CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Tecnologia em Segurança da Informação

Luidson Lucas Bortolatto

CONTROLES DE ACESSO LÓGICO: Buscando soluções para evitar o compartilhamento de senhas entre usuários

Americana, SP
2014

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Tecnologia em Segurança da Informação

Luidson Lucas Bortolatto

CONTROLES DE ACESSO LÓGICO: Buscando soluções para evitar o compartilhamento de senhas entre usuários

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Segurança da Informação, sob a orientação do Prof. Esp. Edson Roberto Gaseta.

Área de concentração: Segurança da Informação

Americana, SP
2014

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Bortolatto, Luidson Lucas
B748c Controles de acesso lógico: buscando soluções para evitar o compartilhamento de senhas entre usuários. / Luidson Lucas Bortolatto. – Americana: 2014.
51f.

Monografia (Graduação de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Esp. Edson Roberto Gaseta

1.Segurança em Sistemas de informação I. Gaseta, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5
681.3.066

Luidson Lucas Bortolatto

CONTROLES DE ACESSO LÓGICO: Buscando soluções para evitar o compartilhamento de senhas entre usuários

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 25 de Junho de 2014.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Especialista
FATEC Americana

Maria Cristina da Luz Farga Moreira Aranha
Mestre
FATEC Americana

Alexandre Mello Ferreira
Mestre
FATEC Americana

AGRADECIMENTOS

Primeiramente à Deus, pela sua graça infinita, por me dar o fôlego de vida todos os dias e estar sempre presente nos momentos bons e difíceis da vida, me concedendo a força necessária para caminhar.

Ao Professor Edson Gaseta pelo apoio, e por me guiar ao longo desse trabalho e também à professora Maria Cristina Aranha pela ajuda e disponibilidade.

Agradeço aos meus Irmãos Harisson e Wellington, minha cunhada Marcela, toda a minha família e à minha namorada Vanessa pela paciência, e compreensão nos momentos em que tive que abrir mão do lazer ou descanso para me dedicar a este trabalho.

Finalmente, a todos os meus amigos que me acompanham, os professores da Fatec, e meus colegas da Turma de Segurança da Informação pelo companheirismo, dedicação e o mais importante, a amizade conquistada ao longo dessa trajetória.

DEDICATÓRIA

Dedico esse trabalho à minha mãe, pelo apoio, incentivo incondicional, e por me ensinar a nunca desistir dos meus objetivos, sendo um exemplo de luta e superação a qual tenho o privilégio de conviver todos os dias.

RESUMO

Segurança da informação e proteção de dados é um assunto muito discutido atualmente. Tanto nas empresas quanto na vida pessoal muito se fala sobre as consequências de pessoas mal-intencionadas terem acesso a informações sigilosas ou que simplesmente não caberiam a elas terem esse acesso por motivos diversos. Entre os métodos mais utilizados para proteção da informação, destaca-se a senha pessoal, muito conhecida, e aplicada nas mais diversas situações. Tratando especificamente dos ambientes coorporativos, as ações para minimizarem o acesso de terceiros a senhas pessoais são as mais diversas: Políticas de criação de senhas complexas, orientação a usuários não deixarem as senhas visíveis, ou atenção na hora de digitá-las, porém o principal problema não é técnico e sim humano. Por isso, é necessário estudar as causas e motivos que podem levar as pessoas a tomarem a ação, acabando por disponibilizar facilmente seus acessos a outras, e buscar soluções para se evitar esse comum descuido com algo tão seguro, se bem utilizado, no controle de acesso à informações.

Palavras Chave: Segurança da Informação, senha, biometria.

.

ABSTRACT

Information security and data protection is a widely discussed issue currently. Both in business and in our personal lives much is said about the consequences of ill-intentioned people have access to sensitive information or who Would not fit to them having this access for any reasons.Among the methods used for protection of information, there is the personal password, well known and applied in different situations. Considering specifically the corporative environments, actions to minimize third party access to personal passwords are the most divers: Policies for creating complex passwords, orientation to users not leave passwords visible, or attention in moment to enter them,but the main problem is not technical but human.Therefore it is necessary to study the causes and reasons that can lead people to take this action, eventually readily available its access to other, and search solutions to avoid this common oversight with something as safe, if properly used, the access control information.

Keywords: *Information Security, password, biometrics.*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CES – *Consume Eletronics Show*

ERP - *Enterprise Resource Planning*

EUA – Estados Unidos da América

OS – *Operating System*

PIN – *Personal Identification Number*

PWC – *Pricewaterhousecoopers*

RH – Recursos Humanos

RG – Registro Geral, Célula de identidade

SI – Segurança da Informação

TI – Tecnologia da Informação

TSE – Tribunal Superior Eleitoral

SUMÁRIO

INTRODUÇÃO

A busca por métodos de proteção às informações têm se intensificado cada vez mais nas empresas. Muitos investimentos são realizados em equipamentos de *firewall*, sistemas de proteção, antivírus, restrição de acesso à redes externas, treinamento de profissionais para especialização na área de segurança, métodos de criptografia de arquivos, buscando uma proteção cada vez maior do ativo mais importante da empresa: Informação.

Dawel (2005) cita que o grande esforço das empresas na busca pela eficácia da Segurança da Informação, através da aquisição de produtos e serviços que auxiliam na proteção, se concentram na busca por proteção de ameaças externas.

Porém apesar desses investimentos serem importantes, é necessário que a organização dispense uma grande atenção ao seu ambiente interno, já que as ameaças podem estar dentro da própria empresa, e essas ameaças, em muitos casos podem não ser proporcionadas por algum recurso tecnológico, e sim humano, ou seja proveniente das pessoas que lidam diariamente com informações vitais para o negócio da empresa.

O usuário é a última parte de todo o processo para se obter a segurança adequada. As empresas que não derem importância a este fato, mesmo que usem outros recursos poderão não obter a proteção efetiva para seu ambiente. (FONTES, 2008).

Por mais que a empresa invista em proteção para sua rede, e consequentemente para os seus dados, se os próprios mantenedores da informação, os usuários que lidam diariamente com elas não tomarem as devidas medidas, não forem devidamente orientados, ou não mostrarem muita preocupação com o assunto, esse bem tão importante para a organização continuará a ter possibilidades altas de acabar caindo na mão de pessoas indevidas (FONTES, 2006).

Um dos pontos que fazem parte da luta dos profissionais de segurança da informação, e que pode trazer consequências tanto para a empresa quanto para o

usuário é o compartilhamento de senhas entre usuários. Essa prática está presente em muitas empresas, em que usuários que não têm, e/ou não deveriam ter acesso, acabam utilizando o *login* e senha de uma pessoa que possui os acessos que necessitam.

O próprio Fontes (2008, p. 123) afirma:

> O comprometimento do usuário é uma atitude fundamental para o sucesso de proteção da informação. Podemos ter o melhor controle de acesso lógico, porém será de pouca valia se é comum na organização o usuário emprestar sua senha para outro ou ausentar-se do local onde está o seu computador e o mesmo não possui uma proteção de tela.

Essa afirmação reitera a importância dos profissionais da área de segurança ficarem atentos a estes detalhes que podem, em alguns momentos até passar despercebidos, porém merecem grande atenção.

Algumas empresas alertam seus funcionários, informando que seus usuários e senhas de acesso ao ambiente de rede e/ou sistema são pessoais e intransferíveis, e recomendando que não compartilhem senhas com terceiros, porém apenas a orientação não é o suficiente. É necessário, também procurar reduzir as chances dos usuários compartilharem seu *login* de acesso, buscando soluções tecnológicas, didáticas e humanas para essa questão. Desse modo, justifica-se a realização desse trabalho vulnerabilidade causada pelo compartilhamento de senhas, oferecendo risco de acesso não-autorizado às informações importantes da empresa.

Esse trabalho busca, de uma forma geral destacar o usuário e sua influência no processo de Segurança da Informação, no que diz respeito ao compartilhamento de *login* de acesso e senha entre os usuários, tendo como objetivo, de forma mais específica sugerir soluções que podem ser utilizadas pela área de TI e Segurança da Informação, em conjunto com a área de negócio na tentativa de conter o acesso não-autorizado às informações da empresa e, através de ações do estabelecimento de políticas de Segurança da Informação, orientação dos usuários e melhoria dos métodos de autenticação mitigar esse problema de compartilhamento de senhas, cuja prática pode trazer malefícios para os usuários e também ao negócio da empresa.

2 INFORMAÇÃO: UM ATIVO VALIOSO PARA A ORGANIZAÇÃO

Nos últimos anos, o tema “Segurança da Informação” tem deixado de ser um assunto de conhecimento apenas de profissionais de Tecnologia da Informação, e tem cada vez mais se estendendo ao conhecimento do público através dos meios de comunicação.

São casos que têm se tornado cada vez mais comuns no dia-a-dia, e que incluem desde a invasão de privacidade de pessoas famosas até os casos recentes de espionagem do governo norte-americano, assunto muito discutido no Brasil nos últimos meses.

No âmbito empresarial, a informação é definida, de acordo com Fontes (2006, p. 2) como “um mecanismo crítico para se alcançar os objetivos do negócio e o cumprimento da missão da empresa. Devendo, assim como todo recurso que é importante para a empresa ser protegida contra possíveis riscos de perda. ”

Pensando nisso, as empresas têm se preocupado cada vez mais em garantir os três pilares da segurança da informação que, segundo FONTES (2006) é composto pelos atributos: disponibilidade, integridade e confidencialidade da informação.

A disponibilidade garante que a informação estará acessível quando necessário para o funcionamento da organização. A Integridade assegura que as informações estão íntegras, ou seja os dados são corretos e não foram manipulados ou alterados, enquanto que a Confidencialidade busca garantir que a informação deve e será acessada apenas pelos que necessitam da mesma para a realização de suas atividades.

Essa preocupação tem feito com que os investimentos na área de Segurança tenham um aumento significativo. De acordo com a pesquisa global de segurança da informação, (PWC, 2014), os investimentos na área aumentaram 51% em 2013, em relação com o ano anterior. Segundo essa pesquisa, os avanços obtidos pelas empresas na área de investimentos em segurança da informação são expressivos, e vêm, inclusive obtendo a atenção e importância por parte dos executivos responsáveis

pelas organizações o que faz com que esses executivos tenham melhorado de forma significativa os processos e estratégias que envolvem a área de segurança da informação nos últimos anos.

