FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Bruno César Aparecido da Silva

A SEGURANÇA DA INFORMAÇÃO EM UNIDADES PRISIONAIS

Americana, S. P.

2013

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Bruno César Aparecido da Silva

A SEGURANÇA DA INFORMAÇÃO EM UNIDADES PRISIONAIS

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do Profº Me. Alexandre Garcia Aguado.
Área temática: Segurança da informação.

Americana, S. P.

2013

Bruno César Aparecido da Silva

A SEGURANÇA DA INFORMAÇÃO EM UNIDADES PRISIONAIS

Trabalho de Conclusão de Curso apresentado à FATEC de Americana como parte dos requisitos para obtenção do título de Tecnólogo em Segurança da Informação.

Americana, 06 de dezembro de 2013.

Banca Examinadora:

_____
Alexandre Garcia Aguado
Mestre em Tecnologia e Inovação
FATEC de Americana

_____
Edson Roberto Gaseta
Especialista
FATEC de Americana

_____
Leandro Halle Najm
Mestre
FATEC de Americana

RESUMO

O crescimento do uso da tecnologia contribui para aumentar o fluxo de informações digitais. De modo similar surgiu a necessidade de armazenar os dados eletronicamente, para facilitar e agilizar o acesso às informações. Entretanto, aumentou-se a vulnerabilidade e os riscos à segurança das informações das organizações. A segurança da informação no ambiente prisional abrange todas as informações carcerárias, que são dados importantes e como qualquer outro ativo, necessitam de uma proteção adequada e que atenda as necessidades da organização. Este trabalho busca identificar os riscos da segurança da informação em um ambiente prisional, propondo também, melhorias através de normas, diretrizes e procedimentos, almejando garantir a integridade, a disponibilidade e a confidencialidade das informações prisionais. Para compreender melhor os aspectos do trabalho, realizou-se um estudo de caso, que identifica as principais ameaças à segurança da informação, reforçando a abundante fragilidade das informações carcerárias.

Palavras-chave: Segurança da informação; informação prisional; prisão.

ABSTRACT

The growing use of technology helps to increase the flow of digital information. Similarly there was a need to store data electronically for fast and easy access to information. However, it increases the vulnerability and risks to information security organizations. The information security is to protect information and seeks to ensure the integrity, availability and confidentiality of this information. The prisional informations are very important data and like any other asset, require adequate protection and meet the needs of the organization. This course work seeks to identify and minimize the risk of information security in a prison environment, through standards, guidelines and procedures, aiming to ensure the integrity, availability and confidentiality of prisional informations. To better understanding of the purpose of this study, we performed a case study that seeks to identify the main threats to information security, reinforcing the fragility of abundant information of incarceration. The result of the case study analysis, results in a better method to mitigate such problems.

Keywords : Information security , prisional information , prison.

AGRADECIMENTOS

Agradeço a Deus, pela saúde, pela determinação e pela sabedoria a mim confiada.

Aos meus pais Vanderlei (in memoriam) e Cleusa, pela dedicação, preocupação e por sempre me incentivarem a buscar o conhecimento.

À minha esposa Bárbara pela paciência e compreensão nos dias em que concentrei toda minha atenção neste trabalho, não podendo demonstrar o quanto ela é especial para mim.

Aos meus colegas de classe, em especial os meus amigos Guilherme Bakhos, Gabriel Sanpey Mochizuki e Kátia Lois Somensari Cardoso, por sempre estarem ao meu lado desenvolvendo trabalhos acadêmicos, compartilhando seus conhecimentos e por participarem da minha fase de graduação.

Ao orientador deste trabalho, o profº Me. Alexandre Garcia Aguado, por dividir sua experiência e conhecimento. Embora tenha me dedicado, sem sua ajuda este trabalho não obteria êxito.

DEDICATÓRIA

À minha esposa Bárbara, por ser atenciosa e me ensinar a nunca desistir de buscar meus objetivos.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

SAP: Secretária de Administração Penitenciaria

PRODESP: Processamento de dados do Estado de São Paulo

ISO: *International Organization for Standartization* (Organização internacional para padronização)

IEC: *International Eletrotechnical Commission* (Comissão Eletrotécnica Internacional)

NBR: Norma Brasileira (Estabelecida pela Associação Brasileira de Normas Técnicas)

RIP: Regimento Interno Padrão

VPN: *Virtual Private Network* (Rede virtual privada)

SUMÁRIO

1 INTRODUÇÃO

A utilização da informática é cada vez mais frequente em unidades prisionais, e tem como principais objetivos o armazenamento, manuseio e troca de informações carcerárias, tais como, fichas qualificativas de internos, cadastro pessoal de funcionários, informações de transferências e apresentações judiciais, além de informações administrativas.

Um dos principais benefícios da informação digital é a agilidade de processamento das informações pertinentes aos trabalhos carcerários, de modo a facilitar a tomada de decisão em situações habituais ou de crise.

Porém, as soluções tecnológicas e de telecomunicações empregadas para a utilização nos sistemas que se valem da informação digital, são complexas e podem trazer riscos de segurança à confidencialidade, à integridade e disponibilidade das informações, podendo expor em situações de risco os internos, os funcionários e/ou a organização.

Devido ao grande fluxo de informações internas e externas, públicas ou confidenciais manuseadas diariamente numa unidade prisional, através de malotes, E-mail, remessas, telefonemas, ou mesmo em anotações e impressões, nota-se que a informação, dentre outros ativos, é de extrema importância para a unidade prisional e necessita de segurança.

Outro fator que pode fragilizar a informação em uma unidade prisional é o mau uso da informação, facilitando seu extravio e seu acesso indevido, principalmente nos sistemas que utilizam sistemas de computadores, pois tornam esses dados vulneráveis a acessos não autorizados. A facilidade de alteração e acesso de dados registrados eletronicamente traz perigos adicionais à vida de detentos e/ou funcionários, como por exemplo, a descoberta de horários de transferências de detentos, que podem acarretar tentativas de fuga e resgate de presos.

A informação carcerária, assim como qualquer outro ativo da unidade, necessita de uma segurança adequada, para a proteção contra ameaças de diversos tipos, minimizando danos que possam ocorrer. As Unidades prisionais onde há recursos tecnológicos, não há política de segurança da informação específica para a área, e se existe é muito falha.

Considerando esses aspectos e a vivência do autor no contexto da tecnologia da informação na área prisional, este trabalho busca compreender a importância e os benefícios de uma política de segurança da informação, bem como o seu cumprimento no ambiente prisional.

Considerando, ainda, a escassez de interesse da sociedade relacionada aos assuntos carcerários e por se tratar de um tema pouco abordado no cotidiano social, o cenário em questão não recebe a atenção necessária para uma razoável segurança de suas informações.

Para a sociedade, este tema representa uma preocupação com o dever social em garantir que as obrigações e tarefas carcerárias sejam realizadas de modo seguro, almejando uma melhor atuação da segurança pública, contribuindo com o progresso e desenvolvimento da mesma.

Quanto ao foco acadêmico, com a abordagem e levantamento dos riscos encontrados no ambiente prisional, desenvolve-se o interesse à pesquisas e trabalhos que podem aprimorar a questão da segurança das informações carcerárias. Leva-se em consideração o desejo profissional do autor em adquirir conhecimentos para implantação de controles e minimização dos riscos relacionados à segurança da informação.

A partir da exposição feita pelo autor do trabalho, os objetivos a serem atingidos estão divididos em objetivos gerais e objetivos específicos. O objetivo geral é identificar vulnerabilidades quanto à segurança da informação em um ambiente prisional, para que este trabalho se base para soluções de melhoria.

Os objetivos específicos são: conscientizar as pessoas que trabalham nesse ambiente quanto aos ricos e vulnerabilidades na segurança, viabilizar momentos

de formação, pensar e propor mecanismos que aumentem a segurança das informações.

Para a realização deste trabalho, e para alcançar os objetivos propostos, pretende-se usar como metodologia, um levantamento bibliográfico quanto à segurança da informação, e bem como as leis que regulamentam esta questão aos órgãos públicos.

Em seguida, para uma melhor compreensão do tema no sistema penitenciário brasileiro, foi realizada uma pesquisa em forma de questionário que foi respondida por 20 pessoas envolvidas diretamente no ambiente prisional, cerca de 15% do corpo funcional de um presídio do interior paulista. A pesquisa foi realizada do período de 21 de outubro de 2013 a 25 de outubro de 2013.

Com a análise dos dados coletados pelo estudo de caso, estabelece-se graficamente os resultados da pesquisa e as conclusões deste trabalho.

2 LEVANTAMENTO BIBLIOGRÁFICO

Esta seção apresenta o levantamento bibliográfico acerca dos pontos principais relacionados à esta pesquisa, buscando esclarecer aspectos da segurança da informação e das peculiaridades existentes em um ambiente prisional.

2.1. A importância da segurança da informação

As informações relacionadas e pertinentes a uma unidade prisional são consideradas como ativos da organização. Esses ativos podem existir em diversos formatos, como por exemplo, impressos ou anotados em folhas de papel, armazenados eletronicamente, mostrados em imagens, citados em conversas, transmitidos por correio eletrônico, dentre outras maneiras. Entretanto, não importa como a informação encontra-se, é necessário que ela seja sempre protegida de maneira adequada.

Para a ISO 27002 (2005), norma que padronizadora internacional, revela que a segurança da informação, é a preservação da confidencialidade, integridade e disponibilidade da informação, e a autenticidade, responsabilidade, o não repúdio e confiabilidade, também são propriedades que podem estar envolvidas.

