

# SEGURANÇA UMA QUESTÃO DE PREVENÇÃO

Fernando Rodrigues

*Universidad Pontificia de Salamanca*

*Calle Compañía, Salamanca, 37002 España*

*Paseo de Juan XXIII, 3, Ciudad Universitaria, 28040 Madrid, España*

[fernando.rodrigues@postgrado.upsam.net](mailto:fernando.rodrigues@postgrado.upsam.net)

*Universidade Autónoma de Lisboa*

*Palácio dos Condes do Redondo, Rua de Santa Marta, 56, 1169-023 Lisboa, Portugal*

[frdrigues@ual.pt](mailto:frdrigues@ual.pt)

## ABSTRACT

Es intención de este artículo contribuir para un mejor acuerdo de la seguridad física y lógica de las tecnologías de la información y comunicación (TIC), caracterizando los mecanismos de la seguridad que son apoyados por tecnologías y herramientas apropiadas, garantizar a protección de los datos y de la información, dinamizando la credibilidad del conocimiento. Esta realidad permitirá identificar algunas tendencias actuales del mercado. Implica mecanismos, tecnologías y herramientas de la seguridad, la ayuda y la definición de una política de la seguridad en las organizaciones, la realización de las tareas de monitorización y auditoria y el concepto e instalación de las soluciones de la seguridad. Aspectos básicos como confidencialidad, la integridad y la disponibilidad que implican los sistemas de información se evidencian por un modelo conceptual que se sugiera.

## KEYWORDS

Segurança, conhecimento, confidencialidade, integridade, disponibilidade, sistemas de informação.

## 1. INTRODUÇÃO

Toda e qualquer organização tem necessidade de proteger os seus recursos. Sejam eles, humanos, materiais ou tecnológicos. A segurança dos dados e da informação reveste-se da maior importância pois determina o conhecimento necessário para pensar a sociedade, os negócios e as actividades de uma forma global em tudo aquilo que directa ou indirectamente possa dar acesso a vantagens competitivas. É, pois, absolutamente vital desenvolver princípios, modelos e metodologias que antecipem e previnam vulnerabilidades na implementação da segurança nas Tecnologias de Informação e Comunicação (TIC). No entanto a segurança informática, sendo uma questão de prevenção, é sempre um risco que tem de ser resolvido, não em termos técnicos, mas sim com base no bom senso. A preocupação com a segurança e o bem estar dos recursos tem início no que é tangível e objectivo. Esta criticidade de crescente importância a nível global deve ser ajustada e adaptada caso a caso dados os riscos que uma organização está permanentemente sujeita. A ausência ou escassa implementação de políticas efectivas pode determinar situações muito desagradáveis. Estes princípios deverão ser apropriados às organizações em causa, permitindo uma base consistente na aplicação de decisões, envolvendo a segurança física e lógica, modelos que poderão ser bastante técnicos mas experimentados, metodologias que devem ser testadas contribuindo para a defesa da missão e responsabilidade social de todos os intervenientes.

## **2. A IMPORTÂNCIA DA SEGURANÇA NAS TIC**

Na maior parte das empresas e organizações, constata-se a ausência de uma função, formalmente definida a nível organizativo, responsável pela segurança da informação (não apenas informática) e dos aspectos que com ela estão relacionados: política de segurança, definição de responsabilidades, normas e procedimentos internos e externos, entre outros. A ausência daquela função revela-se no espaço empresarial como uma lacuna significativa, tanto mais que a sua carência produz os seguintes efeitos indesejados:

- as medidas de segurança existentes são resultado, em muitos casos, da improvisação e intuição, sem fazer parte de um esquema global e coerente no seu conjunto;
- a falta do mencionado esquema global, potencia que as medidas existentes deixem lacunas incobertas, podendo transmitir-se uma falsa ideia de segurança;
- em teoria, esta situação poderia permitir a existência de medidas redundantes, o que faria com que fossem corridos riscos de ineficiência nalgumas áreas, enquanto outras não ficavam suficientemente protegidas.

A segurança de um equipamento, rede ou sistema de informação abrange diversos aspectos complementares (ex.: autenticação de utilizadores, encriptação da informação transmitida), que usam um conjunto diversificado de mecanismos de segurança. Esses mecanismos existem para fazer face a ameaças com diversas origens ou motivações, capazes de causar danos que poderão ser mais ou menos elevados.

A determinação do nível de segurança a implementar deve ter em conta os riscos associados à quebra de segurança, os custos de implementação dos mecanismos de segurança necessários à minimização de riscos e os respectivos benefícios. Desse balanço resultará um conjunto de soluções que suportarão uma dada política de segurança.

Em face do exposto, as organizações deverão ter consciência absoluta da necessidade da criação de um Plano Global de Segurança (P.G.S.) que deverá estar assente em três permissas fundamentais:

- ⇒ a segurança não é um problema tecnológico, mas humano e de organização (a tecnologia é apenas uma ajuda). Constitui um erro muito frequente a adopção de planos de segurança nos quais a única tarefa a que é dada importância consiste na implementação de medidas informáticas;
- ⇒ a segurança da informação é algo que transcende o ambiente meramente informático e deverá ser uma área distinta da actividade da organização mas transversal em todas as suas divisões. Neste sentido, o citado plano deverá ser um projecto global que envolverá toda a organização;
- ⇒ a necessidade de segurança da informação deverá ser assumida e impulsionada pela administração / gestão de topo da organização. É ao mais alto nível que se fixa a estratégia e as grandes linhas mestras a seguir. Além disso, a segurança não se consegue num acto imediato. É necessário o apoio e empenho de todos para que venha a ser efectiva a todos os níveis organizacionais e empresariais.

O **P. G. S.** é um processo que visa elevar a segurança da organização para o nível requerido pela mesma através da introdução de medidas que permitam reduzir a exposição a todos os riscos presentes previamente definidos. Este processo implica a aceitação de determinados riscos (reduzidos ou de impacto inferior ao custo das medidas necessárias à sua redução), a transferência de outros riscos (por exemplo, através da contratação de um seguro) e a redução dos riscos cuja probabilidade de ocorrência e/ou impacto estejam acima do limite definido.