Isso ratifica a importância da Segurança da Informação e proteção dos dados no ambiente empresarial. Porém, para que os procedimentos de segurança da informação sejam executados de forma eficaz, existe a necessidade da participação dos colaboradores e prestadores de serviço, inclusive dos executivos da organização afinal, a proteção da informação é uma atitude essencial para a continuidade dos negócios da empresa. (FONTES, 2008)

Por isso deve ser dispensada uma grande atenção às pessoas que trabalham na empresa (Vide apêndice A), já que, conforme afirma Fontes (2008), as pessoas constituem um dos elementos fundamentais para os negócios da empresa, e são essas pessoas que manuseiam a informação diariamente na empresa, e que devem ter consciência da importância de seu papel na contribuição com a conservação, e proteção dos dados da corporação.

2.1 O USUÁRIO E A SEGURANÇA DA INFORMAÇÃO

Os usuários que utilizam os recursos da empresa e trabalham diariamente com as informações do negócio, sendo eles funcionários efetivos, estagiários ou terceiros são ponto chave no processo da segurança e proteção das informações da organização.

Está claro que a área de TI tem grande responsabilidade em implementar, revisar, modificar, e informar sobre as normas e procedimentos de segurança. Porém quem, efetivamente lida com dados importantes da empresa são os usuários, e é de extrema importância que estes estejam comprometidos com o processo de segurança e proteção dos dados da empresa.

Lembrando os conceitos apresentados por Fontes (2008, p. 125), sobre a importância do papel das pessoas nos negócios da empresa, pode-se dizer que esta importância é classificada quanto aos seguintes aspectos:

- A administração da organização é realizada pelas pessoas, por isso o processo de segurança da informação deve ser de conhecimento dessas pessoas e estar devidamente inserida nos objetivos gerais da organização;

- O desenvolvimento e operação dos sistemas e execução dos processos é feito pelas pessoas, sendo assim a consciência quanto a segurança dos dados deve existir desde o desenvolvimento até a execução dos softwares e processos;

- São as pessoas que até podem pensar em proteger seu computador, se esquecendo, porém, de outras informações como papéis importantes em cima da mesa, ou discussões verbais em locais inapropriados, que podem ocasionar a divulgação de informações sigilosas;

- As pessoas podem ser vítimas de tentativas de fraudes ou técnicas de engenharia social de pessoas mal-intencionadas;

- Os regulamentos podem ou não ser cumpridos pelas pessoas, ou seja, as regras são criadas, porém podem ou não serem seguidas por parte dos usuários, seja intencionalmente ou não;

- As pessoas podem divulgar e fazer com que o conceito de Segurança da Informação se espalhe por todo o ambiente corporativo;

- A superação de expectativa de rendimento, quando ocorrem, é provocada pelo resultado do trabalho e esforço das pessoas;

Por esses e outros motivos, é possível tomar conhecimento, e compreender a importância do compromisso do usuário para o melhor desenvolvimento do processo de segurança da informação. Para se obter esse comprometimento de forma efetiva, as empresas buscam estabelecer normas de Política de Segurança da Informação. Diversos aspectos de segurança são abordados. Entre eles, a determinação de níveis de acesso do usuário aos recursos da empresa. (FONTES, 2008).

Entre as normas de segurança deve existir aquela que garante o acesso tanto físico como lógico à informação apenas a pessoas devidamente autorizadas, e isso é realizado através da identificação do usuário que deve ser pessoal e intransferível.

Considerando o controle de acesso lógico que pode incluir acesso aos computadores da empresa, sistemas, e outros acessos, a pessoa que utiliza o recurso deve realizar a autenticação através de um usuário fornecido por parte da TI, e uma senha que deve ser definida pelo próprio funcionário, de acordo com as regras de formação de senha, descritas na Política de Segurança da Informação da organização, portanto tornar a senha conhecida por outras pessoas é uma atitude de risco que pode comprometer todo o controle de acesso definido nessa política, burlando-a e, muitas vezes, entregando o acesso às informações nas mãos de pessoas não autorizadas.

2.2 IDENTIFICAÇÃO DO USUÁRIO

Fontes (2006) afirma que a autenticação tem por finalidade garantir a autenticidade do usuário, ou seja, garantir que a pessoa que está se identificando é realmente quem diz ser. No ambiente de TI, conforme citado por Fontes (2006) os usuários podem ser validados e autenticados através de algo que é de seu conhecimento (senha), algo que o mesmo possui (cartão inteligente ou *token*) ou por algo que o usuário é (características físicas, biometria).

Apesar dessas opções, a senha pessoal ainda é o método mais utilizado para autenticar um usuário, devido a facilidade de implantação, baixo custo, e também por ter uma segurança que pode chegar a níveis aceitáveis, conforme Fontes (2006) afirma.

Tecnicamente, esse tipo de autenticação é estritamente seguro, afinal, os sistemas só liberam o acesso se a identificação e senha informada estiverem corretos, e como a senha é uma forma de autenticação pessoal, o usuário, consequentemente só irá acessar a sua própria conta. Porém, ao considerar o lado humano, do usuário, sabe-se que toda essa segurança acaba sendo comprometida.

Segundo Ferreira e Araújo (2008), deve ser impossibilitada toda e qualquer chance do uso compartilhado de senhas. Porém, tanto em usuários de domínio quanto em sistemas cruciais nas empresas, como ERP, sistemas de controles, entre outros, as pessoas acabam compartilhando seu usuário e senha com outras pessoas sem se preocupar com as consequências e riscos que essa atitude pode gerar posteriormente.

Por mais que os dispositivos físicos, lógicos, e controles de segurança estejam corretamente implementados na rede, se o usuário não for conscientizado, e não tomar os devidos cuidados, as informações poderão estar facilmente disponíveis às pessoas que não deveriam ter o acesso.

Caso essas informações cheguem ao alcance de pessoas mal-intencionadas, as consequências poderão ser desastrosas, já que o dono da identificação poderá até ficar sem o próprio acesso, e até que essa situação seja resolvida, (comprovando sua

identidade, relatando o ocorrido, e solicitando a redefinição da senha à equipe de TI, por exemplo), a pessoa que está utilizando a conta indevidamente poderá ter causado danos irreversíveis para a empresa, e também ao real proprietário da conta.

Isso é enfatizado por Fontes (2006) que afirma que ninguém na empresa deve ter acesso à senha de um outro usuário. Fontes, inclusive reitera que algumas pessoas terão o acesso de **bloquear** ou **redefinir** a senha. Geralmente, nas empresas essa responsabilidade cabe à equipe de suporte, ou ao administrador da rede. Nessa redefinição, deve ser inserida uma senha temporária, que expire no primeiro uso, forçando o usuário a realizar a troca e inserir sua própria senha para poder continuar o acesso ao sistema.

Apesar disso, os usuários parecem não se preocupar com seu acesso, talvez em sua maior parte pela falta de conscientização, que faz com que não tenham conhecimento de que o compartilhamento de usuário e senha pode trazer problemas para si mesmo, pois o funcionário que está utilizando a conta pode acabar tomando alguma ação, intencionalmente ou não, que prejudique alguma informação da empresa, seja apagar um arquivo dos diretórios de rede, infringir alguma Política de Acesso à Internet, realizar ações no sistema ERP, como liberar a compra de materiais erroneamente, emissão de nota com valores e/ou tributações erradas, baixa no material errado do estoque, entre outros.

Essas e outras inúmeras ações que podem gerar sérios problemas no processo da empresa, seja de fabricação, compra, entrada, ou expedição de materiais, já que os danos causados serão de responsabilidade do dono da conta, considerando que através das análises dos *logs* é possível identificar o seu usuário, e o mesmo poderá estar sujeito às penalizações internas estipuladas pela área de negócio, por causa dos problemas gerados como advertência, suspensão, podendo levar, em alguns casos mais extremos, à demissão do colaborador.

2.3 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Na tentativa de encontrar soluções para a mitigação (diminuição da intensidade) do risco do uso de usuários e senhas compartilhados, o primeiro passo visando o tratamento desse risco é a criação ou revisão, caso já exista, de uma Política de Segurança da Informação.

Há empresas que alocam recursos materiais em quantidade, para proteção da rede, mas não se preocupam em adotar Políticas de Segurança da Informação coerentes com a postura geral da empresa, fazendo assim com que os recursos investidos estejam alinhados com as Políticas de SI da organização, sendo mais eficazes no processo de segurança da informação (MENEZES, 2006).

Assim vale a pena destacar a importância que uma Política de Segurança da Informação no controle e proteção dos dados não somente para a área de TI como para a empresa em um âmbito geral. Segundo Fontes (2008), a Política de Segurança da Informação é o elemento responsável por expor os critérios e regras necessárias para o uso da informação na organização.

São essas regras que esclarecerão aos usuários dos recursos de TI as condutas permitidas e também as que não são recomendadas ou até coibidas, visando sempre garantir que o bem de alto valor da empresa, denominado “informação” esteja seguro. Conforme afirmado por Araújo e Ferreira (2008 p. 36), “A política deve ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação”.

Sendo assim, deve ser bem redigida, utilizando uma linguagem compreensível para o usuário final, e, é recomendado que seja criada antes da ocorrência de problemas de segurança ou, caso não seja possível, após as ocorrências, a fim de evitar que esses problemas surjam novamente assim como reiterado por Araújo e Ferreira (2008 p. 36).

Baseando-se nessa política, os usuários terão acesso às normas, e consciência do que é permitido ou não é permitido dentro e/ou fora da empresa utilizando os recursos de TI, e cientes que com o descumprimento dessas regras os mesmos

estarão sujeitos às penalizações internas, também especificadas na Política de Segurança da Informação.