Para Fontes (2006), a segurança da informação pode ser definida como um conjunto de orientações, normas, procedimentos, políticas, e demais ações que visam proteger a informação, para garantir a disponibilidade, integridade, confidencialidade, legalidade, não repúdio de autoria e a autenticidade da informação.

Sêmola (2003) define a segurança da informação, como uma área de conhecimento que está voltada à proteção dos ativos da informação contra possíveis ameaças, tendo como principal objetivo garantir a integridade, confidencialidade e disponibilidade da informação.

A segurança da informação é constituída por três atributos básicos que juntos formam os pilares da segurança da informação. Estes atributos têm por objetivo manter os requisitos básicos para garantir a segurança da informação.

Os atributos essenciais para a segurança da informação são: integridade, disponibilidade e confidencialidade.

Figura 1- Pilares da segurança da informação (MACEDO, 2013)

A confidencialidade é definida pela proteção da informação contra a leitura, cópia ou alteração, por qualquer individuo que não seja autorizado pelo proprietário da informação. Como no caso das redes de computadores, enquanto as informações trafegam pela rede, não podem ser interceptadas, alteradas ou extraviadas por pessoas não autorizadas.

Toda informação deve ser protegida conforme o grau de sigilo de seu conteúdo, ficando disponível apenas para pessoas autorizadas. Sêmola (2003)

define a confidencialidade como sendo a garantia de que a informação é acessível apenas por pessoas a qual ela é destinada.

Se um sistema encontra-se indisponível quando um usuário autorizado necessita da informação, acarretará problemas graves ao usuário, prejudicando-o tanto quanto se a informação fosse removida do sistema.

Por isso, Sêmola (2003), diz que a disponibilidade visa garantir que os usuários autorizados tenham acesso à informação e aos ativos correspondentes quando necessário para qualquer finalidade.

A disponibilidade também consiste na proteção da informação para que não seja destruída ou se torne indisponível sem autorização. Também inclui a manutenção dos acessos aos dados disponíveis. O objetivo é que a mensagem chegue aos usuários de forma integra e confiável.

Para se obter integridade os dados devem estar seguros para que não sejam modificados por pessoas não autorizadas. A preocupação com a gravação ou alteração dos dados, é essencial, pois se a integridade de um sistema é violada, então a confidencialidade do mesmo arquivo pode ser facilmente alterada.

A integridade consiste em evitar que dados sejam apagados ou alterados, sem a prévia autorização do proprietário da informação. Segundo Sêmola (2003), garantir a integridade é assegurar que a informação seja mantida na mesma condição em que foi disponibilizada pelo proprietário da informação.

Para melhor compreensão, a figura 2 mostra como o padrão de segurança ISO 27002 define os princípios básicos da segurança da informação:

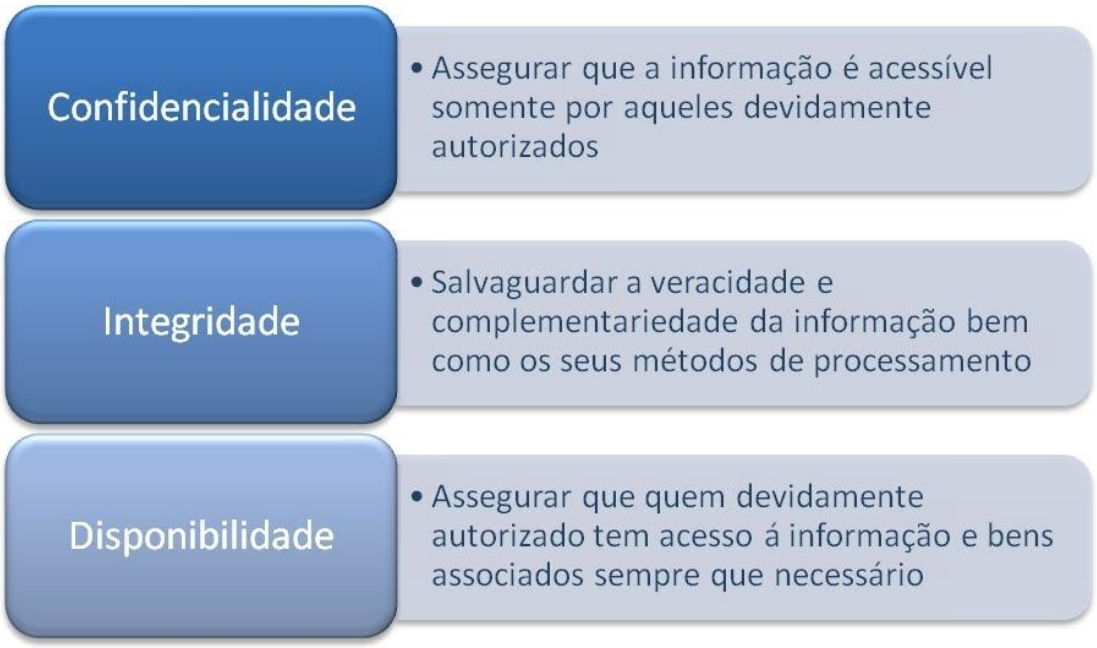

Figura 2: Norma ISO 27002 (2005)

Não se garante que a informação esteja segura, sem que essa informação seja controlada e gerenciada, e para que isso ocorra, é necessário o levantamento e a classificação dos riscos da informação, a fim de minimizar os riscos existentes na proteção da informação.

2.2 Classificação da informação

Para que as informações recebam a segurança adequada, é necessário classificá-la de acordo com sua criticidade. Esta classificação é necessária para manter e proteger o sigilo e a segurança das informações carcerárias. Porém este processo classificatório pode variar de organização para organização, e o nível de sigilo e criticidade das informações do tipo de negócio realizado pela organização.

A classificação pela criticidade das informações identifica os riscos para a organização, caso a informação seja divulgada de maneira indevida. Nas unidades prisionais esta classificação varia de acordo com a necessidade do proprietário da informação. A confidencialidade das informações em um ambiente prisional é muitas vezes subjetiva, ao invés de objetiva, e somente o proprietário da informação pode classificar o grau de sigilo e confidencialidade desta informação.

Para poder classificar uma informação é necessária uma avaliação do negócio, dos processos e atividades que são realizadas pela organização. A seguir encontram-se definições que para Ferreira e Araújo (2008) devem ser estabelecidas no início do processo de classificação das informações.

- Classificação: Atividade que tem como objetivo atribuir o grau de sigilo necessário das informações;
- Proprietário: Profissional responsável pelo ativo da informação na organização;
- Custodiante: Profissional responsável por garantir que as informações estão de acordo com o estabelecido pelo proprietário da informação;
- Criptografia: Proteção por meio de codificação que permite proteger a informação de acessos não autorizados;
- Perfil de acesso: Define os direitos de acesso de cada informação;

Após a definição dos critérios junto ao proprietário da informação, classifica-se a informação segundo seu nível de criticidade. Vale ressaltar que, este processo de classificação pode variar conforme a organização.

Ferreira e Araújo (2008) classificam as informações em três níveis de confidencialidade: pública, interna e confidencial.

- **Informação pública**: São informações que não necessitam de nenhum sigilo ou proteção, pois se forem divulgadas não trarão impactos para a organização;
- **Informação interna**: são informações que devem ser protegidas de acessos externos, porém se tais informações forem divulgadas as consequências não serão críticas;
- **Informação confidencial**: É a informação que necessita de recursos de proteção e só poderá ser acessada por pessoas autorizadas. Caso seja divulgada, esta informação pode comprometer as operações, ou até mesmo a segurança da organização.

Cada organização tem sua necessidade quanto a classificação das informações e pode criar a quantidade de níveis de confidencialidade que atenda às suas necessidades.

Haja vista que as informações que circulam em um ambiente prisional, são extremamente sigilosas e confidenciais, as prisões apresentam desafios e requerem recursos intensos de segurança das informações, e também uma política de segurança da informação bem estruturada para que as informações continuem integras e seguras.

2.3 Política de segurança

Para Ferreira e Araújo (2008), uma política de segurança da informação é um conjunto de regras e padrões sobre o que deve ser feito para garantir que as informações de uma organização recebam proteção adequada, por meio de métodos e procedimentos utilizados para a manutenção da segurança da informação.

A política de segurança da informação pode ser composta por normas, instruções e procedimentos que estabelecem os critérios de segurança que serão utilizados, visando à padronização e normalização da segurança, tanto no aspecto humano, quanto no aspecto tecnológico.

A política de segurança da informação, pode ser dividida em três aspectos hierárquicos: diretrizes, normas e procedimentos.

- Diretrizes de segurança da informação: São as estruturas, diretrizes e obrigações referentes à segurança da informação;
- Normas de segurança da informação: Estabelecem os métodos e obrigações definidas de acordo com as diretrizes da segurança da informação;

- Procedimentos de segurança da informação: É a concretização do disposto nas normas e na política, e permite a aplicação direta nas atividades da organização;

A política deve conter procedimentos regulamentados para a criação, o manuseio, o armazenamento e o descarte de informações. Porém, cada organização tem suas próprias prioridades, e a política de segurança da informação deve ser estruturada de acordo com a necessidade de cada uma delas de modo personalizado.

2.4 As informações prisionais

As unidades prisionais do Estado de São Paulo têm como diretriz o Regimento Interno Padrão (RIP), constituído pela resolução SAP – 144 de 29 de junho de 2010, que padroniza o trabalho desenvolvido no âmbito das unidades prisionais, de forma que não haja condutas diferentes para situações análogas, por meio de métodos de melhores práticas os procedimentos, a fim de mitigar riscos à segurança das informações prisionais.

