capacitação do pessoal.

Com as conclusões deste trabalho, os controles podem ser revistos pontualmente e a Política de Segurança atualizada. Algo importante a ressaltar é a necessidade permanente de divulgação, conscientização, treinamento e, principalmente, a criação de um ambiente sinérgico na empresa capaz de manter o nível de risco sob controle.