2.4 CONSCIENTIZAÇÃO E TREINAMENTO

Existindo uma Política de Segurança da Informação clara, objetiva, que o usuário consiga compreender, e entenda que não deve compartilhar sua senha, o próximo passo é, talvez o trabalho mais árduo e extenso: o de conscientizar as pessoas. Mitnick e Simon (2003), classificam o ser humano como elo mais fraco da segurança da informação. Segundo o autor,

> O único meio verdadeiramente efetivo de amenizar a ameaça da engenharia social é usar a conscientização para a segurança combinada a políticas de segurança que definem as principais regras para o comportamento do empregado, junto com sua educação e treinamento (MITNICK e SIMON, 2003, p.195).

No caso da engenharia social, o atacante utiliza de métodos de persuasão para fazer com que a vítima ceda informações que devem ser confidenciais, porém no caso da concessão de usuário e senha, o usuário acaba, espontaneamente entregando o acesso, muitas vezes sem que ninguém solicite. É muito comum, por exemplo encontrar usuários que costumam, ao sair de férias deixar suas senhas com os colegas, autorizando-os a responderem seus *e-mails*, acessarem os diretórios de rede, enfim, fazerem o que bem entenderem em sua ausência.

Outra situação que vale a pena destacar, encontra-se nos casos de suporte técnico ao usuário. Na intenção de facilitar o atendimento, algumas pessoas acabam passando suas senhas aos profissionais de TI, dando ao atendente acesso livre ao equipamento com sua própria senha.

Existem também, algumas empresas em que não há um contato físico entre o pessoal da TI e o usuário, e muitas vezes esse contato só é realizado via telefone e os usuários acabam compartilhando suas senhas por telefone, em alguns casos até citando-a em voz alta sem se dar conta de que está rodeado de pessoas que podem estar escutando a conversa, acabarem descobrindo a senha, e conseguindo o acesso ao sistema, trazer problemas ao dono da conta.

Além disso, também vale a pena citar casos em que pessoas, de certa forma forçadas pela Política de Segurança da Informação, por exemplo, criam senhas até complexas, porém com receio de esquecer, acabam por anotar em papeis, e deixar

visível em monitores, cadernos, embaixo do teclado, e outros locais que qualquer pessoa má intencionada encontraria com facilidade.

É importante que os funcionários entendam que são responsáveis pela parte da informação que manipulam, que a senha é a sua segurança, e que devem suspeitar de qualquer solicitação que envolva a divulgação de suas senhas (MITNICK e SIMON, 2003).

Para isso, há a necessidade de que os usuários sejam orientados, conscientizados através de treinamentos, que, referenciam as Políticas e Normas de Segurança da Informação na empresa.

Segundo Mitnick e Simon (2003) apenas ter uma Política de Segurança da Informação visível ao usuário, ou o acesso a documentos que informem sobre essa política não é o suficiente para que as pessoas entendam, e sigam as regras de segurança sendo necessário, através de um programa de conscientização, fazer com que as pessoas sejam influenciadas e motivadas a contribuírem de forma positiva para a eficiência do processo de proteção dos ativos da organização.

Fontes (2008) cita a responsabilidade da área de Segurança da Informação no processo de conscientização dos usuários, e que todos os funcionários, independente de seus níveis hierárquicos devem ser orientados. Fontes cita, também, que apesar de caber ao departamento de SI, é recomendado que a área de recursos humanos realize esses treinamentos, e que eles sejam parte do plano anual de treinamentos do departamento.

Assim, tanto funcionários novos quanto os que já fazem parte da organização poderão compreender a importância de proteger os dados da empresa e a parcela que cada um pode ter de contribuição para que esse processo seja realizado da melhor maneira possível. Existem diversas formas de conscientização que podem ser aplicadas aos colaboradores, as quais pode-se destacar:

1. Treinamento formal sobre a segurança da informação e a importância da proteção dos dados da empresa, e a conscientização que isso não cabe

apenas a área de TI, mas a cada manipulador de informações, que são os próprios usuários. É interessante conscientizar o usuário de sua grande parcela de responsabilidade no quesito da proteção das informações que são um bem valioso para a empresa. É importante a participação nesses treinamentos, se possível de um profissional da área de TI com um conhecimento em segurança e boa didática;

2. Feito o treinamento, pode ser realizada uma pesquisa interna entre os colaboradores, de forma a salientar que os mesmos entenderam as importâncias e responsabilidades descritas no treinamento, e também ratificar que estão colocando em prática as ações e procedimentos recomendados;
3. A equipe de segurança pode, regularmente, elaborar boletins informativos aos usuários (vide “ANEXO A”), com as Políticas de SI, e também dicas importantes, utilizando uma linguagem simplificada que podem ser aplicadas no dia-a-dia pelos funcionários da empresa. Esses boletins podem ser impressos e fixados em lugares estratégicos (Restaurante, mural de informações, nos departamentos) assim como, também pode ser utilizado o correio eletrônico.
4. Outra forma de relembrar os usuários conforme recomendado por Mitnick e Simon (2003) é a criação de lembretes de segurança que poderão aparecer ao usuário, ao ligar o equipamento. Essa mensagem não poderá ser fechada antes que o usuário confirme o recebimento e leitura da mesma. Existe no mercado ferramentas de comunicação coorporativa em que é possível enviar mensagens para todos os computadores da rede, facilitando a comunicação, e atingindo, também os usuários que não possuem *e-mail* para receberem os boletins informativos descritos anteriormente.
5. Não se pode esquecer também dos novos funcionários. Os colaboradores, conforme forem iniciando suas atividades na empresa, podem ter, em seu processo de integração, a inclusão de um treinamento sobre segurança e, também a entrega de uma cartilha desenvolvida pela equipe de segurança, com as normas e regras de segurança, e também não esquecer de informar e incluir os novos contratados na lista de recebimento dos boletins informativos de segurança da informação.

Mitnick e Simon (2003) enfatizam a importância de se ter um programa de conscientização constante. Ele recomenda, inclusive, que se evite textos parecidos nas mensagens a serem enviadas e que as mesas sejam escritas das mais diferentes formas possíveis, evitando cansar o usuário com mensagens repetidas, fazendo com que o mesmo acabe ignorando o conteúdo.

É de extrema importância que o usuário esteja ciente e comprometido com o que foi proposto nos treinamentos e boletins, ou seja comprometido com a proteção dos dados da empresa.

As pessoas precisam entender que apesar da tendência em se buscar uma forma mais fácil de realizar alguma tarefa, principalmente quando há certa pressão ou prazo se esgotando, o que geralmente inclui burlar ou ignorar os procedimentos de segurança, é preciso se conscientizar de que a segurança da informação e a busca por cumprir sua parte no processo de proteção dos dados devem fazer parte do seu dia-a-dia conforme afirmado por Mitnick e Simon (2003).

3 ALTERAÇÃO OU MELHORIA DE MÉTODOS DE AUTENTICAÇÃO

Conforme já citado anteriormente, a utilização da senha, apesar de ser o método de autenticação mais comum nos sistemas computacionais, como única forma de identificação pode tornar o sistema vulnerável, já que pode abrir espaço a alguma pessoa não-autorizada de modo que a mesma consiga o acesso, seja através de engenharia social ou por disponibilização do usuário, como reiterado nos capítulos anteriores.

Partindo do princípio já citado anteriormente, a autenticação pode ser baseada no que se conhece, no que se possui, ou nas características individuais (PINHEIRO, 2008).

Quando existe apenas a autenticação baseada no que se conhece, outras pessoas poderão ter acesso sem nenhum problema, e o sistema não será capaz de identificar se a conta está sendo utilizada por outra pessoa.

Porém quando essa autenticação é utilizada combinada a outros métodos, as chances do acesso de pessoas não-autorizadas tornam-se remotas, já que apenas o conhecimento da senha não é o suficiente. Existem outros métodos e tecnologias utilizados para autenticação de usuários nos sistemas. Entre os mais conhecidos e que são utilizados atualmente destacam-se:

3.1 SMART CARD

Os *smart cards* (Figura 1), ou cartões inteligentes são sucessores dos antigos cartões magnéticos, populares devido ao uso diário no comércio e transações bancárias. Basicamente são similares ao seu antecessor, porém possuem um *chip* capaz de armazenar e processar informações de seus usuários (PINHEIRO, 2008).

Esses tipos de cartões são comuns atualmente, em bancos e comércios (cartões de débito e crédito), crachás de funcionários para liberação de controle de acesso, e até em estacionamentos e condomínios.

Os *smart cards*, popularmente conhecidos como “cartões magnéticos com *chip*” são utilizados, também para armazenamento de certificado digital, muito utilizado pelas empresas na busca pela segurança de transações pela Internet, como acesso a serviços da Receita Federal, autenticação e identificação da empresa no ambiente virtual, emissão de notas fiscais, e até assinatura de documentos eletrônicos (Figura 1). Nesse caso, o cartão é conectado a uma leitora, que por sua vez é ligada a uma porta *usb* do computador (SERASA EXPERIAN, 2014).

O *smart card* é um tipo de identificação bastante comum atualmente. Porém se utilizado como única forma de autenticação possui alto risco de falha, já que caso o cartão for perdido, roubado, ou emprestado, poderá ser utilizado facilmente por terceiros, e isso representa um alto risco à empresa.

Se considerar-se, por exemplo, um controle de acesso físico ao CPD da empresa ser feito por esse tipo de identificação, sem grandes dificuldades, um invasor poderá ter acesso a todos os equipamentos que armazenam as informações mais importantes de todo o negócio, e caso não seja descoberto a tempo, poderá involuntariamente ou não causar danos irreversíveis a organização.

Figura 1 – Exemplo de *Smart cards*: Cartão de Crédito e Certificado digital com a leitora *USB*

Adaptado de: <http://www.turistaprofissional.com/2013/09/26/e-bom-levar-cartao-de-credito-em-viagem/>
<http://serasa.certificadodigital.com.br/produtos/para-emissao-de-nf-e/certificado-a3/>

3.2 TOKEN

Os *tokens*, segundo Pinheiro (2008) podem ser divididos entre *tokens* de armazenamento, e *tokens* dinâmicos. Os de armazenamento consistem em um dispositivo físico que é utilizado em conjunto com uma senha para validação e autenticação.