As informações prisionais, segundo Resolução SAP – 144 (2010), que institui o regimento interno padrão das unidades prisionais do estado de São Paulo, são constituídas por várias informações sobre a pessoa presa, tais como antecedentes criminais, informações pessoais, informações de seus familiares (visitantes), bem como a localização do mesmo na unidade em tempo real. Dentre essas e outras informações pode-se citar:

- Ficha qualificativa do detento;
- Perfil classificatório de periculosidade do detento;
- Motivo de sua prisão;
- Documentos de familiares visitantes;
- Localização exata do detento na unidade prisional;
- Data e local para transferência, quando esta ocorrer;

- Agenda de apresentações judiciais;
- Condenação (quando houver);
- Fotografia e Informações datiloscópicas ou biométricas (detentos, visitantes, terceiros e funcionários);
- Controle de população carcerária;
- Informações sobre denúncias;
- Controle de procedimentos operacionais internos;
- Prontuários de detentos;

Estas informações se aplicam não somente aos detentos que estão reclusos na prisão, mas também àqueles que já passaram por ela, como por exemplo os que já foram postos em liberdade por força de alvará de soltura ou transferidos.

Vale lembrar que informações de núcleo de pessoal dos funcionários também são informações pertinentes à área de segurança da unidade, pois segundo a Secretaria de Administração Penitenciária (SAP), tendo por base a Resolução SAP – 144, em áreas de segurança prisional deve-se sempre saber a quantidade e a identificação dos funcionários que estão trabalhando no momento.

Portanto, todas estas informações podem estar armazenadas impressas ou eletronicamente, e devem estar atualizadas e protegidas de alterações, para não atrapalhar o bom andamento dos trabalhos penitenciários, em momentos de crise, para uma rápida tomada de decisão.

2.4.1 A segurança da informação nas prisões

A Lei 12527/11 regulamenta o acesso às informações de órgãos públicos, e os auxilia a manterem a integridade, disponibilidade e confidencialidade da informação, incluindo em seu processo a responsabilidade, autenticidade e auditabilidade dos mesmos.

E assim como qualquer outra organização, as prisões necessitam implementar controles de segurança, devido ao grande fluxo e a diversidade de informações que necessitam ser armazenadas, processada e gerenciadas.

Caso isso não ocorra, a falta de controles de segurança pode deixar as informações expostas às pessoas não autorizadas e o uso indevido dos sistemas de informações pode comprometer as informações sigilosas da unidade prisional e resultar em sérios problemas, que vão desde falta de alimentação, tentativas de fugas, rebeliões, e até morte.

Um controle de segurança adequado para área prisional assegura a confidencialidade, integridade, e disponibilidade das informações, além de ajudar a evitar erros resultantes da incapacidade de manter a segurança das informações carcerárias (Sêmola, 2003).

A segurança nas unidades prisionais que manipulam as informações, eletronicamente ou não, é extremamente importante, pois a segurança das pessoas envolvidas no processo carcerário depende da manutenção da confidencialidade das informações armazenadas.

2.4.2 O armazenamento das informações carcerárias

As informações carcerárias podem ser armazenadas em meios eletrônicos ou em meios físicos. De modo geral, as informações são armazenadas em prontuários e arquivos em forma de papel, de maneira que após cada procedimento, efetua-se um novo registro.

Unidades prisionais no estado de São Paulo, que possuem o recurso da informática, armazenam suas informações carcerárias em servidores nas próprias unidades, além de utilizarem um recurso integrado de informações, o Centro de Processamento de Dados do Estado de São Paulo (PRODESP), visando a melhor eficiência do setor público (PRODESP, 2013), onde se armazenam e atualizam-se as informações referentes à carceragem, que podem ser acessadas por outras unidades de maneira integrada e restrita.

2.4.3 Os riscos das informações nas unidades prisionais

Risco consiste na probabilidade de que alguma ameaça explore as vulnerabilidades de um ativo, e provoque algum dano à organização. Para a NBR ISO/IEC 17799/2005, as ameaças podem ser definidas como uma causa potencial de um incidente indesejado, que pode causar danos à organização e as vulnerabilidades se definem como a fragilidade de um ativo da organização que pode ser explorado por uma ameaça.

A segurança da informação é uma prática voltada a eliminar as vulnerabilidades existentes, para reduzir os riscos das ameaças se concretizarem. A ISO 27002/2008 mostra que a existência do risco é determinada a partir das ameaças e das vulnerabilidades dos ativos da informação. A figura a seguir ilustra o relacionamento entre riscos e a fonte de riscos.

Figura 3: Os riscos e as fontes de riscos (ISO 27002, 2005)

Considerando o nível de tensão no ambiente prisional, o risco de aumento das vulnerabilidades dos sistemas de informação tem um aumento significativo. Tal grau de tensão eleva a taxa de erro humano e com isso a probabilidade de risco aumenta.

O ambiente prisional contem ameaças e vulnerabilidades únicas, que devem ser consideradas com certo cuidado, para garantir que nenhum risco relacionado à informação venha a existir.

No ambiente prisional apresentam-se vários tipos de ameaças existentes. As ameaças a seguir devem ser consideradas pelas unidades prisionais quando forem avaliar os riscos para a confidencialidade, a integridade e a disponibilidade das informações.

Os tópicos a seguir referem-se às principais ameaças que podem ser encontradas no ambiente prisional, considerando os regimentos, diretrizes, normas e os recursos disponíveis:

- Funcionários utilizando usuário e senhas de outros usuários;
- Anotações e documentos descartados indevidamente;
- Uso não autorizado do sistema por estranhos;
- Uso não autorizado dos sistemas de informação por prestadores de serviço;
- Uso de software prejudicial ao sistema;
- Uso indevido de recursos do sistema;
- Infiltração de indivíduos não autorizados na rede interna;
- Não confidencialidade das informações por falta de criptografia na comunicação;
- Repúdio de autoria, envio ou recebimento das informações;
- Falha na conexão à rede de computadores;
- Códigos maliciosos no sistema;
- Sistemas indisponíveis;
- Envio de informações de maneira acidental;
- Falhas técnica no hardware ou software da rede;
- Falhas ocasionadas por ameaças naturais;
- Falhas de segurança na rede;
- Falhas humanas por falta de conscientização;
- Falta de capacitação dos funcionários;
- Furto de equipamentos ou dados;

A resolução SAP – 144 releva que tais riscos e ameaças variam de ambiente para ambiente conforme art.183.

> "**Artigo 183** - Consideradas as peculiaridades próprias, podem as unidades prisionais expedir normas complementares e adequadas às suas condições, respeitadas as disposições deste Regimento, no que couber, comunicando-se a Secretaria da Administração Penitenciária, por meio da respectiva coordenadoria regional ou de saúde." (Resolução SAP-144,2010)

Cada ambiente tem suas próprias características, e por sua vez cada ambiente tem seus próprios riscos, que podem ser considerados ou não no momento de identificação destes riscos. O ideal é que haja um alinhamento estratégico entre a política de segurança e o objetivo da organização.

Para se avaliar o tratamento adequado que deve ser aplicado a cada risco é importante definir junto à organização, os critérios que determinam a aceitabilidade deste risco. Nestes critérios, consideram-se os objetivos da empresa, requisitos, regulamento, custos de implementação, a operação em relação aos riscos, a necessidade de balancear o investimento de implementação e controles, dentre outros.

O tratamento de risco refere-se à atividade de reduzir os riscos a níveis aceitáveis. A avaliação e definição do que é ou não aceitável deve ser definido pela organização prisional.

Caso a organização escolha não implementar um determinado controle de tratamento de risco, é inteiramente aceitável e válido. Porém, é conveniente que isso seja registrado de maneira formal na política de segurança.

Em unidades prisionais é extremamente necessária a documentação dos níveis aceitáveis de riscos, por se tratar de uma instituição onde a segurança é prioridade em seus processos.

2.5 Política de segurança da informação nas unidades prisionais

Para se atingir um controle adequado de segurança da informação, é necessária a implementação de uma política de segurança que seja aprovada pela alta administração. Além disso, ela deve ser publicada e comunicada a todos os funcionários e pessoas envolvidas no sistema carcerário. O conteúdo da política de segurança da informação deve basear-se nos resultados da avaliação de risco feita pela unidade prisional.

Cada colaborador é responsável por utilizar os recursos tecnológicos disponíveis de forma a aumentar a produtividade e contribuir para os resultados e a imagem pública da unidade prisional. A política da informação no ambiente prisional tem o propósito de fornecer apoio e orientação à gestão de segurança da informação. Porém, nos órgãos carcerários existentes no Estado de São Paulo, não há políticas de segurança da informação implementadas.

2.5.1 A criação, revisão e disponibilização da política

A norma ISO/IEC 27002 (2005) fornece orientações sobre o que deve ser abordado em uma política de segurança. Com base nessas orientações pode-se analisar o que uma política de segurança da informação voltada para ambiente prisional deve abordar:

- Abordar a necessidade de segurança da informação na área carcerária;
- Abordar as metas de segurança da informação;
- A política deve ser adotada, divulgada e revista pela unidade prisional;
- Abordar os requisitos regulamentares da organização;
- Abordar a amplitude das informações carcerárias;
- Abordar os direitos e responsabilidades éticas dos profissionais;
- Abordar os protocolos e procedimentos adotados no compartilhamento de informações para garantir a segurança da mesma;

Como toda política de segurança, a política de segurança da informação para unidades prisionais, também está sujeita às revisões periódicas. A unidade deve determinar o tempo em que estas revisões deverão ser efetuadas. A política deve

ser revisada ao menos uma vez ao ano, segundo a NBR ISO 27002 (2005). Mas caso ocorra um incidente na segurança da informação, a política deve ser revista, imediatamente após o incidente.