Para garantir que este plano se encontra de acordo com os objectivos de responsabilidade social da empresa, de modo a contribuir para um desenvolvimento sustentável, trabalhando para e com os empregados, as suas famílias, a comunidade local e a sociedade como um todo para melhorar a sua qualidade de vida, é necessário identificar antecipadamente o nível de segurança pretendido pelos seus responsáveis.

### **2.1 Criação do Plano de Segurança**

A segurança informática empresarial é norteada por um conjunto de documentos que conferem consistência e exequibilidade às medidas implementadas. Estes documentos são o Plano Global de Segurança, a Política de Segurança, as Normas de Segurança e os Procedimentos de Segurança que a seguir se descrevem.

### **2.1.1 O Plano Global de Segurança (P.G.S.)**

O **P.G.S.** é o documento principal da segurança na Empresa. É neste documento que se irá encontrar a análise de risco da Empresa, a estratégia e o plano de acção para a implementação das medidas. O **P.G.S.** visa garantir a protecção das pessoas, informação e instalações contra as ameaças quotidianas, bem como a continuidade do negócio da Empresa face a desastres de impacto regional ou a um nível mais reduzido.

### **2.1.2 A Política de Segurança**

A Política de Segurança é um conjunto reduzido de regras que definem, em linhas gerais, o que é considerado pela Empresa como aceitável ou inaceitável, contendo ainda referências às medidas a impor aos infractores. Esta “política” deverá referenciar todas as outras políticas existentes na Empresa que contenham regras de segurança, bem como fazer alusão às Normas de Segurança. Toda a informação armazenada, transmitida ou processada pelos sistemas de informação da Empresa é propriedade dessa empresa. Para permitir a utilização rigorosa das políticas, as regras incluídas deverão ser numeradas e específicas. Acesso remoto, uso aceitável do acesso à Internet e do correio electrónico, ligação à rede, entre outros dispositivos móveis, são meros exemplos que todos os colaboradores deverão ter conhecimento.

### **2.1.3 As Normas de Segurança**

As Normas de Segurança são documentos compostos por todas as regras de segurança da Empresa, concretizando em detalhe as linhas orientadoras estabelecidas na Política de Segurança.

É neste documento que deverão estar referenciadas as tecnologias utilizadas na Empresa e a forma segura de as utilizar. Tome-se como exemplo a necessidade dos sistemas operativos deverem, sempre que tal seja possível, ser configurados por forma a impedir a instalação de software pelos utilizadores.

### **2.1.4 Os Procedimentos**

Um procedimento é um documento que descreve uma operação de forma muito detalhada, ou seja, indicando todos os seus passos. Este tipo de documento poderá sofrer alterações frequentes e, tipicamente, não é escrito unicamente por causa da segurança, pelo que deverá ser feito um trabalho de sensibilização junto dos técnicos da Empresa no sentido de que estes garantam a conformidade dos procedimentos por eles escritos com as Normas de Segurança.

É por conseguinte, nestas principais linhas de orientação que o mencionado Plano deverá desenvolver-se. O objectivo básico é proteger o “activo informação” gerando conhecimento e proporcionando uma adequada segurança desse activo em todas as funções da organização, para todas as formas e em relação a todos os seus requisitos de confidencialidade, integridade e disponibilidade.

Em termos de implementação, e sua articulação, concentrar-se-ão as seguintes tarefas:

2.1.4.1. Criação da função de gestão da segurança da informação, definição da missão e atribuição de responsabilidades;

2.1.4.2. Definição e divulgação de uma política de segurança da informação, identificação de funções, responsabilidades, desenvolvimento de procedimentos e normas para todas as funções da instituição envolvidas, assim como para todos os utilizadores externos que estejam ligados aos sistemas informáticos da organização;

2.1.4.3. Desenvolvimento e implementação de um sistema de classificação dos dados da entidade com base na sua confidencialidade (p. exemplo: restrito, confidencial, de uso interno, de uso público). Definição dos tratamentos associados a cada um dos graus de confidencialidade (p. exemplo: armazenar em caixa-forte, enviar por mensageiro, criptografar para transmitir);

2.1.4.4. Estabelecimento de uma classificação de utilizadores internos e externos com base nas suas necessidades de acesso à informação disponibilizada pela organização;

2.1.4.5. Desenvolvimento de um programa de consciencialização de todo o pessoal da organização e, caso existam, dos utilizadores externos;

2.1.4.6. Definição da política de seguros que melhor cubra os riscos associados ao “activo informação”, com base nos níveis de segurança que sejam considerados economicamente adequados;

2.1.4.7. Definição, implementação e manutenção de um Plano de Continuidade de Negócio para fazer face a situações de interrupção das capacidades do serviço informático;

2.1.4.8. Realização periódica de auditorias à segurança da informação. No caso de serem realizadas por pessoal interno, dever-se-à considerar que o referido pessoal deve estar funcionalmente separado do departamento de informática, por forma a respeitar a independência da equipa de auditores.

## **2.2 Objectivos da Segurança nas TIC**

Conforme as TIC se vão tornando o principal suporte de certas actividades de investigação, industriais, tecnológicas, administrativas, maior deverá ser a preocupação com as questões de segurança. Independentemente das acções de sabotagem, terrorismo, ameaças, riscos, assiste-se em Portugal e um pouco por todo o mundo, a algum desleixo das organizações sobre esta matéria.

A nível empresarial, esta situação deve-se normalmente a uma excessiva pressão sobre os Departamentos de Informática na promoção de melhores soluções ao nível do Software Aplicacional para responder aos objectivos de negócio sendo descuradas com frequência as áreas estritamente técnicas como a Administração de Sistemas dado não ser visível o resultado dos trabalhos desenvolvidos.

Neste contexto, basicamente podemos dividir a segurança nas TIC em duas grandes áreas:

- Segurança Física – compreende problemas relacionados com infra-estruturas (localização, estrutura das instalações, energia eléctrica, climatização, controlo de entradas e saídas, entre outros);

- Segurança Lógica - trata do controlo lógico de acessos, da segurança dos suportes lógicos, recolha, processamento e divulgação de resultados, planos de contingência, entre outros.