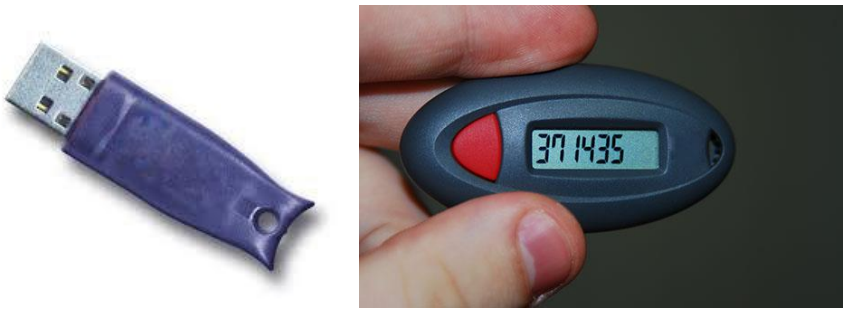
Basicamente, trata-se da junção de um cartão (dispositivo físico) com um *PIN* (senha), combinando, algo que o usuário possui (Cartão ou dispositivo *USB*), e algo que o mesmo conhece (*PIN*). Um exemplo bastante comum é utilizado na maioria dos caixas eletrônicos dos bancos, em que o usuário insere seu cartão, e sua senha para a realização de transações bancárias.

Outro tipo de aplicação são os *tokens* que armazenam (Figura 2) certificados digitais, como os do Serasa citado anteriormente, tendo a mesma função do *smart card* conectado na leitora *USB*. O *token*, nesse caso, armazena de modo criptografado o certificado digital, fazendo com que o seu uso, em conjunto com um o *PIN* valide e autentique de forma eficaz e assim seja possível que o usuário ou a organização consiga se identificar e realizar as transações necessárias na Internet.

O *token* dinâmico (Figura 2), como o nome sugere, consiste na geração de um *PIN*, normalmente temporário e aleatório por um dispositivo que é utilizado como confirmação para a autenticação do usuário. Assim como acontece com os *tokens* de armazenamento, os *tokens* dinâmicos também são utilizados em conjunto com a senha para validar a autenticação.

Esse tipo de validação é muito utilizado nas transações bancárias realizadas através da Internet, dispensando o uso de cartões com senhas, que podem ser roubados e garantindo mais segurança, já que o código gerado é aleatório e disponibilizado por dispositivo de posse do usuário, ou até em casos mais atuais, o *token* SMS, a qual o banco, durante o acesso envia uma mensagem de texto para o celular cadastrado pelo cliente, informando um código de validação para que seja inserido, e assim realizada a autenticação.

Figura 2 – *Token* de armazenamento e *token* dinâmico



Adaptado de: <http://gadicas.blogspot.com.br/2013/07/instalacao-de-certificado-digital-no.html>
<http://g1.globo.com/Noticias/Tecnologia/0,,MUL1189074-6174,00->

3.3 BIOMETRIA

A Biometria, no âmbito das redes de computadores, segundo Pinheiro (2008) pode ser definida com como um conjunto de métodos cujo objetivo é autenticar, identificar ou verificar de forma automática um indivíduo através de suas características físicas ou comportamento.

A biometria permite que o usuário seja identificado através de uma característica única de cada um, podendo ser classificada como uma forma de autenticação baseada no que o indivíduo é.

Segundo Pinheiro (2008), a característica que esse tipo de autenticação utiliza, pode ser baseada em dois tipos: Fisiológica, em que se obtém a identificação a partir de traços originários da própria genética da pessoa (impressão digital, face) ou comportamental, que se baseia na constante utilização (voz, por exemplo). Essa última, pode ser influenciada mais facilmente através de diversas formas como clima, tempo, ou própria vontade do usuário.

A implementação de autenticação por biometria, sem dúvida contribui grandiosamente com a resolução do problema que a autenticação baseada apenas em senhas alfanuméricas proporciona: A possibilidade de divulgação ou roubo de senhas, já que se baseia em características que são exclusivas de cada ser humano, ou seja, com a biometria as chances de uma pessoa se passar por outra diminui

drasticamente. Porém é interessante lembrar que conforme afirmado por Pinheiro (2008, p. 39), “Nenhuma característica biométrica digital consegue atender com perfeição aos requisitos de uma característica biométrica ideal, fato que impossibilita uma unicidade absoluta sobre qual tecnologia biométrica é melhor”.

Por isso é interessante que seja avaliada, estudada qual a forma de autenticação biométrica que mais se adapta às necessidades da empresa, de acordo com os objetivos estabelecidos na Política de Segurança da Informação.

3.3.1 IMPRESSÃO DIGITAL

A identificação através da impressão digital é, muitas vezes associada como sendo sinônimo de biometria. Na verdade, a verificação da digital é um tipo muito conhecido de identificação biométrica.

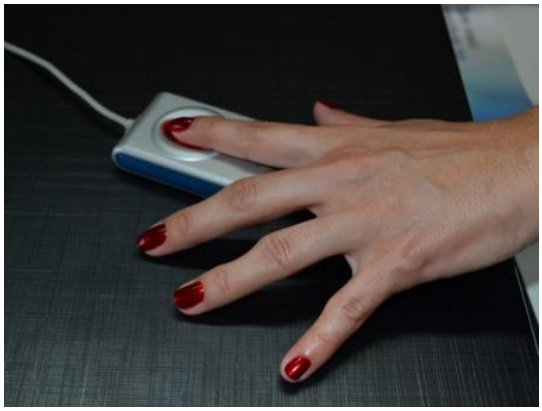
Essa identificação consiste, conforme afirmado por Pinheiro (2008) na captura das impressões digitais por leitores ópticos. Essa imagem é processada pelo sistema, que identifica e compara com as que foram cadastradas no banco de dados, liberando ou não o acesso.

Esse tipo de identificação, que atualmente é muito comum começou a ser utilizada por volta do século XIX como método de identificação de indivíduos (Pinheiro, 2008), e vem sendo empregada em documentos, como o RG, Carteira de Habilitação, entre outros, inicialmente sendo apenas impressa nos documentos, porém atualmente, para emissão dos mesmos são realizados cadastros em leitores biométricos.

No Brasil, por exemplo, desde a publicação da resolução 249.2007 em Agosto de 2007 (posteriormente revogado pela resolução 287.2008, que por sua vez foi alterada para a resolução 361/10) por parte do Conselho Nacional de Trânsito - CONTRAN, a identificação de novos candidatos a primeira ou renovação da carteira de habilitação tem sido realizado através da identificação utilizando impressão digital (Figura 3), em que os alunos se identificam e autenticam durante o cumprimento das aulas obrigatórias para obtenção ou renovação da carteira (CONTRAN, 2007, 2008).

Outro exemplo, mais recente de uso de impressão digital em nosso país, é o Programa de Identificação Biométrica do Eleitor, que se iniciou em Dezembro de 2007 em caráter experimental, através da resolução 22688 do Tribunal Superior Eleitoral. Na ocasião, 40 mil eleitores utilizaram a identificação através de impressão digital. Nas eleições de 2010, esse número subiu para 1,1 milhão de eleitores, e em 2012 foram convocados cerca de 7 milhões de eleitores a cadastrarem suas digitais. Para as eleições de 2014, o número de cadastros realizados foram de 11,2 milhões de eleitores. (TSE, 2014).

Figura 3 – Leitor biométrico utilizado para identificação de alunos em auto-escolas

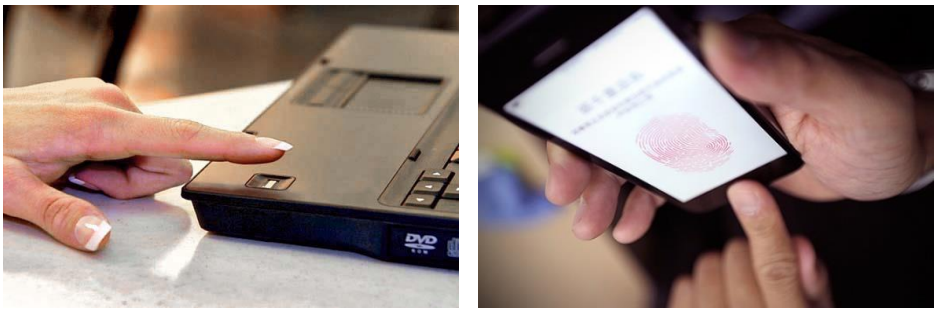


Fonte: <http://noticias.r7.com/distrito-federal/noticias/detran-df-anuncia-licitacao-para-instalar-sistema-biometrico-em-auto-escolas-20130321.html>

A impressão digital é o método mais comum de autenticação biométrica, e também apresenta um baixo custo de implementação e facilidade de coleta. Atualmente os leitores biométricos têm custo relativamente baixo, inclusive, grande parte dos *notebooks*, por exemplo já são vendidos com leitor de impressão digital para acesso ao sistema operacional, em que é possível utilizar o mesmo em substituição a senha alfanumérica ao acessar sua conta no domínio.

Além dos *notebooks*, os *smartphones* também seguem a tendência da autenticação através da impressão digital (Figura 4), e hoje é possível encontrar leitores biométricos nos principais *smartphones* do mercado, sendo possível se autenticar tanto no próprio aparelho, quanto em sistemas de terceiros, como de pagamento de compras, e até transações bancárias.

Figura 4 – Biometria presente em *notebooks* e *smartphones*



Adaptado de: <http://www.cursosprime.com.br/blogprime/2011/08/debate-computadores-de-mesa-estao-morrendo/>
<http://www1.folha.uol.com.br/tec/2013/12/1384484-smartphones-biometricos-serao-comuns-em-2014-diz-pesquisa.shtml>

Outro uso, que tem se tornado muito comum, é nos caixas eletrônicos (Figura 5). Atualmente, os principais bancos do país já possuem leitores biométricos em seus caixas eletrônicos, combinando com os já comuns sistemas de autenticação como senha numérica e alfabética, *token*, entre outros, ou até utilizando apenas a biometria, dispensando o uso de cartões, como já é disponibilizado pelo banco Itaú em seus caixas eletrônicos.

Figura 5 – Caixa eletrônico com leitor biométrico de impressão digital

Fonte: <http://corporate.canaltech.com.br/noticia/seguranca/Clientes-do-Itau-poderao-realizar-saques-sem-cartao-apenas-com-a-biometria/>

No âmbito empresarial, atualmente é uma tecnologia acessível, vantajosa, e eficaz conforme citado anteriormente, podendo ser implementada sem grandes problemas, e também utiliza como fonte uma característica imutável do ser humano, ou seja, que não sofre grandes mudanças com o tempo conforme afirmado por Costa, Obelheiro e Fraga (2006).