A NBR ISO 27002 (2005) também fornece orientações para realização de revisão na política de segurança que deve abordar:

- Abordar a natureza mutável das operações da organização prisional;
- As alterações feitas na infraestrutura de Tecnologia da Informação;
- Mudanças no ambiente externo que podem acarretar impactos na organização;
- Novos controles implementados;
- Os desafios relacionados à segurança da informação existentes na política anterior;

Muitas organizações disponibilizam eletronicamente e/ou pela Internet os documentos da política de segurança da informação, mas além deste meio deve-se tomar ciência dos colaboradores da política também através de termos de ciência. Este procedimento inclui a alta diretoria e até mesmo os prestadores de serviços temporários.

Quando a unidade prisional utiliza de serviços de empresas terceirizadas, o documento de política de segurança deve conter controles e procedimentos que cobrem tais interações e que especifiquem as responsabilidades de todas as partes envolvidas no processo carcerário.

Para que haja uma interação e conscientização, que possa agregar benefícios e segurança à organização, a política deve estar disponível para todos os colaboradores da organização.

2.6 Normas de segurança da informação para o setor público

Com a frequente preocupação relacionada à segurança da informação em órgãos públicos e a necessidade de maior transparência e disponibilidade de informações públicas, regulamentaram-se os acessos às informações dos órgãos públicos com a lei 12.527/11, sancionada pela presidente Dilma Rousseff no dia 18 de novembro de 2011.

Essa lei regulamenta a disposição da informação de órgãos públicos, baseando-se nos princípios de integridade, disponibilidade e confidencialidade da informação, abordando além de suas disposições gerais, normas de acesso, divulgação da informação, também os procedimentos e restrições de acesso às informações.

Trata também da proteção e do controle das informações consideradas sigilosas, assim como os procedimentos de classificação, reclassificação ou desclassificação do grau de sigilo destas informações.

Regulamenta também o acesso às informações pessoais dos funcionários envolvidos no setor. Publicam, como por exemplo, seus vencimentos, e descrevem quais as responsabilidades do agente publico na disposição das informações.

O objetivo das normas e resoluções existentes é ressaltar a importância da segurança da informação e garantir a integridade, disponibilidade e confidencialidade das informações de ordem pública.

3 Estudo de caso

Para se ilustrar e compreender a questão da segurança da informação em unidades prisionais realizou-se um estudo de caso desenvolvido para identificar as possíveis ameaças e falhas na segurança da informação.

3.1 Aspectos do caso

O estudo de caso realizou-se em um presídio no interior do Estado de São Paulo, classificado como um centro de detenção provisória. A escolha deste cenário se deu pelo fato do mesmo apresentar grandes fluxos de informações carcerárias diariamente.

Para a realização da pesquisa, adotou-se como método de coleta de dados, um questionário (Anexo A) contendo 7 perguntas objetivas e 1 descritiva, no intuito de conhecer e avaliar os riscos à segurança da informação, bem como o nível de conhecimento e compreensão dos funcionários quanto às possíveis falhas e riscos de segurança da informação neste ambiente de trabalho.

Para uma coleta de dados transparente, precisa, completa e fiel à realidade, foi assegurado às pessoas pesquisadas o direito de anonimato, sigilo e a liberdade de participar e, em qualquer momento, sair da pesquisa.

A coleta de dados concretizou-se do período de 21 à 25 de outubro de 2013, e foi respondida por vinte pessoas (aproximadamente 15% do corpo funcional da unidade prisional). Dentre os participantes, estavam funcionários de todos os setores carcerários de modo que a abrangência da pesquisa seja amplamente difundida. Após a coleta dos dados, efetivou-se uma análise detalhada.

3.2 Resultados e discussões

Todo processo investigativo aqui detalhado, desde a criação das questões até a análise dos resultados, tem por objetivo, obter contribuições acerca da problemática do trabalho. A primeira questão do questionário aplicado, diz respeito à questão do acesso à rede de computadores.

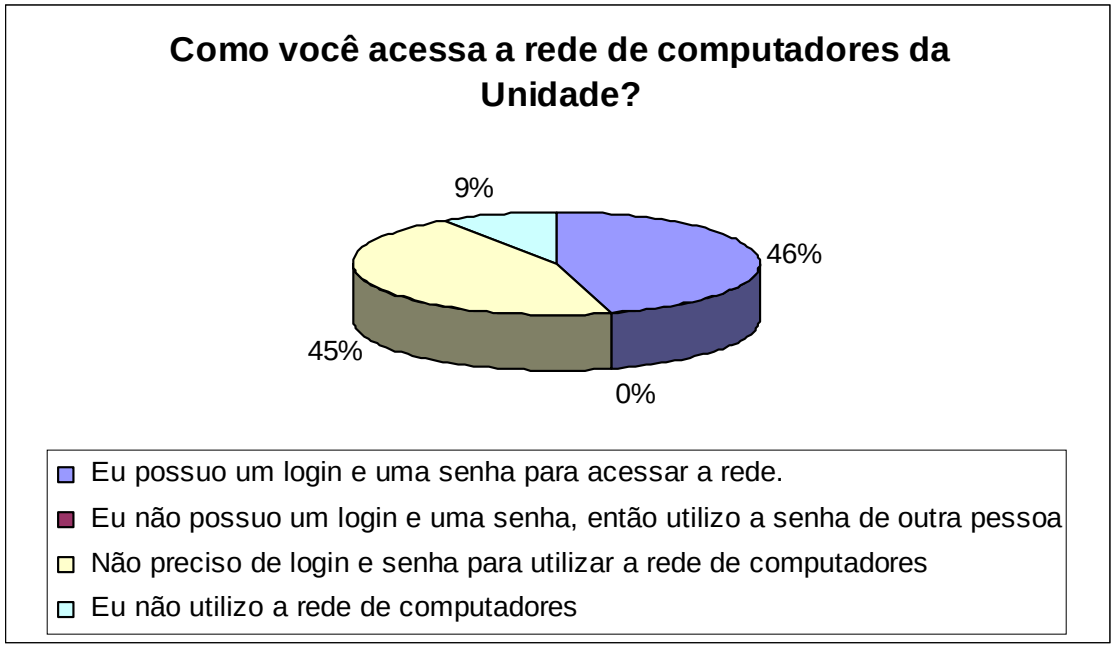

Figura 4: Acesso à rede (Autoria própria, 2013)

Ao se fazer a pergunta acima (figura 4) aos entrevistados, nota-se que a grande maioria tem acesso à rede de computadores (91%), porém ressalta-se a forma que se obter esse acesso.

A metade dos entrevistados que tem acesso à rede, alega possuir login e senha, enquanto a outra metade dos entrevistados, dizem que não precisam. Encontra-se assim, a primeira vulnerabilidade da segurança da informação, que viola o princípio da confidencialidade na segurança da informação. O fato de não se identificar quem acessa a rede, torna toda rede vulnerável, pois pessoas não autorizadas podem ter acesso às informações.

Salienta-se que, segundo os entrevistados, ninguém utiliza o login e a senha de outra pessoa para ter acesso à rede de computadores. Isso se dá ao fato de que 45% dos entrevistados não se identificam através de login e senha para acessar a rede, tornando desnecessário o fato de utilizar ou solicitar a senha de outro usuário.

Os usuários da rede também alegaram que algumas aplicações utilizadas diariamente, requerem o registro de login e senha para execução no sistema. Desta maneira cria-se um compromisso de responsabilidade com o usuário pelos dados que serão manipulados no sistema. Por outro lado, nem todos os usuários possuem este login e senha para uso destas aplicações. E se, por exemplo, este usuário for transferido, ou até mesmo sair de férias, o mesmo fornece seu login e senha para o seu sucessor até que a situação cadastral se legalize, tornando o acesso às informações vulnerável.