## **2.3 A Segurança Física**

Entende-se por Segurança Física, todos os aspectos físicos (pessoal, instalações, equipamento e manutenção) que tenham como objectivo:

a) Tratar dos dados e programas de modo a existir conformidade com a classificação de segurança dos documentos que lhe deram origem, sempre que a salvaguarda dos interesses nacionais, de países aliados, organizações públicas e privadas, e outras instituições justifiquem a sua aplicação;

b) Responsabilizar os directores dos estabelecimentos, empresas, organismos ou serviços pela protecção de dados e programas, instalações, material informático, do pessoal, das comunicações e de outras actividades contra quebras de segurança, comprometimentos e acções de sabotagem, espionagem e ainda pelo implemento de medidas que garantam a fiabilidade do equipamento e suportes lógicos, a integridade da informação e a continuidade dos trabalhos.

Na segurança física das instalações, por exemplo, são vitais:

- a) A protecção contra inundações (no caso de Centros de Informática instalados em pisos térreos, ou perto de canalizações de água ou esgotos);
- b) O correcto dimensionamento da alimentação eléctrica e suas respectivas protecções;
- c) Sendo a protecção de incêndios importante, a protecção contra radiações electromagnéticas é preocupante pois poderá gerar quebras de segurança dificilmente detectáveis dado não serem visíveis.

Para além disso muitos dos problemas de funcionamento de periféricos passa pela localização incorrecta da cablagem que fica muitas vezes sujeita a radiações electromagnéticas de outros cabos ou aparelhos eléctricos.

A localização e a estrutura das instalações são aspectos que merecem atenção. É necessário comprovar que a construção do edifício, a distribuição interna e as circunstâncias do ambiente envolvente asseguram as condições adequadas de isolamento dos sistemas informáticos.

Complementarmente, se em torno do próprio edifício estão reunidas as condições e meios adequados para um rápido acesso e intervenção a partir do exterior em caso de incêndio ou acidente grave.

A localização de um centro informático deve evitar estar condicionado às seguintes características:

- a) existir um índice acentuado de poluição atmosférica;
- b) ter interferências electromagnéticas, como linhas de alta tensão, emissores de rádio e outros;
- c) existir intensa vibração, designadamente por linhas férreas, metropolitano, e semelhantes.

Em termos de estrutura, para obter um bom nível de segurança é necessário que a sala ou salas destinadas ao computador central, sistemas envolventes e seus periféricos sejam dotados de condições mínimas funcionais.

Essas condições passam pela reunião de um conjunto de aspectos fundamentais tais como:

- evitar subsolos por causa de inundações;
- inviabilizar a localização do centro de informática nos últimos andares por causa da propagação de gases e fumos;
- anular a possibilidade de existirem janelas para o exterior sendo a iluminação artificial;
- dispor de uma única entrada;
- possuir saídas de emergência, com portas a abrir para o exterior da sala e que se abram exclusivamente por dentro;
- existir uma sala para a unidade central, equipamento crítico, unidades de controlo, equipamento que suporta as comunicações, unidades de banda e disco, colocando as impressoras e demais equipamentos que lidam com papel noutra sala;
- instalar os equipamentos de recolha em sala própria;
- permitir que a passagem dos cabos de energia e de ligação nas salas onde se instalam os equipamentos, se faça por chão ou tecto falsos, bem como a instalação de condutas e saídas para o ar condicionado;
- prever o isolamento das salas do calor e poeiras devendo as superfícies primárias (chão e tecto falsos) ser pintadas com tinta anti-poeira;
- distar a sua acessibilidade de locais de aglomeração e manifestações públicas;
- evitar imediações de bombas de gasolina, garagens, fábricas ou depósitos de ácido, depósitos de inflamáveis e corrosivos, estacionamentos;
- concretizar a construção em alvenaria, ou de aço e alvenaria;
- impedir que os canos de água e esgoto atravessem o ambiente informático;
- possuir portas e paredes que sejam resistentes ao fogo e que devam ir do chão ao tecto;
- possuir divisórias, pisos, acabamentos, tectos falsos, revestimentos acústicos que sejam de material igualmente resistente ao fogo.

### 2.3.1 Sistema de Alimentação Eléctrica

A alimentação da energia eléctrica possui uma influência considerável no funcionamento dos equipamentos informáticos, pelo que deve haver especiais diligências no seu projecto e instalação.

No caso de equipamentos de médio e grande porte, muito sensíveis, mesmo a pequenas variações, há que procurar uma potência adequada, uma qualidade e uma estabilidade que permitam um trabalho contínuo indispensável, se forem utilizados processamentos em tempo real.

Os fabricantes de *hardware* fornecem geralmente um conjunto de especificações sobre o tipo e características da rede de energia eléctrica a instalar, de forma a maximizar o rendimento desses equipamentos, pelo que estas instruções devem ser sempre tomadas em consideração.

A alimentação eléctrica deve possuir sistemas de regulação autónoma (estabilizadores) para além de eventuais esquemas de segurança adicionais, tais como geradores de corrente eléctrica e sistemas *no break*. Um centro de informática tem necessidade de energia eléctrica para além da utilizada no equipamento informático, nomeadamente a relacionada com o consumo dos sistemas de climatização, de iluminação e dos sistemas de alarme contra incêndios e intrusão.

Numa instalação eléctrica deste tipo, devem ser usadas fases distintas para os vários sistemas, que devem ser comutadas, permitindo um balanciamento da carga, bem como devem igualmente ser respeitados os regulamentos de segurança de instalações de utilização de energia eléctrica. A utilização de disjuntores com curva de disparo especial também deve ser considerada.

A instalação eléctrica corresponderá a circuitos claros com separação dos cabos por tensão e separação dos cabos de comunicações e sua blindagem. Todos os cabos devem estar etiquetados por código a definir caso a caso. Os planos de passagem dos cabos e a tabela de correspondência das etiquetas devem ficar guardados em local seguro e sempre actualizados.