As principais desvantagens quem podem atrapalhar a implantação, segundo Costa, Obelheiro e Fraga (2006) são as rejeições por parte de diferentes culturas (Devido a esse tipo de identificação estar ligada a criminosos, pessoas iletradas e também por questões de higiene), e a qualidade das impressões digitais das pessoas (principalmente em trabalhadores manuais, e pessoas que utilizam produtos químicos).

3.3.2 GEOMETRIA DA MÃO

A identificação biométrica através da geometria da mão, assim como a impressão digital não é uma tecnologia recente. Segundo Costa, Obelheiro e Fraga (2006), a primeira patente de um dispositivo que media a geometria da mão e

registrava para comparações futuras foi registrada em 1960, construída por Robert P. Miller.

Nesse tipo de tecnologia, segundo Matos (2011) a identificação pode ser realizada através da geometria da mão, sobre a impressão palmar da mão ou as duas em conjunto.

No caso da identificação da geometria da mão ou reconhecimento dos dedos, são levados em consideração apenas alguns pontos como formato, tamanho dos dedos, proporção entre articulações, conforme Pinheiro (2008), enquanto na impressão palmar, são reconhecidas algumas linhas como linhas da vida, do coração, da cabeça e, também a textura como acontece também nas impressões digitais (MATOS, 2011).

A aquisição dessa identificação é realizada através de *scanners* que podem se utilizar de fixadores (Figura 6) para que a mão do usuário sempre esteja na posição definida, ou sem os fixadores, porém com as respectivas marcas que orientem o local aonde o utilizador deverá posicionar a mão para que o cadastramento ou identificação seja realizado (Matos, 2011).

Figura 6 – Leitor biométrico de Geometria da mão com fixadores

Fonte: <http://www.pontoonline.net/pol/index.php/produtos/controle-de-acesso/biometrico>

Assim como ocorre com as impressões digitais, a biometria baseada na geometria da mão também é bastante utilizada. Podemos facilmente encontrar esse tipo de autenticação nos caixas eletrônicos em nosso país, principalmente nos caixas do banco Bradesco que iniciou o uso dessa tecnologia no Brasil, que se baseia na leitura na impressão palmar da mão, em meados de 2007 (G1, 2012).

Desde então esse sistema tem sido utilizado combinado com outras formas de autenticação. Em 2012, segundo publicação no G1 (2012) o banco anunciou que já seria possível realizar transações sem utilizar o cartão, fazendo uso apenas do sistema biométrico.

Figura 7 – Leitor biométrico de palma da mão em caixa eletrônico

Fonte: <http://www.viamaxi.com.br/2011/10/bancos-se-preparam-para-o-uso-da-biometria-clientes-apontam-vantagens-e-desvantagens-do-sistema/>

Assim como ocorre com os casos de biometrias baseados em impressões digitais, os sistemas baseados na geometria da mão também possuem baixo custo e facilidade de implementação (PINHEIRO, 2008).

Porém, segundo Matos (2011) entre as principais limitações desse tipo de sistema estão aquelas determinadas pelos problemas de conforto tanto nos *scanners* em que existem os pinos demarcando a área de captura quanto os *scanners* que não utilizam esses pinos, que acabam tendo muitas restrições quanto ao posicionamento das mãos, resultando na maior possibilidade de erro de posicionamento e consequentemente, falha na autenticação.

Além disso, o mau posicionamento da mão, iluminação, ou até suor podem resultar na necessidade de repetição até que o mesmo reconheça a identidade e realize a autenticação, tornando esse tipo de sistema não muito ágil, tanto na aquisição quanto na identificação do usuário.

3.3.3 RECONHECIMENTO FACIAL

O processo de reconhecimento facial é uma característica natural do ser humano. É através dessa característica que as pessoas são capazes de reconhecer, e identificar mesmo após vários anos, a face de pessoas com as quais tiveram algum tipo de contato.

As tecnologias de reconhecimento facial buscam, assim como os seres humanos realizam naturalmente, identificar as pessoas através do seu rosto. Esse processo consiste, segundo Pinheiro (2008) na captura da imagem da pessoa através de câmera, considerando as medidas do rosto e comparando a mesma com banco de dados armazenado anteriormente.

Atualmente, esse tipo de autenticação tem alta precisão, e é capaz de captar pequenas diferenças, que muitas vezes as pessoas não conseguem identificar, como gêmeos, por exemplo, (Olhar digital, 2011). O sistema realiza a leitura do rosto, e codifica em uma sequência digital, e é armazenado no banco de dados para comparações posteriores.

Além da alta precisão, esses sistemas mais atuais são capazes de identificar vários rostos ao mesmo tempo, são difíceis de serem burlados, já que, além de identificar a distância entre olhos, queixo, boca, entre outros, o sistema identifica também a profundidade, fazendo com que não seja possível burlá-lo com uma foto, ou vídeo, por exemplo, (Olhar digital, 2011).

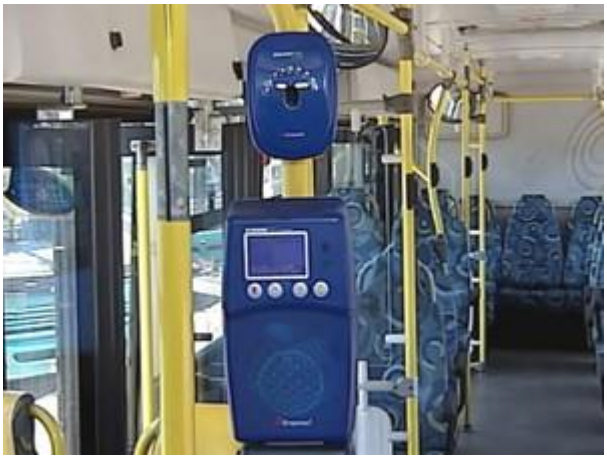
O uso dessa tecnologia tem se tornado cada vez mais comum, sendo utilizados, por exemplo nos *smartphones* atuais que já possuem ferramentas capazes de desbloquear o telefone através do reconhecimento facial. Além disso, existe a tendência da utilização dessa tecnologia para realizar compras, como a da empresa alemã *Uniqul*, que desenvolveu um sistema que utiliza única e exclusivamente o

reconhecimento do rosto do comprador para autorizar a compra, dispensando o uso de cartões de crédito (TECMUNDO, 2013).

No Brasil, diversas empresas de ônibus já adotaram o reconhecimento facial em suas frotas de ônibus (Figura 8). Essa tecnologia, que tem a cidade de Caruaru no Pernambuco como uma das pioneiras no uso dentro dos ônibus, e foi adotada recentemente pelo município de Uberlândia, em Minas Gerais é utilizada visando fiscalizar e coibir o uso irregular dos benefícios de vale transporte.

O Detector realiza a captura do rosto do passageiro ao passar pela catraca do ônibus, e armazena os dados, que posteriormente são coletados, e analisados. Caso a imagem da pessoa que estiver utilizando o cartão não coincidir com a respectiva face armazenada no banco de dados o cartão é bloqueado, podendo fazer com que o usuário possa perder o benefício em caso de reincidência (CORREIO DE UBERLÂNDIA, 2014).

Figura 8 – Sistema de reconhecimento facial em ônibus



Fonte: <http://g1.globo.com/minas-gerais/triangulo-mineiro/noticia/2014/03/sistema-em-onibus-de-uberlandia-registra-mais-de-40-fraudes-diarias.html>

Outra aplicação dessa tecnologia em nosso país começou a ser testada recentemente pelo Clube de futebol S.C Internacional, do Rio Grande do Sul. O sistema, procura, através de câmeras de segurança identificar torcedores não

autorizados, e evitar que os mesmos consigam assistir os jogos nos estádios. (UOL, 2014).

O sistema de reconhecimento facial possui entre suas vantagens a precisão, e o fato de ser um dos sistemas menos intrusivos. Atualmente os sistemas mais modernos conseguem inclusive identificar rostos em ambientes não muito colaborativos (Esteta, 2014). Além disso, são difíceis de serem fraudados. Entre as desvantagens, existe a da influência do ambiente onde é realizada captura, que pode ser prejudicado por falta de iluminação, ou obstrução da face da pessoa, por exemplo.

3.3.4 LEITURA DA ÍRIS

A Íris é a parte do olho que se localiza em torno da pupila, e é responsável pela cor dos olhos. Esse órgão, segundo Pereira (2012) possui diversas características únicas a cada ser humano, e proporciona 266 pontos de identificação.

A identificação através da íris é estável, já que suas características não são alteradas conforme o tempo (PINHEIRO, 2008). Além disso, possui baixíssima probabilidade de erro, algo em torno de 1% (PEREIRA, 2012).

O processo de identificação através da íris, segundo Pinheiro (2008) consiste na aquisição da imagem da íris através e um leitor (Figura 9), seguido de uma etapa em que é aplicado o algoritmo de reconhecimento das características da íris. Após isso, é iniciado o processo de extração das características da íris para a geração do chamado *IrisCode* que é utilizado para comparações no sistema.

Esse tipo de autenticação possui grandes vantagens, como a precisão, citada anteriormente, a característica da íris de não se alterar conforme o tempo, e também a rapidez na captura e comparação através desse método (PINHEIRO, 2008). Além disso, por ser um órgão interno, segundo Pereira (2012) a Íris é bem protegida pelas pálpebras, o que faz com que seja mais preciso, se comparado com as formas de biometria citadas anteriormente, que tem maior probabilidade de sofrerem cortes e deformações e assim atrapalhar a identificação.

Figura 9 – Leitor de íris

Fonte: <http://www.atusvigilancia.com.br/servicos/5/automacao-predial-e-empresarial/34/leitores-de-ris.html/>

Entre as desvantagens do uso dessa tecnologia, existe o próprio acesso ao órgão, já que as pálpebras estão em constante movimento, e pode ocultar parte da íris durante a leitura. Por isso, esse tipo de tecnologia depende bastante da colaboração do usuário. Além disso, doenças como conjuntivite, catarata, ou alergias podem dificultar a autenticação (PEREIRA, 2012).