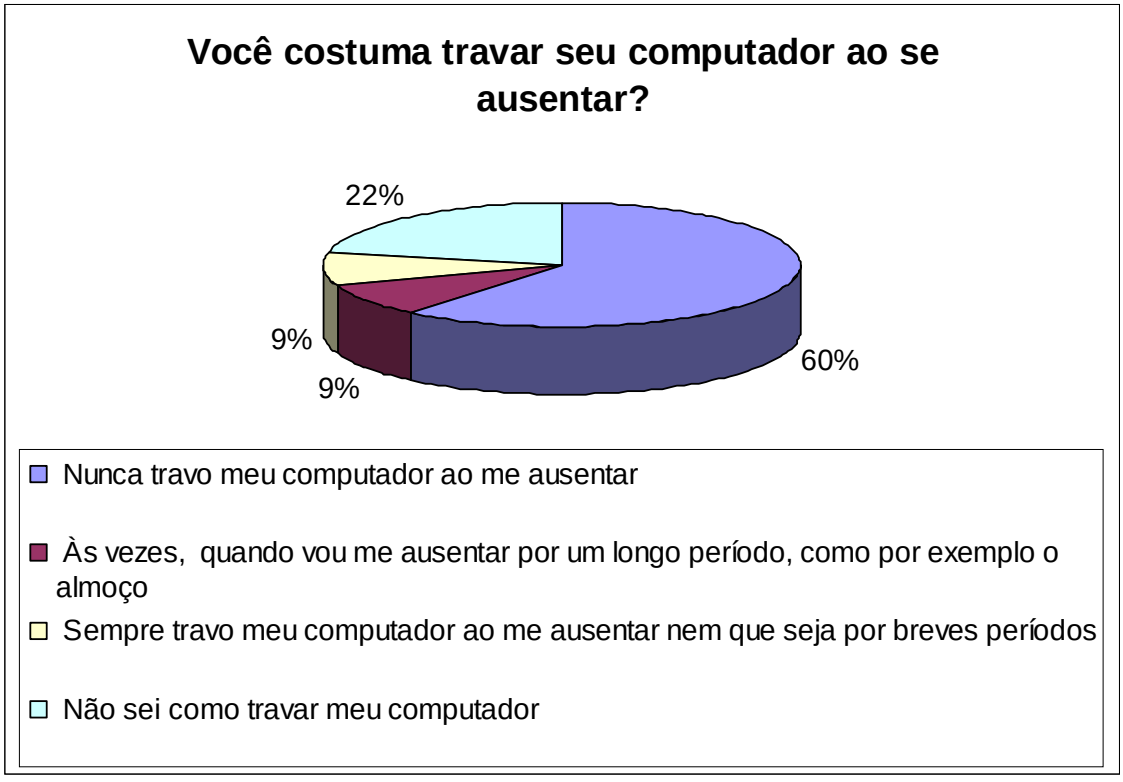

Figura 5: O computador nos períodos ociosos (Autoria própria, 2013)

A figura 5 retrata o quanto as informações estão vulneráveis na ausência dos seus gestores, uma vez que como visto na figura 4, a maior parte dos entrevistados não necessitam de permissão para acessar a rede, desrespeitando novamente o princípio da confidencialidade. Isso ocorre pelo fato do computador permanecer ligado à rede quando seu usuário se ausenta, aumentando o risco de um usuário não autorizado adentrar a rede em busca de informações.

A maior parte dos entrevistados nunca trava seus computadores ao se ausentarem (60%), gerando uma falha de segurança da informação. Se a informação manipulada for classificada como sigilosa, esta falha de segurança pode arruinar todo o trabalho da política de segurança da informação.

Um dado considerável é que 22% dos entrevistados sequer sabem como travar seus computadores. O fator humano na segurança da informação é primordial e se o pessoal autorizado, que manipula as informações, não está devidamente instruído a realizar tarefas básicas de segurança da informação, toda a política será inútil. A ciência dos colaboradores é essencial para o bom andamento da política de segurança da informação.

Com a questão do fácil acesso à rede, tem que se levar em conta onde ficam armazenadas as informações, pois se o acesso à rede for facilitado, o acesso aos documentos e arquivos na rede também podem estar vulneráveis. A figura a seguir nos mostra os locais onde os documentos são salvos com mais frequência.

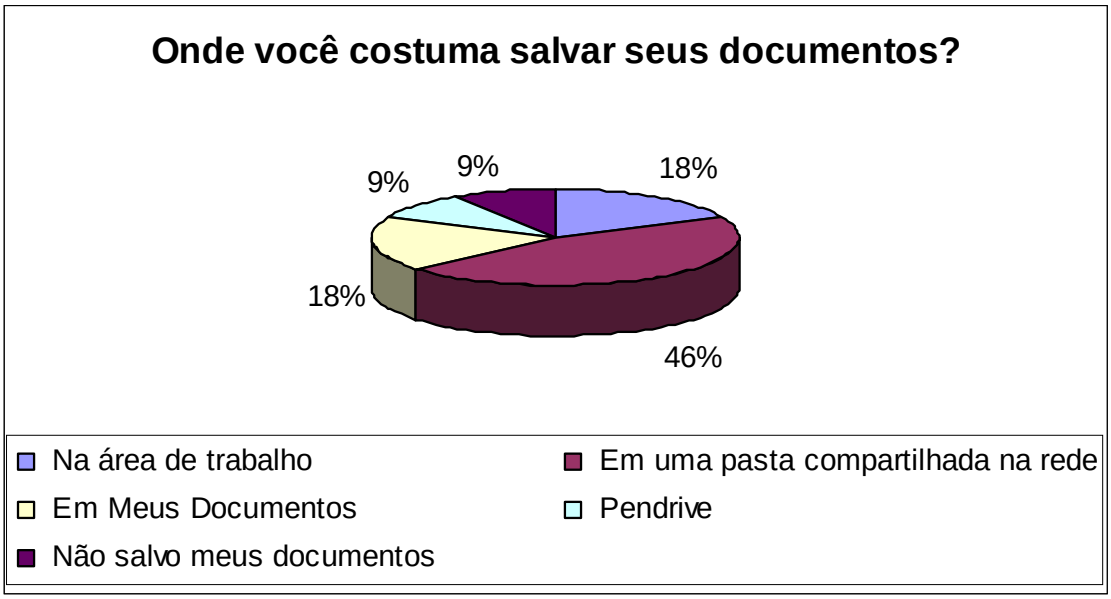

Figura 6: Documentos salvos (Autoria própria, 2013).

Conforme a pesquisa a maior parte dos entrevistados (46%) salvam seus documentos em pastas compartilhadas na rede. Porém, como visto na figura 4, quase metade dos entrevistados acessa a rede sem precisar fazer uso de login e senha.

Isso reforça a ideia de que a informação não está segura, já que a maior parte das informações da rede está salva na própria rede, que tem acesso irrestrito, e disponível para qualquer usuário da rede.

A segunda maior parcela ressalva que os documentos utilizados pelos usuários são salvos na pasta Meus Documentos (18%) e na Área de Trabalho (18%). Observando os documentos salvos nestes locais, as informações ali contidas também ficam vulneráveis, uma vez que estão salvos no próprio computador. Vale lembrar que, na maior parte do tempo que fica ocioso, não é travado, o que facilita o acesso aos arquivos e pastas. (vide figura 5)

Entretanto, 9% dos entrevistados sequer salvam seus documentos, gerando contratempos na recuperação de dados e documentos. Segundo os próprios entrevistados, isso ocorre por falta de instrução e ciência desta parcela de funcionários, facilitando a transgressão do principio da confidencialidade, e se os

dados forem alterados sem permissão do usuário da estação de trabalho, abala o principio da integridade.

Ainda sobre o princípio da integridade e confidencialidade na segurança da informação, e para entender e compreender melhor o porquê de proteger ou salvar as informações carcerárias, identificou-se à quais informações as pessoas que utilizarem a rede terão acesso. A figura 7 nos mostra a abrangência de informações carcerárias que o usuário tem acesso.

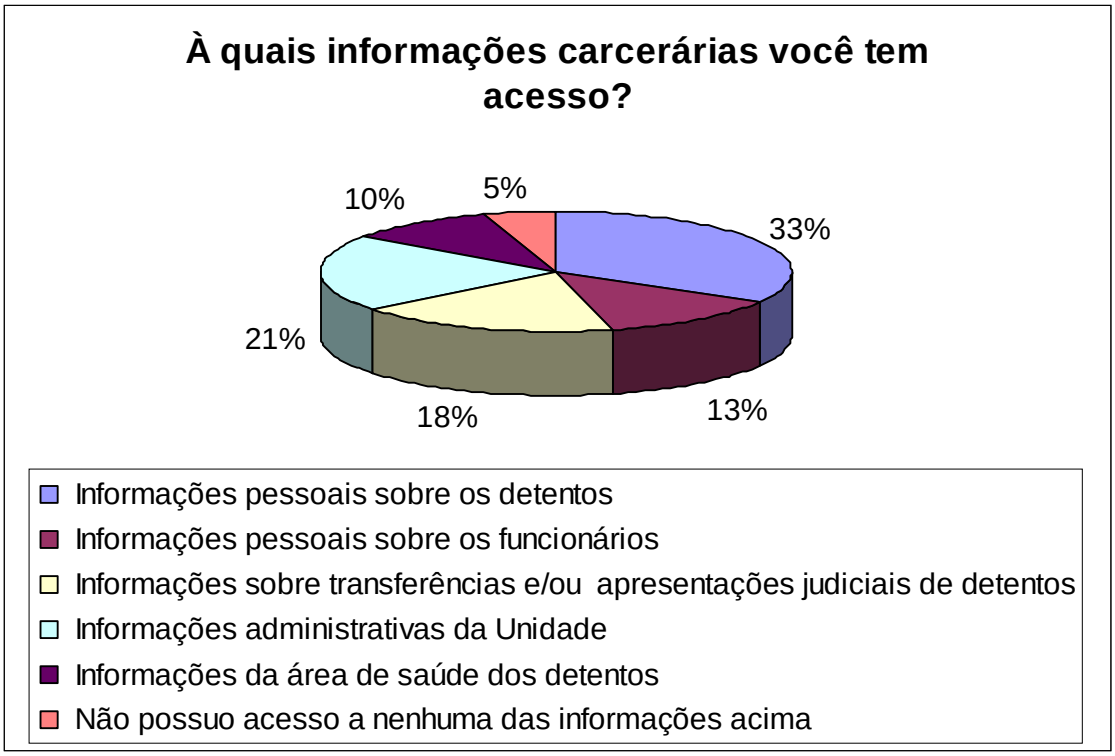

Figura 7: As informações carcerárias (Autoria própria, 2013).