Em resumo, as principais características para bom funcionamento de um sistema de alimentação eléctrico passam pela:

- existência de *no break* para manter o processamento em ambiente *real time* por ocasião de queda de alimentação na fonte de energia principal;
- accionamento de geradores para substituir a fonte de energia principal desactivada;
- operação dos estabilizadores para a manutenção da fonte de energia em condições ideais para o funcionamento dos computadores (voltagem e ciclos);
- blindagem dos cabos para evitar água e ataque de predadores;
- calhas de suporte para manter os cabos acima do chão protegidos;
- caixas de distribuição instaladas em locais seguros e fechadas;
- depósito de combustíveis para manter os geradores em funcionamento;
- verificação das terras lógicas e físicas.

Assegurar que o transporte de energia eléctrica se efectua através de instalações e com a certeza de uma manutenção regular que garantam a capacidade de processamento e a continuidade das operações da organização. Assegurar ainda assim que as contingências de uma queda de energia são tratadas de forma a que sejam minimizadas as interrupções no serviço.

Devem-se verificar ainda os aspectos de relação potência instalada/consumida, o sistema de continuidade de energia, o estado geral da instalação e ter em conta ainda em conta as seguintes considerações do tipo geral como sejam:

- as normas oficiais (comunitárias, nacionais, municipais, regionais, entre outras);
- as normas e requerimentos das companhias fornecedoras de energia;
- as recomendações da entidade reguladora do sector eléctrico;
- as instruções e recomendações dos fabricantes;
- “*standards*”;
- normas de segurança.

### **2.3.2 Controlo de Condições Ambientais**

Deverá estar comprovado que a instalação oferece garantias suficientes de funcionamento e que tem capacidade para atender às necessidades actuais e futuras.

Quase todos os médios e grandes equipamentos requerem um sistema de climatização que garanta não só um determinado nível de temperatura, com valor médio de 22° C, com um certo grau de humidade, na ordem dos 50%, sendo de toda a conveniência que estes valores sejam estáveis.

Devem ainda ser tomados em consideração os valores padrão fornecidos pelo construtor do equipamento, uma vez que os limites aceitáveis dependem do próprio equipamento. Embora os pequenos sistemas não tenham uma tão grande exigência de temperatura e humidade, devem, no entanto, enquadrar-se nos padrões ambientais normais.

Para que o sistema de climatização esteja adequado às necessidades do centro de informática, é necessário dimensioná-lo, tendo em linha de conta os seguintes factores:

- difusão do ar por condutas ou directamente;
- humidificação do ar;
- filtração do ar.

Em todos os sistemas de climatização deve existir um sistema automático de segurança que garanta a estabilidade das condições exigidas e que detecte qualquer anomalia, de modo a permitir uma rápida correcção da mesma. Os aspectos principais a contemplar são os seguintes:

- a) existência de um piso elevado ou rebaixado para facilitar a circulação do ar condicionado;
- b) climatização do ambiente, em termos de:
  - nível de poeiras;
  - temperatura ambiente;
  - nível de humidade.
- c) qualidade e capacidade das instalações;
- d) potência instalada/consumida;
- e) manutenção.

Como salvaguarda, verificam-se normalmente nestas situações que, os contratos registam garantias de fornecimento e manutenção, assim como penalizações por incumprimentos.

### **2.3.3 Segurança contra Incêndio e outros Riscos**

A respeito de incêndios, o objectivo é avaliar, se o conjunto das instalações onde está instalado o centro nevrálgico informático, se encontram protegidas de maneira eficiente e eficaz independentemente da sua origem.

O incêndio é um dos riscos mais graves, uma vez que os centros atingidos por um incêndio não conseguem retomar a sua actividade normal em tempo útil, obrigando a recorrer a complicados e onerosos processos de *backup* para substituição.

Todos os centros de informática devem estar dotados de um sistema de detecção e incêndios, providos de alarmes sonoros ou visuais que permitam uma rápida acção no sentido de os combater desde o seu início. A escolha do tipo de detector de incêndio dependerá do local a proteger. A sua instalação não se deve resumir às salas informáticas mais importantes, mas alargada aos locais adjacentes.

Para além dos meios de detecção, devem existir meios de combate a incêndio. Estes meios devem ser sistemas semi-automáticos de forma que só seja accionado o sistema de combate um certo tempo após o sistema de detecção o ter sido.

Devem ser tomadas em conta as seguintes medidas específicas de protecção contra incêndios:

- isolamento das salas dos equipamentos com paredes resistentes ao fogo de, pelo menos, seis horas;
- não utilizar materiais inflamáveis na decoração dessas salas;
- não armazenar nessas salas, materiais inflamáveis, designadamente papel e cartões;
- manutenção das salas limpas;
- colocação de extintores manuais em todo o centro de informática;
- aquisição de um sistema de detecção de incêndios para equipar o centro;
- realizar inspecções periódicas do estado de funcionamento destes sistemas de detecção;
- treino regular do pessoal, de forma a dotá-lo de uma boa capacidade de resposta em situações de emergência.

A prevenção contra incêndios é fundamental. Consta de um sistema de detecção através de sensores de fumo e calor, existência de manutenção permanente ao sistema de detecção, treino de pessoal através da formação de brigadas de incêndio, e um sistema de combate a incêndio automático ou manual e a água.

### **2.3.4 Condutas de Água, Riscos de Inundação e Prevenção**

Tal como o fogo, a água é um dos elementos da natureza que em excesso e em determinados locais pode levar a catástrofes. Comprovar as instalações e avaliar as medidas dispostas em cada caso, para prevenir e reduzir na medida do possível, os riscos derivados da água, no que diz respeito às dependências distintas que constituem o departamento de informática.

Neste contexto, cabe destacar quatro aspectos: as instalações circundantes, o próprio departamento, uma manutenção preventiva e formação do pessoal perante possíveis incidentes.

### **2.3.5 Sistema de Controlo de Acessos**

A existência de um plano geral de acessos ao centro informático, que contemple devidamente formalizadas, as normas de entrada, controle e circulação para o pessoal, quer seja interno ou externo, é uma situação que deve estar prevista. Comprovar que este plano contém os sistemas e procedimentos estabelecidos para a entrada ou saída de emergência é outra das medidas a tomar.