Apesar de aparentar distante, esse tipo de tecnologia está cada vez mais acessível, inclusive, podendo ser utilizado em computadores pessoais, como por exemplo, o sistema apresentado pela empresa *Voxx Internacional Corporation* durante a CES 2014, a maior feira de tecnologia do mundo, realizada na segunda semana de Janeiro, em Las Vegas (EUA).

Esse produto consiste em um dispositivo com um leitor de íris a qual pode ser utilizado como método de autenticação tanto em softwares quanto no próprio computador, bastando instalar o aplicativo, compatível com os Sistemas Operacionais *Windows, Mac,* e até com *Chrome OS* na máquina. Com o software instalado, basta olhar fixamente para o leitor de retina que fará a autenticação, substituindo as tradicionais senhas.

3.3.5 LEITURA DA RETINA

A retina é composta por vasos sanguíneos, e está localizada na parte interna do globo ocular. Os vasos sanguíneos que a compõem possuem um padrão único e pessoal. (PINHEIRO, 2008).

Sendo assim, a identificação da pessoa é realizada através da captura, utilizando um leitor de retina, e a análise desses vasos sanguíneos. Segundo Pereira (2012) o leitor utiliza uma fonte de luz que reconhece os padrões de retina sendo, portanto uma técnica muito precisa, e segura por estar diretamente relacionada com os sinais vitais da pessoa a ser identificada.

Entre as desvantagens dessa tecnologia vale a pena destacar que algumas pessoas podem sentir-se desconfortáveis devido à necessidade de olhar fixamente enquanto o leitor realiza a captura da retina. Além disso, existe problemas de leitura quanto a ambientes muito claros, e também, o alto custo de implementação (PINHEIRO, 2008). Por fim, alguns médicos defendem que as características da retina podem ser alteradas por alguns tipos de doenças, diferentemente da íris que é praticamente imutável (PEREIRA, 2012).

3.3.6 VOZ

A identificação através do reconhecimento de voz é uma forma de autenticação que se pode considerar pouco intrusiva, e natural, afinal, as pessoas são acostumadas a se comunicar, e utilizar um método de autenticação que aproveite essa naturalidade pode gerar um bom resultado, e facilidade na implementação e utilização, principalmente em ambientes telefônicos, em que isso se torna mais natural ainda, já que o usuário naturalmente está se utilizando da comunicação oral para receber o atendimento, ou informações.

Esse tipo de identificação consiste, segundo Pereira (2012) na análise do timbre (características) da voz capturada através de um microfone ou telefone. O usuário cadastra uma amostra de sua voz que será utilizada para realizar a comparação e consequentemente a identificação através da voz. O método de captura e comparação dessa amostra pode ser realizado das seguintes formas, segundo Pinheiro (2008):

- Texto fixo: O usuário pronuncia uma palavra ou frase pré-determinada pelo sistema, já gravada anteriormente;

- Dependente do texto: A pessoa deve pronunciar algo específico entre as várias palavras ou frases cadastradas durante a fase de registro;

- Independente: O indivíduo pode pronunciar frases ou palavras a seu critério, já que o sistema processa qualquer que seja a frase ou palavra dita;

- Conversacional: O sistema interroga a pessoa, basicamente como o método dependente de texto, porém as palavras possuem certo nível de segredo;

A autenticação por meio do reconhecimento da voz, como já citado anteriormente, pode ser uma boa alternativa de identificação já que é uma forma pouco intrusiva, fácil de ser utilizada, e possui baixo custo de implementação.

Porém, esse tipo de identificação pode ser influenciado por ruídos no ambiente, e também pelo estado físico (Resfriados, rouquidão, faringite) e emocional (Stress, pressa, ansiedade) do indivíduo, o que pode fazer com que a voz se altere, gerando falsos positivos ou negativos, e comprometendo a eficiência do sistema, além da possibilidade de gerar stress devido à demora no processo de cadastramento do padrão de voz, caso o sistema solicite a repetição constante das palavras ou frases.

3.4 COMBINAÇÕES

Conforme citado ao longo deste trabalho, existem diversos tipos de identificação alguns mais acessíveis e baratos, e outros mais caros, cada um com suas características peculiares, vantagens e desvantagens de implementação.

Na busca pela redução de erros, e, também pelo aumento de segurança e confiabilidade, um ponto a ser observado é o de realizar combinações entre essas várias formas existentes de autenticação.

Nas tabelas a seguir, encontram-se de forma geral, exemplos de algumas combinações e seus níveis de segurança e/ou eficiência. Nesse caso, a segurança de cada tipo de combinação será dividida em três níveis: Baixa, média e alta, considerando baixa, a combinação que mesmo sendo realizada, por dois ou mais meios de autenticação, ainda é possível ser fraudada ou compartilhada, e consequentemente utilizada por outra pessoa, já que se baseia, em autenticações que são de conhecimento, e/ou de posse do usuário, podendo ser roubadas, perdidas, ou até divulgadas propositalmente.

Tabela 1 – Combinações baseadas na posse e conhecimento do usuário

Combinação	Vantagens	Desvantagens	Segurança
Senha e *smartcard* ou senha e *token*	Formas de autenticação de baixo custo e fácil implementação	Apesar de combinada duas formas de autenticação, ainda existe possibilidade de divulgação ou de perda das identificações, ocasionando acesso por pessoas não autorizadas.	Baixa
Exemplo1: Usuário utiliza um *smartcard* conectado a uma leitora, e também faz uso de uma senha com os requisitos mínimos de segurança previamente estabelecidos na Política de Segurança da Informação.			
Exemplo 2: É utilizada uma senha segura, e também um *token* dinâmico ou de armazenamento como identificação de posse do usuário.			

Na tabela 1, a combinação das autenticações baseadas no que o usuário conhece (senha) e no que o usuário possui (*token* ou *smartcard*), apesar de ser mais segura do que a utilização de apenas um tipo de autenticação, ainda é vulnerável, já que pode ocorrer, coincidentemente ou não, por exemplo, da senha ser divulgada ou descoberta, e o *token* ou *smartcard* ser perdido, extraviado ou até roubado, deixando o caminho livre para pessoas não autorizadas.

Na tabela 2, encontra-se outro tipo de combinação, em que se pode classificar como média, sendo composta por um tipo de autenticação que é de conhecimento do usuário, e por esse motivo pode ser divulgada ou descoberta, e também por um tipo de autenticação composta pelas características físicas do usuário, tendo, portanto um nível de segurança maior se comparado a dois tipos de combinação citados na tabela anterior.

Tabela 2 – Combinações baseadas no conhecimento e características físicas do usuário

Combinação	Vantagens	Desvantagens	Segurança
Senha e biometria	Utiliza uma forma de autenticação comum e acessível (Senha), mesclada com a biometria, aumentando a segurança consideravelmente.	Apesar do aumento significativo, caso a senha seja descoberta por um invasor, o mesmo poderá ter certo acesso, mesmo que parcial ao sistema, e poderá realizar alguma operação, dependendo de como o sistema solicita a confirmação de identidade.	Média
Exemplo1: A autenticação é realizada através do uso de uma senha conforme as diretrizes da Política de SI, e biometria baseada em leitura de impressão digital.			
Exemplo 2: Baseia-se na autenticação realizada, também por senha pessoal, e biometria de leitura de íris			

Nesse caso, a autenticação baseada no conhecimento (senha) e nas características físicas do usuário (biometria) combina o uso de uma forma de autenticação comum e muito utilizada, e de baixo custo com biometria, aumentando o nível de segurança, e reduzindo as chances de acessos por pessoas não autorizadas.

Por último, consideram-se as combinações que possuem um alto nível de segurança, as que são compostas por dois ou mais tipos de biometria. Como é baseada exclusivamente em características físicas dos usuários, a possibilidade de uso por pessoas não autorizadas é reduzida a níveis baixíssimos, conforme detalhes na Tabela 3:

Tabela 3 – Combinações baseadas nas características físicas do usuário

Combinação	Vantagens	Desvantagens	Segurança
Duas ou mais autenticações baseadas em biometria	Utiliza uma forma de autenticação comum e acessível (Senha), mesclada com a biometria, aumentando a segurança consideravelmente	O uso de duas ou mais formas de autenticação baseados na biometria, pode aumentar os custos e as dificuldades de implementação. Além disso, pode comprometer a usabilidade e agilidade do sistema, já que a identificação biométrica pode ser mais lenta e suscetível a falsos negativos de acordo com o ambiente, e posicionamento perante o leitor biométrico.	Alta
Exemplo1: Autenticação baseada em reconhecimento facial, e impressão digital			
Exemplo 2: Autenticação baseada na leitura da retina, e reconhecimento de voz			

Nesse último caso, apresentado na Tabela 3, a combinação entre duas ou mais autenticações biométricas elevam a segurança a um alto nível, reduzindo drasticamente as chances do uso indevido ou acesso de outros a contas que não são de sua propriedade.

Considerando as formas e métodos apresentados neste capítulo, cabe a empresa estudar, e definir quais tipos e métodos de autenticação e/ ou as combinações que poderão ser utilizadas e que estejam dentro da realidade financeira, porém sem abrir mão da busca pela segurança e proteção das informações cruciais para o desenvolvimento do negócio.

4 CONSIDERAÇÕES FINAIS

Através dos conteúdos apresentados nesse trabalho, é possível destacar-se que o processo de Segurança da Informação, e proteção dos dados, não somente no quesito “compartilhamento de senhas entre usuários” não depende somente da tecnologia, e sistemas de proteção extremamente modernos e eficientes.

Todo o processo que envolve a proteção dos dados da empresa depende do comprometimento da área de negócio em apoiar e auxiliar na definição de uma Política de Segurança da Informação clara, objetiva, que estabeleça limites e regras visando sempre o bem do negócio por parte do time de gestão de Tecnologia da Informação.

Também, é de extrema importância que haja a divulgação dessa política, e também o treinamento adequado, visando informar, conscientizar, e orientar os usuários dos procedimentos, normas e recomendações descritos na Política de Segurança da Informação, e também boas práticas no uso dos recursos tecnológicos no desenvolvimento de suas atividades.