Com base nos dados acima, as informações relacionadas são classificadas como confidenciais, exceto as informações administrativas. As informações administrativas (18%) são classificadas como internas, pois necessitam de proteção, porém se forem divulgadas, as consequências não são críticas para a unidade prisional. Vale ressaltar que as informações administrativas, por força de lei, devem ser tratadas de maneira transparente para a sociedade, e por isso a maior parte de suas informações são divulgadas diariamente.

A grande parte dos entrevistados (33%) tem acesso às informações pessoais sobre detentos. Tendo por base que a principal atividade desta organização gira em torno dos detentos, o resultado era esperado. Porém deve-se avaliar quem tem acesso às informações sobre detentos. Por exemplo, uma pessoa que trabalha no setor de manutenção não necessita acessar as informações pessoais dos detentos para realizar seu trabalho, diferentemente do setor de assistência social.

Seguido da segunda maior parcela destas informações, que são as administrativas (21%), encontram-se as informações sobre transferências e apresentações judiciais de detentos (18%). Estas informações são de bastante importância para a unidade, e necessitam de muito sigilo, pois se forem divulgadas podem afetar criticamente a unidade.

Este tipo de informação em posse de pessoas não autorizadas pode servir de base para tentativas de resgate de detentos, uma vez que se sabe a hora e o local que os mesmos irão estar, fora da unidade onde a segurança é mais vulnerável. Então, uma parcela de 18% para este segmento de informação é considerado alto, em virtude de sua criticidade ao ser divulgada.

Outra informação critica que se for divulgada pode afetar criticamente a organização é a informação pessoal sobre os funcionários (13%). Esta informação é classificada como confidencial por se tratar de informação da vida pessoal e particular dos funcionários.

Dentre estas informações encontram-se endereço, telefone, declarações de imposto de renda, dentre outros dados de funcionários. Esta informação, se manipulada por pessoas não autorizadas, serve como base de tentativas de ameaças ou intimidação dos funcionários por pessoas marginalizadas à lei, e por isso deve ser protegida de maneira eficaz.

Uma informação que também deve ser protegida é a da área de saúde dos detentos (10%). Há leis específicas que regem a segurança deste tipo de informação, como por exemplo a ISO IEC 27799 (2008). Dentre estes dados depara-se com os prontuários de saúde dos detentos, lista de medicamentos,

doenças atuais e anteriores, dentre outras. Estas informações segundo a ISO 27799 (2008), não podem ser divulgadas para evitar constrangimentos aos detentos enfermos.

Nota-se que 5% das pessoas não tem acesso a nenhuma informação carcerária. O fato de não se ter acesso deve-se ao fato de não precisar destes dados para dar segmento aos trabalhos rotineiros. Entretanto, como a rede pode ser facilmente acessada, esta parcela de usuários de rede, pode adquirir a qualquer momento, as informações que lhe seja conveniente.

Como visto no gráfico anterior (Figura 7) cerca de 95% dos entrevistados tem acesso à informações internas e confidenciais na unidade prisional. A questão a seguir é conhecer se estes usuários têm permissão para modificar as informações do sistema.

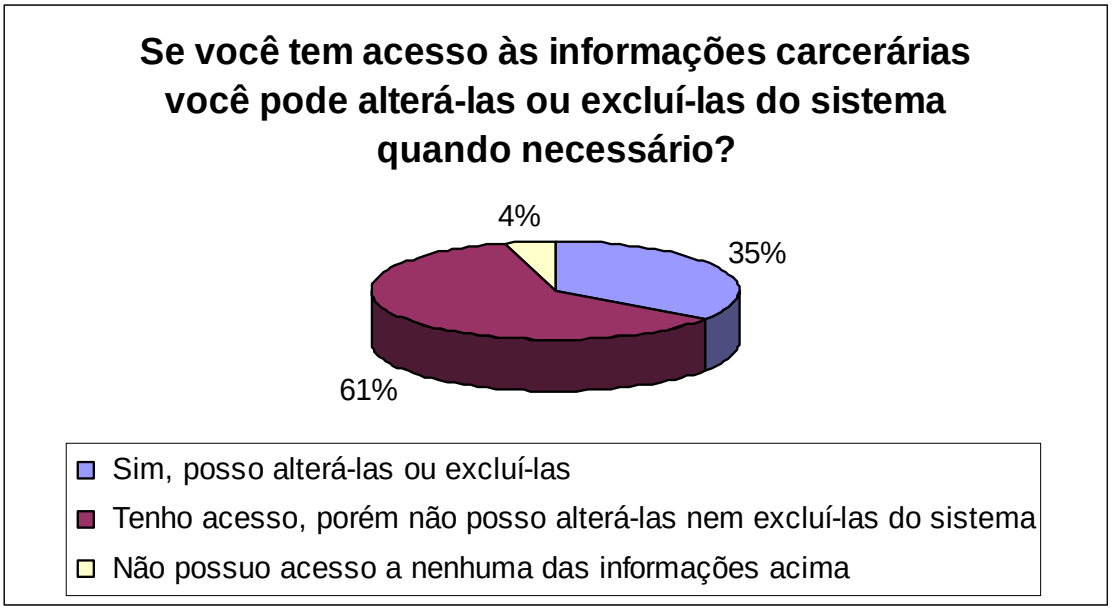

Figura 8: Alteração e exclusão de informações (Autoria própria, 2013).

Segundo os próprios usuários do sistema 35% das pessoas que acessam a rede de computadores podem alterá-las e excluí-las do sistema. O fato de poder alterar estes dados sem qualquer restrição, é uma ameaça à segurança das

informações carcerárias, pondo em risco o princípio da integridade na segurança das informações.

O ideal é criar controles, ou seja, registrar as modificações e exclusões, bem como quando e quem realizou as alterações dos dados do sistema. Assim, inibe e desencoraja o ato de alteração dos dados por pessoas não autorizadas, além de rastrear as modificações de uma forma que controle as alterações e exclusões.

O fato de que 61% dos entrevistados terem somente direito de leitura dos dados, não tornam as informações da rede totalmente seguras. Deve-se controlar se quem tem esta permissão de leitura é, de fato, autorizado a acessar esta informação.

Neste caso, se um usuário puder simplesmente acessar as informações, mesmo que não as modifique, ele pode transmitir esta informação às pessoas que não estão autorizadas a acessar esta informação, e infringir o principio da confidencialidade dos dados. Por isso deve-se salientar a importância da ciência dos usuários da rede quanto à segurança da informação. O gráfico a seguir (Figura 9) retrata esta realidade.

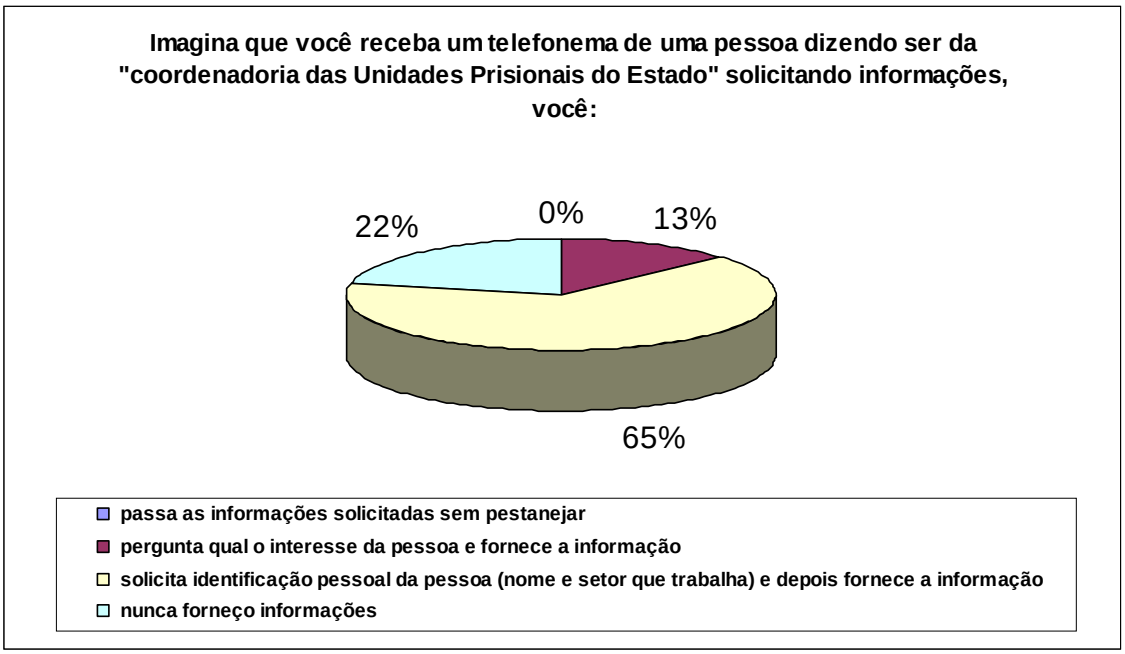

Figura 9: Telefonema de importância social (Autoria própria, 2013).

Na situação apresentada aos entrevistados (Figura 9) repara-se que nenhum dos participantes da entrevista disse que passam a informação de maneira automática. Isso se deve ao fato do ambiente prisional ser bastante tendencioso quanto às suspeitas. As pessoas que trabalham em prisões são induzidas a suspeitar e questionar situações estranhas, por força do ambiente em que trabalham.

Por outro lado, 65% dos entrevistados somente solicitam o nome e o setor que o solicitante trabalha, para passar as informações solicitadas. Deve-se levar em conta que o simples fato de se identificar, não comprova quem realmente está do outro lado da linha telefônica. Cerca de 13% dos entrevistados apenas perguntam o interesse do solicitante, que neste caso, não precisa se identificar para conseguir informações.