Os sistemas de controlo de acessos podem ser de três tipos distintos:

- a) sistemas não automáticos:
  - porteiro ou recepcionista para controlar o acesso através de identificação por bilhete de identidade, cartão da empresa ou outro documento com fotografia;
- b) sistemas semi automáticos:
  - através de interfone e porteiros electrónicos que caracterizam:
    - a redução dos recursos empregues;
    - identificação através de voz ou imagem requerente ao acesso;
    - pode ser aplicado um circuito fechado de TV.
- c) sistemas automáticos:
  - através de teclados e equipamentos de identificação combinados com suporte informático apropriado implicando:
    - diminuição dos recursos humanos;
    - utilização de cartões magnéticos e senhas;
    - identificação através de voz, impressões digitais, geometria da mão, retina, assinatura, entre outros.

O pessoal de segurança na vigilância das entradas e saídas do centro informático, deve ser confiada a pessoal devidamente credenciado e instruído, cuja missão é limitar o acesso unicamente às pessoas autorizadas e assegurar a protecção física das matérias classificadas, não devendo qualquer forma de protecção física ser considerada eficiente se não for sujeita a permanente ou à periódica fiscalização por meios humanos.

As rondas fora das horas normais de serviço devem ter a responsabilidade de verificar se a temperatura e humidade se encontram dentro dos limites impostos e se não houve violação às normas de segurança da instituição ou outras emanadas pela direcção de informática a nível de segurança.

### 2.3.6 Segurança dos Recursos Humanos

Esta situação pode ser vista como:

- a) forma de recrutamento do pessoal técnico para a área de processamento electrónico de dados;
- b) treino dos profissionais em situações de insegurança no ambiente informático;
- c) monitorização de situações agressivas aos seres humanos como:
  - necessidade de ter férias regulares;
  - acompanhamento de doenças de trabalho;
  - segregação de funções para evitar sobrecarga de trabalho;
  - estabelecimento de uma política de técnicos substitutos para evitar interrupções na continuidade operacional do centro informático;
- d) estabelecer um plano de greves para o centro informático;
- e) o responsável máximo pelo centro de informática deve designar um responsável pela segurança informática, quando este não exista, a quem competirá especialmente a aplicação e verificação das medidas de segurança que estiverem em vigor.

### 2.3.7 Segurança dos Recursos Materiais

Tal como a segurança dos recursos humanos, esta situação específica pode ser vista como:

- a) armazenagem externa de dados:
  - armazenar dispositivos de *backup* em local físico distinto do centro de informática;
  - limitar o acesso autorizado ao ambiente de *backup*;
  - realizar a reprodução periódica do *backup* para evitar dificuldades em futuras leituras;
- b) transporte de meios magnéticos:
  - realizado em dispositivos que evitem choque térmico, físico ou desmagnetização;
- c) aspectos gerais:
  - cuidados com limpeza, guarda e manuseio de equipamentos e demais componentes.

### 2.3.8 Protecção contra Radiações Electromagnéticas

Um equipamento de tratamento eléctrico ou electrónico de dados emite radiações detectáveis a grande distância, o que induz sinais eléctricos, que se propagam pelas linhas de transporte de energia eléctrica ou de transmissão. A existência de circuitos vizinhos ou condutores estranhos funcionam como sondas na zona sensível e captam sinais que comprometem o segredo das informações.

A utilização de métodos paralelos de transferência de dados a grande velocidade possibilita que as radiações emitidas por esse tipo de equipamento possam ser captadas.

Tendo em vista a eliminação das radiações emitidas e quando o grau de classificação dos dados e programas a proteger o justifique, a instalação do centro de informática deve obedecer aos seguintes requisitos:

- a) a instalação deve estar o mais próximo possível do centro do edifício ou do sector controlado, a fim de que a área de segurança, onde podem ser tomadas medidas positivas contra uma escuta clandestina, tenha um alcance mínimo;
- b) devem ser instalados filtros nas linhas eléctricas e de transmissão do equipamento;
- c) o equipamento deve estar rodeado de uma zona livre de qualquer elemento metálico, para que nenhum sinal, por contacto ou indução, seja transmitido através de estruturas metálicas exteriores, tais como os móveis, condutas, canalizações e armaduras metálicas;
- d) os circuitos, cabos e outros materiais não essenciais devem ser retirados, designadamente telefones, sistemas de intercomunicadores e campainhas, e os circuitos essenciais devem estar isolados por filtros e/ou por elementos de separação física;
- e) todas as estruturas metálicas condutoras, tais como de ventilação, canalizações, tubos pneumáticos, e outros que entram na área de irradiação, devem ser interceptadas por um elemento não condutor, instalado nos pontos de saída e de entrada de irradiação;
- f) os vidros das janelas existentes devem ser duplos e laminados com estrutura metálica.

### 2.3.9 Procedimentos Administrativos

Todas as casas-fortes ou contentores e móveis de segurança contendo matérias classificadas de qualquer grau devem possuir uma etiqueta de grandes dimensões com a palavra “Aberto” em fundo vermelho de um lado e a palavra “Fechado” em fundo verde no outro, para que permita alertar, claramente, os responsáveis para a situação em que se encontram aquelas zonas, e no exterior, em local bem visível, deve ser colocada uma relação dos nomes, endereços e telefones particulares de todas as pessoas que devem ser avisadas numa qualquer eventualidade anormal que se registre.

Para além desta etiqueta estes locais devem afixar do lado exterior, um registo, no qual a pessoa que proceder à respectiva abertura ou encerramento, inscreva a data e a hora em que esta se efectuou e a sua rubrica. Deverá igualmente existir um controlo das chaves e combinações apenas para as pessoas autorizadas, estando vedada a sua posse e utilização fora das horas normais de serviço.

As combinações dos segredos devem ser retidas em memória pelas pessoas com necessidade de as conhecer e os duplicados das chaves devem ser conservados em envelopes lacrados e confiados à guarda dos encarregados de segurança, apenas para utilização em situações de emergência.

O número de pessoas que tem conhecimento das combinações deve ser limitado ao mínimo indispensável e estas devem ser mudadas:

- quando da recepção do dispositivo de segredo do fornecedor;
- no mínimo todos os seis meses;
- sempre que haja mudança de pessoal que as conheça;
- quando se tenha verificado qualquer quebra de segurança ou se suspeite dessa possibilidade.

O acesso a toda a área de segurança, considerada crítica, deve ser definido por escrito, bem como as pessoas que o podem fazer.