Outro ponto importante é a eficiência dos recursos de segurança que a empresa deve possuir, buscando sempre as melhores práticas para proteção das informações da empresa. Essa eficiência, considerando o escopo adotado nesse trabalho, o de compartilhamento de senhas entre usuários, poderá ser difundida com a melhoria dos métodos de autenticação além dos treinamentos e definição de uma Política de Segurança da Informação, propostos anteriormente.

As organizações, com base em seus procedimentos, normas, políticas internas, e também de recursos tecnológicos e financeiros disponíveis para investimento poderá buscar a melhor maneira de melhorar esses métodos, seja implementando autenticações baseadas em sistemas biométricos, ou mesclando o seu uso com algum recurso já utilizado, como cartão, *token* ou senha, porém tendo a consciência de que não há recurso que deixe a empresa totalmente segura, porém quanto maior o investimento, em pessoas, métodos e tecnologia, maior o nível de segurança, e consequentemente menor chance de acessos indevidos que poderiam ocasionar roubo, perda ou alteração de informações cruciais para o negócio.

Por isso, utilizando-se da Política de Segurança da Informação para normatizar, do treinamento, para conscientizar, e da Tecnologia para garantir que essas políticas e estão sendo cumpridas, fazendo com que o usuário além de ter consciência de que o compartilhamento de seu usuário é um risco a si próprio e a organização, não consiga divulgá-lo ou ter seu perfil roubado por algum invasor, já que sua forma de autenticação está devidamente reforçada por um ou mais métodos, garantindo a melhora significativa de segurança na autenticação, e consequentemente nos dados da organização.

5 REFERÊNCIAS BIBLIOGRÁFICAS

DAWEL, George. **A Segurança da Informação nas empresas**. 1. ed. Rio de Janeiro: Ciência Moderna, 2005.

FERREIRA Fernando Nicolau Freitas; ARAÚJO Márcio Tadeu De. **Política de Segurança da Informação da Informação – Guia Prático para Elaboração e Implementação**. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

FONTES, Edison. **Praticando a Segurança da Informação**. 1. ed. Rio de Janeiro: Brasport, 2008.

FONTES, Edison. **Segurança da Informação: O usuário faz a diferença**. 1. ed. São Paulo: Saraiva, 2006.

MENEZES Josué das Chagas. **Gestão da Segurança da Informação.** Leme: Ciência Moderna, 2008.

MITNICK, Kevin; SIMON William L. A arte de enganar. 1. Ed. São Paulo: Pearson, 2003

PINHEIRO José Maurício. **Biometria nos Sistemas Computacionais – Você é a Senha.** Rio de Janeiro: Ciência Moderna, 2008.

PRICEWATERHOUSECOOPERS SERVIÇOS PROFISSIONAIS LTDA. **Pesquisa Global de Segurança da Informação**, 2014.

MATOS, Hélder José Da Silva. **Reconhecimento Biométrico Baseado na Geometria da Mão**. 2011. 132 f. Dissertação (Mestrado em Engenharia Eletrotécnica e de Computadores) - Mestrado Integrado em Engenharia Eletrotécnica e de Computadores, Faculdade de Engenharia da Universidade do Porto, Porto, 2011.

PEREIRA Cipriano Luís Arede. **Dispositivos de identificação**. 2012. 155 f. Dissertação (Mestrado em Sistemas e Tecnologias de Informação para as Organizações) – Mestrado em Sistemas e Tecnologias de Informação para as Organizações, Escola Superior de Tecnologia e Gestão de Viseu, Viseu, 2012.

COSTA, Luciano R.; OBELHEIRO, Rafael R.; FRAGA, Joni S. **Introdução à Biometria.** In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS - SBSEG, Santos. **Anais eletrônicos...**Santos: Biblioteca Digital Brasileira de Computação. p. 103 à 151. 2006. Disponível em: <http://gcseg.das.ufsc.br/wssec/publicacoes.html>. Acesso em: 12 mar. 2014.

CONSELHO NACIONAL DE TRANSITO (CONTRAN) **Resolução RE nº 249, de 27 de Agosto de 2007**. Regulamenta o procedimento de coleta e armazenamento de impressão digital nos processos de habilitação ou renovação da Carteira Nacional de Habilitação – CNH. Disponível em: <www.denatran.gov.br/download/Resolucoes/Resolução%20249.2007.doc>. Acesso em: 18 abr. 2014.

CONSELHO NACIONAL DE TRANSITO (CONTRAN) **Resolução RE nº 287, de 29 de Julho de 2008**. Regulamenta o procedimento de coleta e armazenamento de impressão digital nos processos de habilitação ou renovação da Carteira Nacional de Habilitação – CNH.Disponível em: <http://www.denatran.gov.br/download/Resolucoes/REPUBLICACAO_RESOLUCAO_CONTRAN_287.pdf >. Acesso em: 18 abr. 2014.

CONSELHO NACIONAL DE TRANSITO (CONTRAN) **Resolução RE nº 361, de 29 de Julho de 2008**. Altera a Resolução nº 287/2008 - CONTRAN, que dispõe sobre a regulamentação do procedimento de coleta e armazenamento de impressão digital nos processos de habilitação ou renovação da Carteira Nacional de Habilitação – CNH. Disponível em: <http://www.denatran.gov.br/download/Resolucoes/RESOLUCAO_CONTRAN_361_10.pdf >. Acesso em: 18 abr. 2014.

TRIBUNAL SUPERIOR ELEITORAL (TSE) **Resolução RE nº 22688, de 31 de Dezembro de 2008**. Disciplina os procedimentos para a atualização do cadastro eleitoral, decorrente da implantação, em caráter experimental, nos municípios que especifica, de nova sistemática de identificação do eleitor, mediante incorporação de dados biométricos e fotografia, e dá outras providências. Disponível em: <http://www.tse.gov.br/internet/eleicoes/2008/pdf/res022688_13122007.pdf>. Acesso em: 18 abr. 2014.

TRIBUNAL SUPERIOR ELEITORAL (TSE) **Resolução RE nº 23335, de 31 de Dezembro de 2008**. Disciplina os procedimentos para a realização de revisões de eleitorado de ofício, com vistas à atualização do cadastro eleitoral, decorrente da implantação, em municípios previamente selecionados pelos tribunais regionais eleitorais, de nova sistemática de identificação do eleitor; mediante incorporação de dados biométricos, dá outras providências. Disponível em: <http://www.tse.jus.br/arquivos/tse-res-23335-2011-procedimentos-para-realizacao-de-revisoes-de-eleitorado-de-oficio/view>. Acesso em: 18 abr. 2014.

TRIBUNAL SUPERIOR ELEITORAL. Justiça Eleitoral encerra 3ª fase da biometria com 11,2 milhões de eleitores recadastrados. Brasília, 2014. Disponível em: <http://www.tse.jus.br/noticias-tse/2014/Abril/justica-eleitoral-encerra-3a-fase-da-biometria-com-11-2-milhoes-de-eleitores-recadastrados>. Acesso em: 08 jun. 2014.

SERASA EXPERIAN. Certificados Digitais. São Paulo, 2014. Disponível em: <http://serasa.certificadodigital.com.br/index2.html?utm_expid=65236189-31.32LHYCUVQ9C1dr_W-x-2WA.1&utm_referrer=http%3A%2F%2Fserasa.certificadodigital.com.br%2Fo-que-e%2F>. Acesso em: 08 jun. 2014.

BEIRA Rio irá testar sistema de reconhecimento facial contra bagunceiros. **UOL Copa**, São Paulo, 19 abr. 2014. Disponível em: <http://copadomundo.uol.com.br/noticias/redacao/2014/04/19/beira-rio-ira-testar-sistema-de-reconhecimento-facial-contra-bagunceiros.htm>. Acesso em: 01 mai. 2014.

CLIENTES do Bradesco já podem fazer saques sem ter de usar cartão. **Portal G1**, São Paulo, 13 dez. 2012. Disponível em: <http://g1.globo.com/economia/seu-dinheiro/noticia/2012/12/cientes-do-bradesco-ja-podem-fazer-saques-sem-ter-de-usar-cartao.html. Acesso em: 18 abr. 2014.

FERNANDES Arthur. **Ônibus de Uberlândia agora têm dispositivo para reconhecimento facial.** Uberlândia, 27 jan. 2014. Disponível em: <https://www.correiodeuberlandia.com.br/cidade-e-regiao/onibus-de-uberlandia-agora-tem-dispositivo-para-reconhecimento-facial/>. Acesso em: 01 mai. 2014.

TECMUNDO. **Que tal trocar o cartão de crédito por seu rosto ao pagar compras?** [S.I.] 19 jul. 2013.Disponível em: <http://www.tecmundo.com.br/reconhecimento-facial/42155-que-tal-trocar-o-cartao-de-credito-por-seu-rosto-ao-pagar-compras-video-.htm>. Acesso em: 01 mai. 2014.

GRUPO do IC cria sistema para reconhecimento facial: Metodologia, desenvolvida em colaboração com Universidade de Harvard, está entre as mais precisas do mundo. **Esteta Beleza e Arte em Tecnologia**, 05 abr. 2014. Disponível em: <http://www.esteta.com.br/noticia.php?intNotID=31838>. Acesso em: 01 mai. 2014

LEITOR de íris quer substituir o uso de senhas. **Olhar Digital**, 18 jan. 2014. Disponível em: <http://olhardigital.uol.com.br/video/39820/39820>. Acesso em: 01 mai. 2014.

NOGUEIRA Daniela. Reconhecimento facial flagra 53 fraudes por dia nos ônibus em Uberlândia**. Correio de Uberlândia,** Uberlândia, 14 mar. 2014. Disponível em: <https://www.correiodeuberlandia.com.br/cidade-e-regiao/reconhecimento-facial-flagra-53-fraudes-por-dia-nos-onibus//>. Acesso em: 01 mai. 2014.

FERREIRA Diclev. É Bom levar o cartão de crédito em viagem? **Turista Profissional** [S.I.], 2013. Disponível em: <http://www.turistaprofissional.com/2013/09/26/e-bom-levar-cartao-de-credito-em-viagem/>. Acesso em: 27 mai. 2014.