Entretanto 22% dos entrevistados nunca fornecem informações por telefone. Este fato pode criar transtornos se o solicitante for realmente da coordenadoria das unidades prisionais. Então quando questionados sobre o fato, os entrevistados disseram que, nestes casos, requerem que a solicitação seja enviada para E-mail interno da unidade prisional.

A unidade prisional conta com uma rede VPN (*Virtual Private Network*), que estabelece uma conexão segura e privada com a coordenadoria, comprovando que as solicitações enviadas realmente correspondem com a coordenadoria. Por isso 22% das pessoas da unidade prisional nunca fornecem informações, ao menos pelo telefone.

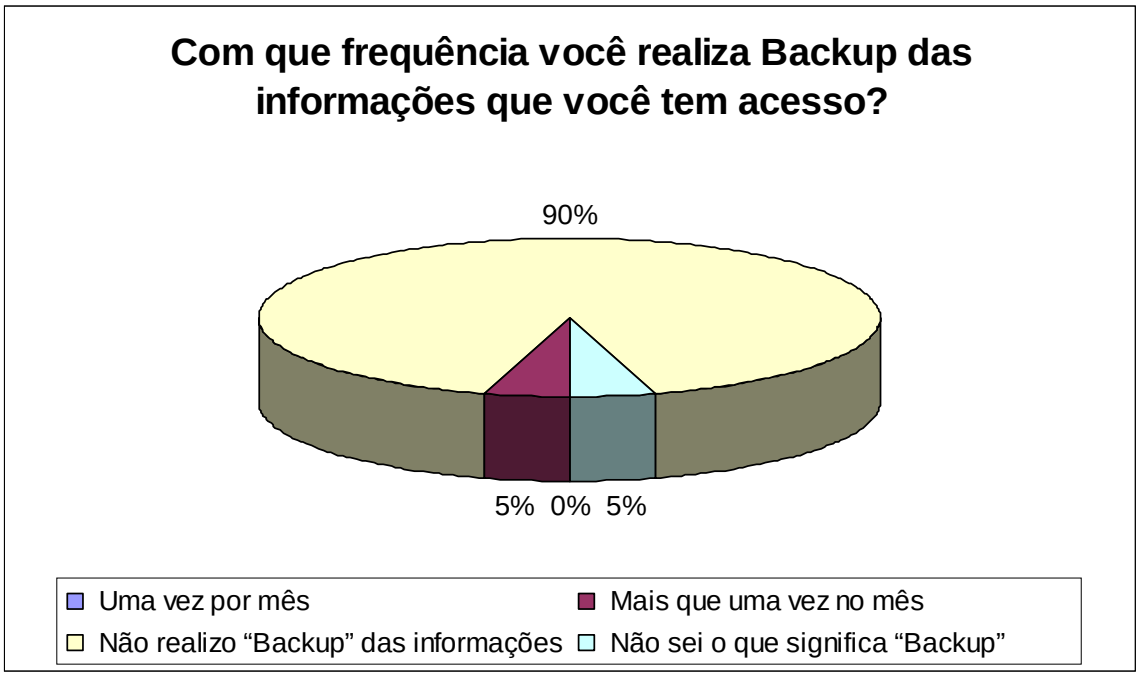

Figura 10: *Backup's* (Autoria própria, 2013).

Foi perguntado aos usuários da rede com que frequência eles realizam *Backup* de suas informações, para se estabelecer o nível de segurança dos princípios da integridade e da disponibilidade das informações carcerárias. O índice de pessoas que não realizam Backup das informações chegou à espantosa marca de 90%. Isso mostra o quanto a informação está vulnerável em casos de perda de dados, pois não há métodos para recuperação de informações.

Apenas 5% dos entrevistados fazem, mais que uma vez ao mês, *Backup* das informações. Este índice é muito baixo, tendo em vista o estrondoso fluxo de informações geradas na unidade prisional diariamente. Outros 5% dos

entrevistados não sabem o que significa *Backup*, ressalvando novamente a falta de consciência dos usuários da rede quanto à segurança da informação.

Para avaliar os níveis de consciência quanto à segurança da informação dos participantes da pesquisa, foi solicitado que eles apontassem as principais falhas na segurança da informação no ambiente em que trabalham. O gráfico a seguir (figura 11) demonstra os dados desta pergunta.

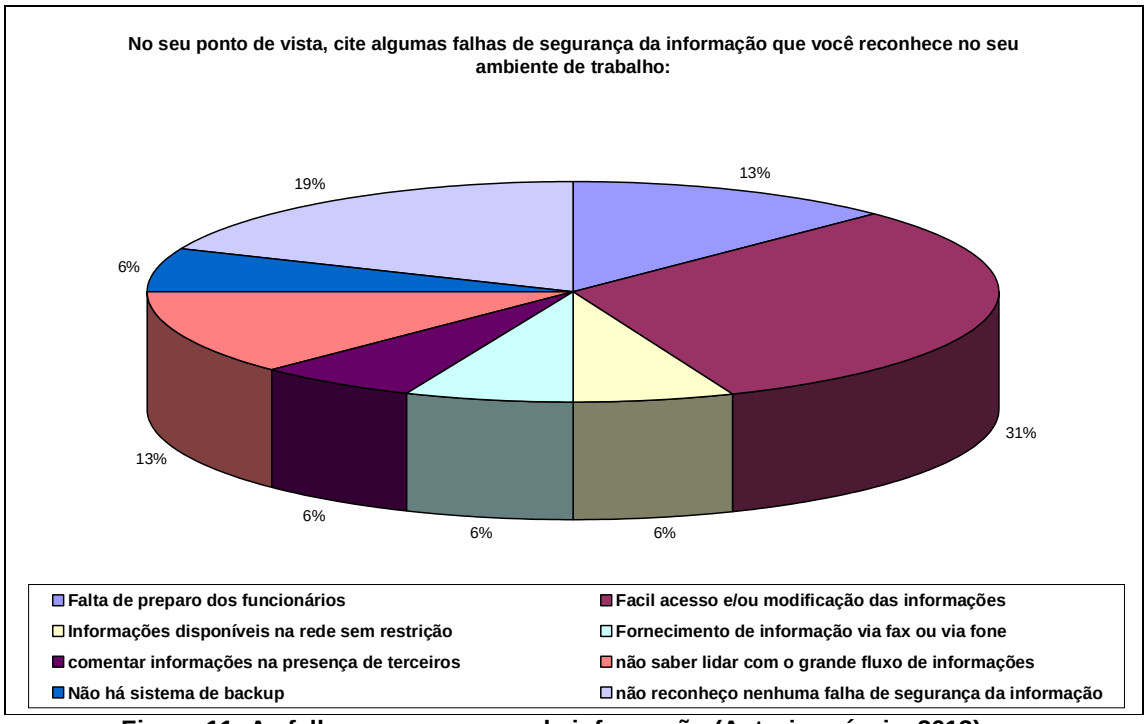

Figura 11: As falhas na segurança da informação (Autoria própria, 2013).

Os dados representados pela figura 11 comprovam o que foi dito anteriormente sobre o fácil acesso às informações da rede, pois a maioria dos entrevistados, cerca de 31%, alegaram que a principal ameaça e falha da segurança da informação é a facilidade de acesso e/ou a modificação das informações.

A segunda falha mais apontada pelos entrevistados foi a falta de preparo dos funcionários (13%), equiparada com o grande fluxo de informações (13%).

Segundo eles, os funcionários não têm um preparo adequado que garanta a confidencialidade, a integridade e disponibilidade das informações carcerárias.

Essa ameaça associada ao grande fluxo de informações causa falhas críticas à organização. A falta de treinamentos e conscientização leva às falhas humanas provocadas pela falta de instrução nos processos da política de segurança da informação.

Dentre as ameaças citadas pelos entrevistados estão: Informações disponíveis na rede sem restrição (6%), o fornecimento de informações via fax ou via fone (6%), comentar informações na presença de terceiros (6%) e a falta de uma política de *Backup* (6%).

O fator que chama a atenção é que 19% dos entrevistados não reconhecerem nenhuma falha de segurança da informação onde trabalham, devido ao fato de não terem ciência da importância da segurança da informação no ambiente prisional.

Todas estas ameaças podem ser sanadas com a implementação de políticas de segurança da informação, visando não só o emprego de controles de segurança, mas também focando o fator humano por trás da política e do ambiente computacional.

A figura 12 mostra uma proposta de política baseada nas principais falhas identificadas neste estudo de caso, e apresenta maneiras de minimização dos riscos a médio e curto prazo, bem como a melhor forma de mitigação das vulnerabilidades.

Este modelo de política tem por objetivo atingir níveis aceitáveis de segurança da informação, levando em consideração os objetivos e recursos disponíveis no ambiente prisional que foi estudado.