As entradas e saídas de equipamento informático devem-se encontrar definidas segundo normas escritas que regulem, nomeadamente:

- saída de *hardware* para manutenção
- saída de *hardware* para outros fins (p. exemplo para apresentações)
- entrada de *hardware*
- entrada de *software* e suportes magnéticos
- saída de *software* e suportes magnéticos
- saída de *hardware* para utilização externa pelo pessoal interno

### 2.3.10 Sistemas de Detecção

A instalação de um centro de controlo de segurança que possua um sistema de informação adequado ao despoletar de equipamentos de detecção e alarme existentes na instituição, é imprescindível.

Também nesta matéria, é igualmente importante, a existência de câmaras de vídeo ou alarmes de presença em todas as entradas/saídas por forma a garantir que todos os acessos ou tentativas de acesso são detectadas. Complementarmente a ligação directa do centro de controlo aos bombeiros e serviços de protecção civil, porque em caso de emergência, como seja um incêndio ou uma inundação, a responsabilidade de contactar os serviços de protecção civil não deve depender apenas do pessoal de vigilância.

Os dispositivos de detecção de intrusos devem prever defeitos de funcionamento, ou qualquer tentativa de neutralização, pelo que o sistema deve accionar um outro sistema de alarme ou de advertência do pessoal de segurança.

A protecção contra a observação e contra a escuta são igualmente medidas a tomar. Tanto durante o dia como durante a noite, os dados e programas classificados correm o risco de ser observados. Os gabinetes e áreas onde é regularmente discutida informação com elevado grau de classificação devem ser protegidos contra as escutas, passiva e activa:

- a protecção contra a escuta passiva exige inspecções de segurança técnica e requer a insonorização das paredes, portas, janelas, telhados e soalhos;
- a protecção contra a escuta activa exige a inspecção de segurança técnica de toda a estrutura do compartimento em causa, do seu mobiliário, decoração, equipamento, material de escritório, máquinas diversas e modos diferenciados na utilização das comunicações.

As áreas protegidas do ponto de vista técnico, devem ser objecto de uma inspecção pelo menos uma vez por ano e sempre que as pessoas não habilitadas ou não vigiadas ali tenham penetrado por quaisquer razões, designadamente manutenção ou decoração.

Nenhum móvel ou material novo deve ser colocado nas áreas protegidas sem que tenha sido inspeccionado e aprovado pelo serviço de segurança. Deve também, ser evitada a colocação de telefones e, se absolutamente necessário, devem ter uma protecção adequada.

## 2.4 A Segurança Lógica

Para além das medidas de segurança física expostas, devem ser também implementadas medidas de segurança que protejam os recursos lógicos, de modo que fique claramente definido que só pode ter acesso à informação quem esteja devidamente autorizado.

Existem inúmeros processos sobre os quais interessa salientar:

- a) procedimentos de prevenção para controlo lógico de acessos:
  - associação de uma *password* a um utilizador (ou grupo de utilizadores);
  - definição para qualquer ficheiro dos privilégios de acesso para leitura e escrita e execução que cada utilizador tem sobre ele;
- b) procedimentos de detecção posteriores para controlo lógico de acessos:
  - confidencialidade do sistema informático na análise e detecção de anomalias ou infracções às regras de acesso;
  - existência obrigatória de procedimentos que registem num relatório diário os acessos realizados ao sistema informático;
- c) generalidades sobre controlo de dados:
  - a grande percentagem de erros é de origem accidental, ocorrendo durante a manipulação dos dados, quer por factores humanos, quer por deficiências do próprio equipamento ou software existente;

- a utilização de medidas e controlos incidindo sobre o pessoal e sobre os dados é obrigatória, para além da formação específica em relação ao trabalho a desempenhar e cumprimento das normas constantes da instituição;
- d) recolha e processamento dos dados e divulgação dos resultados:
  - verificação e validação na recolha de dados;
  - detecção de processamentos incompletos ou duplicados, reposição e recuperação dos ficheiros, comparação dos resultados obtidos com os resultados esperados;
  - assegurar o transporte correcto dos dados, por meios tradicionais;
  - destruir, adequadamente, toda a informação (listagens) já obsoleta;
- e) generalidades sobre segurança de suportes lógicos:
  - garantir que o *software* obedece a um mínimo de normas e de requisitos de segurança;
  - assegurar a não redundância ou proliferação do *software*;
  - proteger o *software* de roubo ou utilização abusiva;
  - assegurar que o *software* é utilizado de acordo com os termos do contrato ou outras disposições legais, o que impedirá acções de fiscalização e penalizações por uso indevido, respondendo o gestor de meios informáticos ou a administração consoante a dimensão da organização por crime e violação de direitos de autor;
- f) plano de recuperação:
  - obrigar à criação de cópias de toda a informação relevante, designadamente ficheiros, base de dados, bibliotecas de programas;
  - controlar periodicamente uma correcta aplicação dos procedimentos;
  - definir a periodicidade quanto à execução dos seguintes quatro tipos de cópias de segurança (*backups*):
    - ✓ *backups* diários – efectuam-se no final de cada período de trabalho, excepto no último dia da semana, e devem ser copiados os ficheiros permanentes criados no período diário e os ficheiros permanentes que foram alterados;
    - ✓ *backups* semanais – efectuam-se no último dia da semana. Serão copiados todos os ficheiros permanentes. Estes *backups* terão a duração de, pelo menos, uma semana;
    - ✓ *backups* mensais – correspondem ao *backup* semanal da última semana do mês e terão, pelo menos, a duração de um mês;
    - ✓ *backups* anuais – são os *backups* mensais efectuados no mês de Dezembro, que terão obrigatoriamente a duração de, pelo menos, um ano.

Ao efectuar *backups* nunca se deverá destruir a cópia imediatamente anterior, mas sim proceder à rotação dos suportes, de modo a garantir uma efectiva reposição da informação.

O número de gerações que se deverá manter depende, nomeadamente, do carácter estratégico da informação, do seu volume, da frequência de actualização e da necessidade dos utilizadores em matéria de rapidez de reposição, após detecção de uma situação de erro ou avaria.