CERTIFICADOS Digitais. [S.I.], 2014. Disponível em: <http://serasa.certificadodigital.com.br/produtos/para-emissao-de-nf-e/certificado-a3/>. Acesso em: 27 mai. 2014.

ANDRADE Gabriel. Instalação de Certificado Digital no ECRV SP. **GA Dicas.** [S.I.], 2013. Disponível em: <http://gadicas.blogspot.com.br/2013/07/instalacao-de-certificado-digital-no.html>. Acesso em: 27 mai. 2014.

ROHR Altieres. Pacotão de segurança: truque para sites falsos e vírus em site de torpedos. **G1** [S.I.], 2009. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1189074-6174,00-PACOTAO+DE+SEGURANCA+TRUQUE+PARA+SITES+FALSOS+E+VIRUS+EM+SITE+DE+TORPEDOS.html>. Acesso em: 27 mai. 2014.

DETRAN-DF anuncia licitação para instalar sistema biométrico em auto-escolas. [S.I.], 2013. Disponível em: <http://noticias.r7.com/distrito-federal/noticias/detran-df-anuncia-licitacao-para-instalar-sistema-biometrico-em-auto-escolas-20130321.html>. Acesso em: 27 mai. 2014.

ARRUDA Felipe. Debate: computadores de mesa estão morrendo? **CURSOS Prime** [S.I.], 2011. Disponível em: <http://www.cursosprime.com.br/blogprime/2011/08/debate-computadores-de-mesa-estao-morrendo/>. Acesso em: 27 mai. 2014.

DA Reuters. Smartphones biométricos serão comuns em 2014, diz pesquisa. **Folha de São Paulo.** [S.I.], 2013. Disponível em: <http://www1.folha.uol.com.br/tec/2013/12/1384484-smartphones-biometricos-serao-comuns-em-2014-diz-pesquisa.shtml>. Acesso em: 27 mai. 2014.

CLIENTES do Itaú poderão realizar saques sem cartão, apenas com a biometria. **Canal Tech.** [S.I.], 2012. Disponível em: <http://corporate.canaltech.com.br/noticia/seguranca/Clientes-do-Itau-poderao-realizar-saques-sem-cartao-apenas-com-a-biometria/>. Acesso em: 27 mai. 2014.

PONTO Online. Biométrico [S.l.], Disponível em: <http://www.pontoonline.net/pol/index.php/produtos/controle-de-acesso/biometrico>. Acesso em: 27 mai. 2014.

OLIVEIRA, Kelly Bancos se preparam para o uso da biometria; clientes apontam vantagens e desvantagens do sistema. **Via Maxi.** [S.I.], 2011. Disponível em: <http://www.viamaxi.com.br/2011/10/bancos-se-preparam-para-o-uso-da-biometria-clientes-apontam-vantagens-e-desvantagens-do-sistema/>. Acesso em: 27 mai. 2014.

SISTEMAS ônibus de Uberlândia registra mais de 40 fraudes diárias. [S.I.], 2014. Disponível em:

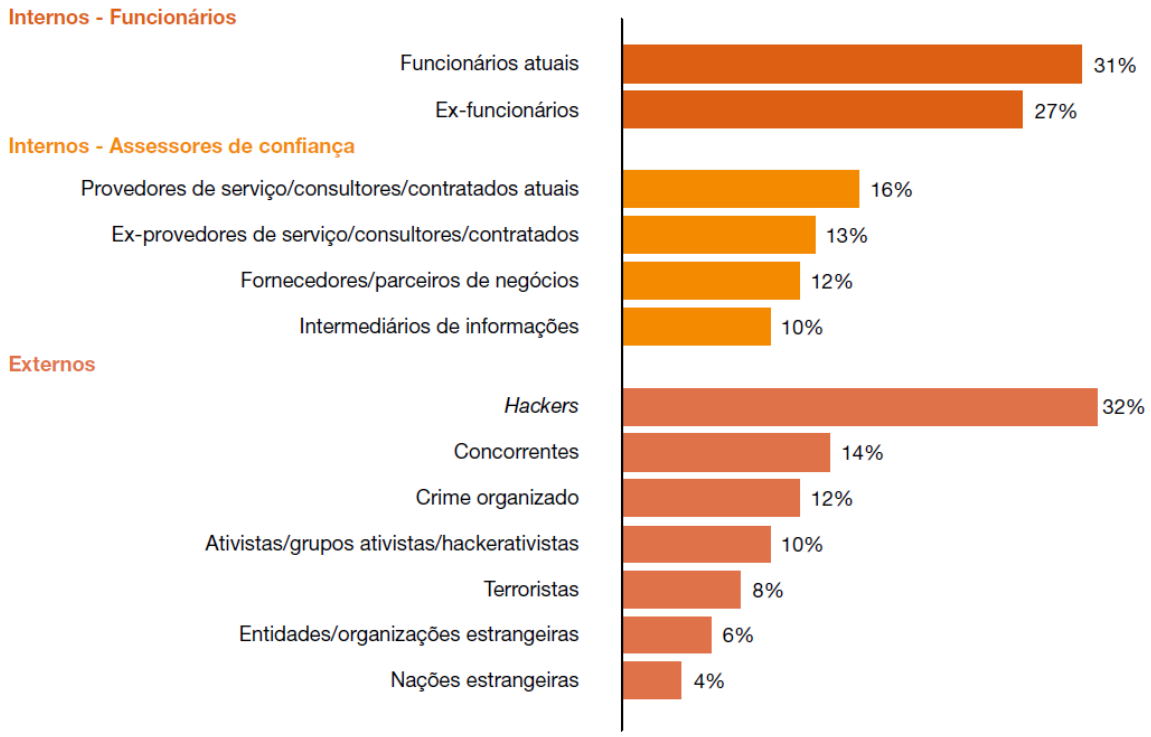
<http://g1.globo.com/minas-gerais/triangulo-mineiro/noticia/2014/03/sistema-em-onibus-de-uberlandia-registra-mais-de-40-fraudes-diarias.html>. Acesso em: 27 mai. 2014.

LEITORES de íris. [S.l.] . Disponível em: <http://www.atusvigilancia.com.br/servicos/5/automacao-predial-e empresarial/34/leitores-de-ris.html/>. Acesso em: 01 mai. 2014.

APÊNDICE A: INCIDENTES RELACIONADOS À ÁREA DE SEGURANÇA DA INFORMAÇÃO - 2014

Na Pesquisa Global de Segurança da Informação (PWC, 2014) encontra-se outra informação importante: Os dados abaixo informam as origens dos incidentes de segurança da informação nas empresas, e suas causas. Entre os maiores causadores, encontram-se um de ameaça externa (*Hackers*) e outros dois de ameaças internas as quais os danos foram causados por funcionários ativos e também por ex-funcionários, reiterando que a importância do usuário no processo de segurança da informação, e o impacto que o mesmo pode gerar, caso forneça o acesso, ou intencionalmente modifique informações importantes para o negócio.

Figura 10: Origem dos incidentes de Segurança da Informação



Observação: Nem todos os fatores são mostrados. A soma não equivale a 100%.
Os respondentes puderam indicar vários fatores.

Fonte: (PWC, 2014)

ANEXO A: EXEMPLO DE BOLETIM DE CONSCIENTIZAÇÃO DO USUÁRIO

Exemplo de um boletim de conscientização de usuário quanto à importância de Segurança da Informação e boas práticas, desenvolvido por EDILSON FONTES em seu livro “Segurança da Informação: O Usuário faz a diferença” (2006, p. 134):

A informação da organização é um bem valioso e necessita ser protegido e bem gerenciado. Cada usuário (funcionário, prestador de serviço) tem a obrigação profissional de cuidar da informação que utiliza. No dia-a-dia, podemos executar pequenas ações que proporcionam uma melhor proteção. Destacamos:

1. Suspenda a sessão de trabalho toda vez que se ausentar do local onde se encontra o computador que você está utilizando. Para o ambiente Windows, digite ao mesmo tempo as três teclas: Ctrl Alt Delete.

2. Programe o computador que você utiliza para entrar em modo proteção de tela com exigência de senha após dez minutos (tempo sugerido de não utilização).

3. Para documento classificado como confidencial, ou que você considere de nível equivalente, guarde-o trancado em armário ou gaveta quando você não estiver utilizando nem estiver no local. Destrua-o fisicamente antes de colocá-lo no lixo.

4. Após cada reunião, não deixe nenhum tipo de informação no ambiente da sala: apague o quadro, retire as folhas de *flip chart* e destrua o material utilizado como rascunho.

5. Ao falar no telefone ou por e-mail com pessoas externas à organização, certifique-se de que ela é realmente a pessoa que diz ser. Não forneça informação particular de outro usuário. Se necessário, faça você o contato com o usuário

6. Ao receber um visitante, garanta que ele estará sempre acompanhado por alguém da organização durante sua estadia nas instalações físicas. Ao final, acompanhe a pessoa até a portaria

Cordialmente,

Equipe de segurança da informação

GLOSSÁRIO

Criptografia: Conjunto de regras cujo objetivo é codificar uma mensagem através de algoritmos, de forma que somente o emissor e o receptor consiga interpretá-la.

Domínio: Método de organizar e gerenciar a rede através de um servidor denominado controlador de domínio, sendo possível aplicar Políticas de Segurança da Informação, gerenciar todas as máquinas e usuários da rede de forma que não seja necessário realizar essas configurações individualmente as máquinas clientes.

Engenharia Social: Método de ataque, onde o engenheiro social utiliza-se da persuasão, aproveitando da ingenuidade da vítima para obter informações que podem ser utilizadas para conseguir acesso à informações privilegiadas, e/ ou confidenciais.

ERP: São sistemas de gestão empresarial que integram os setores da empresa, automatizando processos, de forma que os departamentos trabalhem sincronizados, centralizando os dados em uma única base, evitando perda de informações, reduzindo custos e melhorando produtividade.

***Firewall**:* É um dispositivo de segurança que pode ser baseado em hardware ou software que, através de regras estabelecidas pelo administrador de redes, determina quais tipos dados provenientes de redes externas podem ser transmitidos ou recebidos.

***PIN*:** Número de identificação pessoal, geralmente utilizado em *smartcars* e *tokens.*