Portanto cada ambiente a ser estudado requer uma atenção única e especializada, conciliando os objetivos da unidade prisional com os objetivos da política de segurança a ser implantada.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO BASEADA NAS FALHAS IDENTIFICADAS NO ESTUDO DE CASO			
FALHAS NA SEGURANÇA DA INFORMAÇÃO	**PRINCÍPIO INFRINGIDO**	**MINIMIZAÇÃO DO RISCO**	**MITIGAÇÃO DA FALHA**
Acesso irrestrito à rede	Confidencialidade	Implantação de Servidor de domínio	Implantação de Política de segurança da informação
Falta identificação no acesso aos dados	Confidencialidade	Implantação de Servidor de domínio	
Não travar o computador ao se ausentar	Confidencialidade	Conscientização de pessoal	
Salvar dados inadequadamente	Integridade/confidencialidade	Conscientização de pessoal	
Fácil modificação dos dados na rede	Integridade	Implantação de Servidor de domínio	
Divulgação de informações não autorizada	Confidencialidade	Conscientização de pessoal/termos de confidencialidade	
Falta de política de Backup's	Disponibilidade/integridade	Criar política de Backup	
Sistema indisponível	Disponibilidade	Replicação dos dados nos servidores	
Repúdio de autoria, envio ou recebimento das informações	Confidencialidade	Registros de logs/termos de ciência	
Falhas ocasionadas por ameaças naturais	Integridade/Disponibilidade	Criar um plano de contingência	

Figura 12: Política de segurança sobre o estudo de caso (Autoria própria, 2013)

Como visto na figura 12, há meios para implantação rápida que baixam os níveis de vulnerabilidade existentes no ambiente prisional, mas o ideal é a criação de uma política de segurança da informação que englobe todas as formas de riscos às informações carcerárias, para assim, garantir que os princípios básicos da segurança da informação sejam obtidos.

Como forma de minimizar os riscos cita-se a implementação de servidores de domínio. Neste caso os usuários que desejam acessar a rede devem efetuar um logon. Assim, o servidor de domínio verifica se as informações que o usuário forneceu são válidas, e em caso positivo, faz a autenticação do mesmo no

sistema, garantindo assim a confidencialidade das informações. Deve-se levar em consideração os diferentes ambientes de rede encontrados, para se definir qual o a melhor opção de servidores de domínio disponível no mercado.

Nos casos de conscientização de pessoal, pode-se realizar trabalhos e campanhas para se promover a consciência da segurança das informações carcerárias. Pode-se utilizar desde papéis de parede com instruções nas estações de trabalho, cartazes e panfletos, até mesmo palestras e treinamentos para realização da campanha. Termos de confidencialidade e compromisso também são aplicáveis para uma formalização da política de segurança da informação.

Políticas de *Backup*, não só minimizam os riscos, mas também são necessárias para manter a integridade e a disponibilidade das informações carcerárias. Esta política sugere que se realizem os processos de *backup* de acordo com a periodicidade necessária e importância de cada informação carcerária. Portanto cada ambiente deve se atentar à quais informações e os períodos que se deve realizar este procedimento.

Criar um plano de contingência é a melhor opção para se assegurar a disponibilidade e integridade das informações carcerárias quando uma ameaça se concretizar. Nestes momentos de crise, estes planos mostram os melhores procedimentos a serem adotados para que as informações sofram os menores impactos possíveis.

Esses procedimentos são uns propostos de política definida de maneira viável ao ambiente estudado. Portanto, ao se criar a política de segurança para qualquer outro ambiente prisional, deve-se levar em consideração as particularidades, recursos e limitações de cada ambiente.

4 CONSIDERAÇÕES FINAIS

A informação digital beneficia os funcionários e a organização, pois facilita o acesso, o manuseio, o transporte e o armazenamento das informações prisionais. Esse fato propicia o aumento das vulnerabilidades e riscos, podendo causar danos críticos às unidades prisionais.

Para abrandar estes riscos, é necessária a implantação de normas que visam garantir a integridade, confidencialidade e disponibilidades da informação. As normas ISO/IEC 17999/2005 e ISO/IEC 27001/2005 fornecem orientações sobre a gestão da segurança da informação de maneira geral. A resolução SAP-144/2011 e a lei federal 12.527/2011 retratam as diretrizes que vinculadas às normas, especificam as políticas de segurança da informação em unidades prisionais.

O estudo de caso deixa clara a importância de uma política de segurança da informação nas unidades prisionais, pois a partir dela, é possível conhecer os principais riscos e ameaças à informação, e inserir procedimentos que garantam os princípios básicos da segurança da informação.

O resultado do estudo de caso revela que o fator humano é crucial para a definição dos procedimentos da política de segurança da informação. A política deve esclarecer o papel e as responsabilidades dos colaboradores para garantir a proteção da informação, e obter resultados satisfatórios.

O estudo das referências bibliográficas e do estudo de caso comprovam que as unidades prisionais estão expostas às vulnerabilidades e às ameaças da segurança da informação, que devem ser sanadas de maneira eficaz e eficiente, com a implementação de uma política que garanta a segurança da informação.

REFERÊNCIAS

ABNT ISO/IEC 17799: Tecnologia da informação – Técnicas de segurança – código de práticas para gestão da segurança da informação.Rio de Janeiro, 2005.

ABNT ISO/IEC 27002: Tecnologia da informação – Técnicas de segurança – código de práticas para gestão da segurança da informação.Rio de Janeiro, 2005.

CASA CIVIL; Subchefia de Assuntos Jurídicos: Lei Nº12.527, 2011. Disponível em <http://www.pmmsama.sp.gov.br/wp-content/uploads/2013/09/lei_12527-2011_acesso_as_informacoes_publicas.pdf> acesso em 21 de setembro de 2013.

FERREIRA, F; ARAUJO, M; Política de segurança da informação.Rio de Janeiro: Ciência Moderna, 2008.

FONTES, E; Praticando a segurança da informação. Rio de Janeiro: Brasport, 2008.

FONTES, E; Segurança da informação: o usuário faz a diferença. São Paulo: Saraiva, 2006.

ISO 27799:2008; *Health informatics – Information security management in health using* ISO/IEC 27002, 2008. Disponível em < http://www.iso.org/iso/catalogue_detail?csnumber=41298> Acesso em 02 de novembro de 2013.

JORDÃO, R; Acesso à informação pública: uma introdução à lei 12527, de 12 de novembro de 2011. Brasília: GCU – Imprensa nacional, 2011.

JUSBRASIL; Publicação do diário oficial do dia 30 de junho de 2010- resolução SAP-144. Disponível em <http://www.jusbrasil.com.br/diarios/6190364/pg-18-executivo-caderno-1-diario-oficial-do-estado-de-sao-paulo-dosp-de-30-06-2010> acesso em 22 de setembro de 2013.

MACEDO, D; Políticas de Segurança da informação, 2012. Disponível em <http://www.diegomacedo.com.br/politicas-de-seguranca-da-informacao/> acesso em 22 de setembro de 2013.

MANZI, F. M; RIP-Regimento Interno Padrão, 2010. Disponível em <http://www.conhecadireito.com.br/wp-content/uploads/downloads/2012/06/Regimento_interno_nas_unidades_prisonais.pdf> acesso em 22 de setembro de 2013.

PALACIO DO PLANALTO; Lei federal 12527 de 2011. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> acesso em 10 de setembro de 2013.

SECRETARIA DE ADMNISTRAÇÃO PENITENCIARIA, 2013. Disponível em < http://www.sap.sp.gov.br/> acesso em 09 de outubro de 2013.

SÊMOLA, M; Gestão da segurança da informação. Rio de Janeiro: Campus, 2003.

PRODESP; Tecnologia da informação, 2013. disponível em < http://www.prodesp.sp.gov.br> acesso em 09 de outubro de 2013.

APÊNDICE A – Formulário de pesquisa

Questionário de estudo de caso

1- Como você acessa a rede de computadores da Unidade?
( ) Eu possuo um login e uma senha para acessar a rede.
( ) Eu não possuo um login e uma senha, então utilizo a senha de outra pessoa
( ) Não preciso de login e senha para utilizar a rede de computadores
( ) Eu não utilizo a rede de computadores

2- Você costuma travar seu computador ao se ausentar?
( ) Nunca travo meu computador ao me ausentar
( ) Às vezes, quando vou me ausentar por um longo período, como por exemplo o almoço
( ) Sempre travo meu computador ao me ausentar nem que seja por breves períodos
( ) Não sei como travar meu computador

3- Onde você costuma salvar seus documentos?
( ) Na área de trabalho
( ) Em uma pasta compartilhada na rede
( ) Em Meus Documentos
( ) Pendrive
( ) Não salvo meus documentos

4- À quais informações carcerárias você tem acesso? (Você pode marcar mais que uma alternativa)
( ) Informações pessoais sobre os detentos
( ) Informações pessoais sobre os funcionários
( ) Informações sobre transferências e/ou apresentações judiciais de detentos
( ) Informações administrativas da Unidade
( ) Informações da área de saúde dos detentos
( ) Não possuo acesso a nenhuma das informações acima

5- Se você tem acesso à alguma das informações acima citadas (questão 4), você pode alterá-las ou excluí-las do sistema quando necessário?
( ) Sim, posso alterá-las ou excluí-las
( ) Tenho acesso, porém não posso alterá-las nem excluí-las do sistema
( ) Não possuo acesso a nenhuma das informações acima

6- Imagine que você receba um telefonema de uma pessoa dizendo ser da coordenadoria das unidades prisionais solicitando informações, você:
( ) passa as informações solicitadas sem pestanejar
( ) pergunta qual o interesse da pessoa e fornece a informação
( ) solicita identificação pessoal da pessoa e depois fornece a informação
( ) nunca forneço informações

7- Com que frequência você realiza “Backup” das informações que você tem acesso?
( ) Uma vez por mês
( ) Mais que uma vez no mês
( ) Não realizo “Backup” das informações
( ) Não sei o que significa “Backup”

8- No seu ponto de vista, cite três falhas de segurança da informação que você reconhece no seu ambiente de trabalho:
_____
_____
_____