Para ficheiros contendo informação classificada deve-se efectuar *backups* duplos, pois é sempre possível durante uma recuperação de informação ocorrer o mesmo incidente ou ocorrer um outro incidente que destrua a protecção. Se existir outra cópia de segurança, deve localizar-se fora do perímetro do centro informático.

A elaboração de um manual com os procedimentos a seguir, de modo a recuperar a informação a partir das cópias de segurança, o controlo periódico para verificar o cumprimento das normas estabelecidas para a protecção da informação, se os suportes contendo os *backups* se encontram em condições físicas de ser utilizados e se o esquema de cópia e procedimentos estabelecidos permitem a recuperação efectiva em caso de avaria ou acidente grave, são também tarefas a respeitar.

- g) plano de reposição:

- recorrer a normas que permitam repor o bom funcionamento do sistema, sempre que tenha ocorrido uma interrupção ou avaria, de forma a reduzir ao mínimo os danos do equipamento e a não provocar grandes perturbações aos utilizadores;
- aplicar essas normas sempre que surjam incidentes do seguinte tipo:
  - ✓ avarias no equipamento
  - ✓ avarias de climatização ou de energia eléctrica
  - ✓ avarias ou erros nas comunicações
  - ✓ erros de programação ou de exploração
  - ✓ destruição de ficheiros
  - ✓ ausência de pessoal

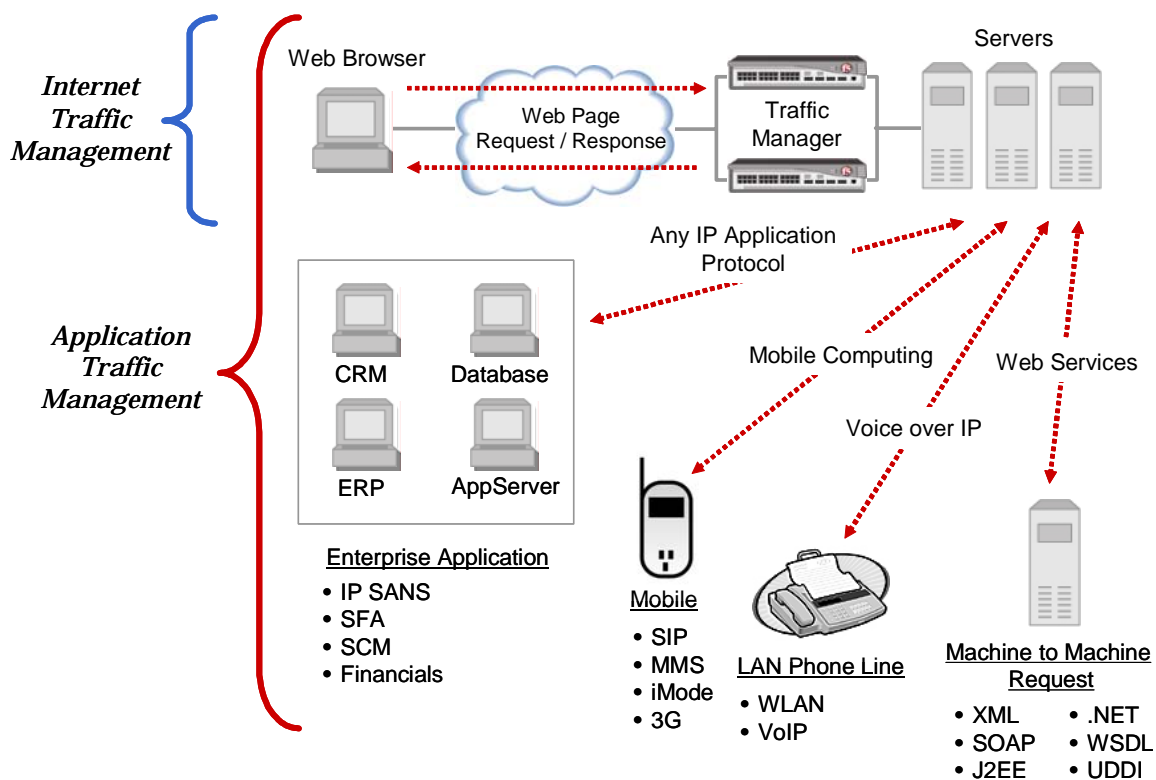
Os procedimentos que integram as normas de reposição estão geralmente descritos nos dossiers de exploração e referem-se, nomeadamente, a recuperações após cancelamento de um programa, reposições de ficheiros, modificações na configuração de determinado equipamento, entre outros.

É conveniente a realização de auditorias informáticas periódicas que tenham como objectivo analisar, avaliar e recomendar se a actividade desenvolvida, cumpre adequadamente as condições que lhe são exigidas. Esta actividade deve confirmar, ou não, a existência de erros, omissão, duplicidade, falta e/ou fraude, quer se trate de procedimentos, quer sejam resultados.

## 2.5 Modelo Conceptual

Um modelo conceptual para uma relação directa entre a segurança física e lógica, envolvendo os recursos humanos, materiais e tecnológicos, deverá ser adaptado, testado e implementado de acordo com as tecnologias actuais e emergentes (figura 1). Este modelo foi conceptualizado com base na criticidade que os sistemas de informação exigem, suportados por soluções independentes e numa perspectiva pessoal do autor. Futuras pesquisas, investigações e metodologias deverão ser requeridas para validar este modelo.

Figura 1. Segurança uma questão de prevenção



## 2.6 Tendências de mercado

As ameaças à informação, são assim e em resumo, cada vez mais um risco potencial no negócio de qualquer actividade. A segurança absoluta de um sistema informático é algo que, do ponto de vista prático, é impossível.

Um “intruso” mesmo não tendo capacidade para analisar ou alterar a informação armazenada num sistema, pode impedir os utilizadores autorizados de o usarem efectivamente, sobrecarregando-o.

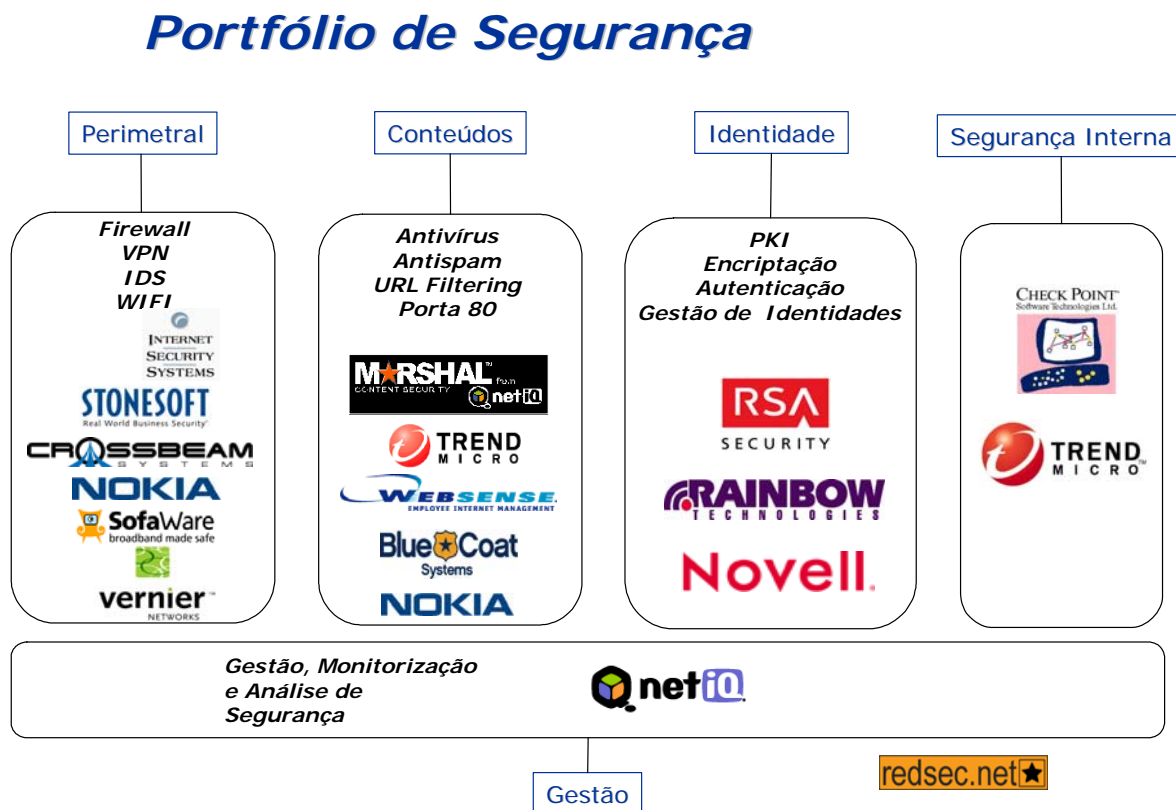
Impedir que isto aconteça é, também, função da segurança informática.

As TIC representam um verdadeiro desafio à segurança. A sua expansão, a melhoria na oferta de serviços, a flexibilidade na sua utilização, fazem da segurança, uma tarefa árdua. Vejamos alguns exemplos:

- Assiste-se a uma transição de produtos para serviços
- *Appliances* dedicadas e optimizadas para cada função
- Segurança Móvel (Wireless)
- Segurança ADSL
- Sistemas biométricos, tokens e Smart Cards para autenticação
- Implementação progressiva de firewalls virtuais
- Migração de soluções de antivirus para implementações de servidores e antispam

A envolvente tecnológica é, neste contexto, absolutamente essencial. Os mecanismos e ferramentas de segurança que envolvem os recursos humanos, materiais e tecnológicos, deverá estar suportado por plataformas independentes conjugadas com as melhores soluções existentes no mercado (figura 2).

Figura 2. Plataformas e soluções possíveis



### 3. CONCLUSÕES

Este artigo tem como intenção proporcionar um melhor entendimento da segurança como uma questão de prevenção possibilitando às organizações uma melhor eficiência e eficácia no que diz respeito às inúmeras soluções existentes adaptáveis e escaláveis para os seus problemas competitivos. A segurança informática tem como objectivo proteger a informação e os sistemas que a envolvem em ambientes cada vez mais complexos promovendo a gestão e a excelência do conhecimento.

Futuras pesquisas deverão:

- Considerar que um qualquer sistema de segurança tem de ser capaz de proporcionar uma resposta satisfatória a qualquer um dos aspectos já referenciados como essenciais neste artigo;
- Evidenciar atitudes que salvaguardem a confidencialidade cujo propósito é assegurar que a informação não é visualizada por entidades ou indivíduos não autorizados;
- Aprofundar procedimentos que envolvam a integridade assegurando que a informação disponível num sistema não é modificada por entidades ou indivíduos não autorizados;
- Incluir pesquisas e validações que documentem a disponibilidade que deverá ser entendida como a capacidade de os utilizadores autorizados fazerem uma utilização efectiva dos sistemas de informação sem barreiras nem limitações.

Este desenvolvimento com base numa metodologia apoiada em ferramentas inovadoras permitirá um maior e melhor alinhamento estratégico das organizações no que diz respeito à segurança. Os custos da inteligência não têm preço. Trata-se somente de desafios ao desempenho.

### REFERÊNCIAS

- Aldegani, G., (1993) *Seguridad Informática*, MP Ediciones, Uruguay.
- Bruce, G. et. al., (1997) *Security in Distributed Computing: Did You Lock the Door?* Prentice-Hall PTR, Alberta.
- Carneiro, A., (2001) *Auditoria de Sistemas de Informação*, FCA-Editora em Informática, Lisboa.
- Carneiro, A., (2002) *Introdução à Segurança dos Sistemas de Informação*, FCA-Editora em Informática, Lisboa.
- Caruso, C., (1993) *A Segurança em Informática e em Redes Locais*, LTC – Livros Técnicos e Científicos, Rio de Janeiro.
- Carvalho, P. et. el., (2003) *Segurança dos Sistemas de Informação*, Centro Atlântico, Lisboa.
- Fernandez, C., (1988) *Seguridad en Sistemas Informáticos*, Ediciones Díaz de Santos, S.A., Madrid.
- Gil, A. L., (1998) *Auditoria de Computadores*, 3.ª ed., Atlas, Rio de Janeiro.
- Thomas, A. et al., (1997) *Auditoria Informática*, Paraninfo, Madrid.