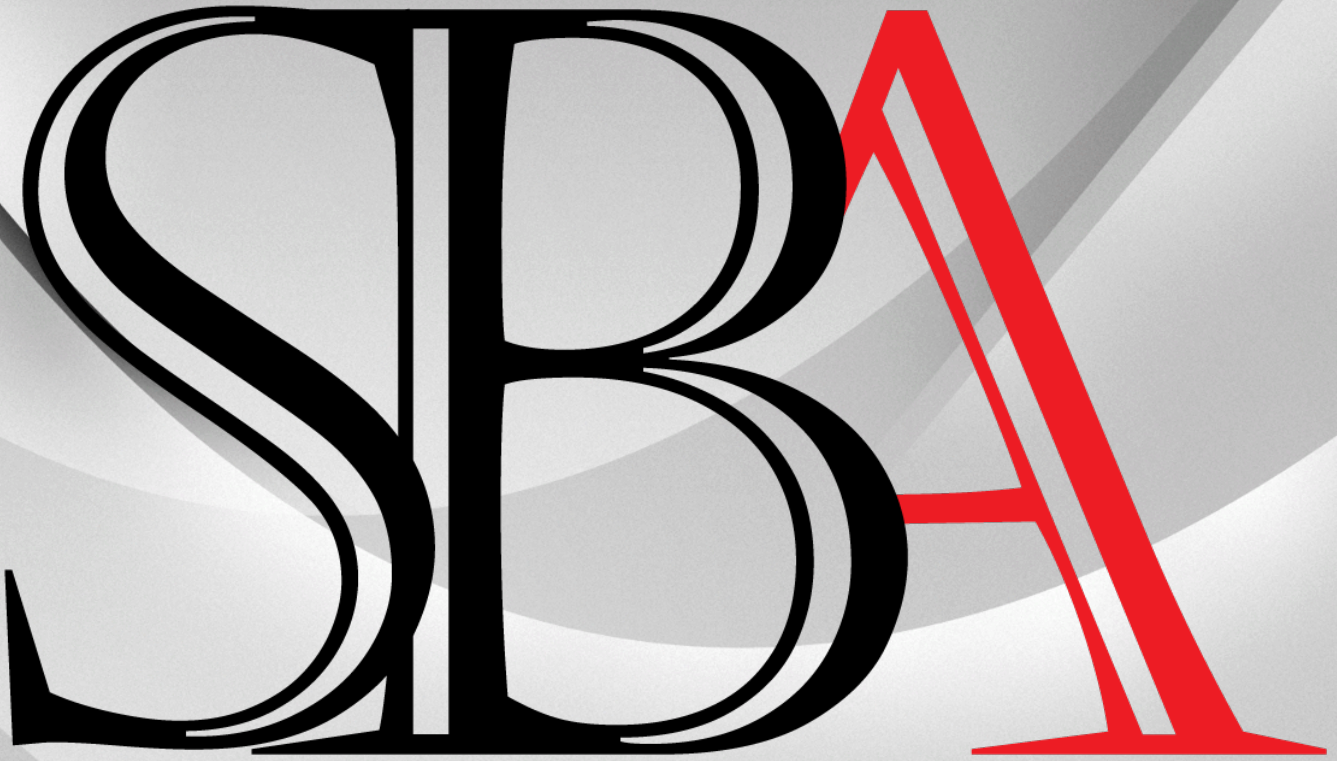


SARAIVA BARROSO & ARAÚJO

ADVOCACIA

SEGURANÇA DA INFORMAÇÃO:

Aspectos jurídicos

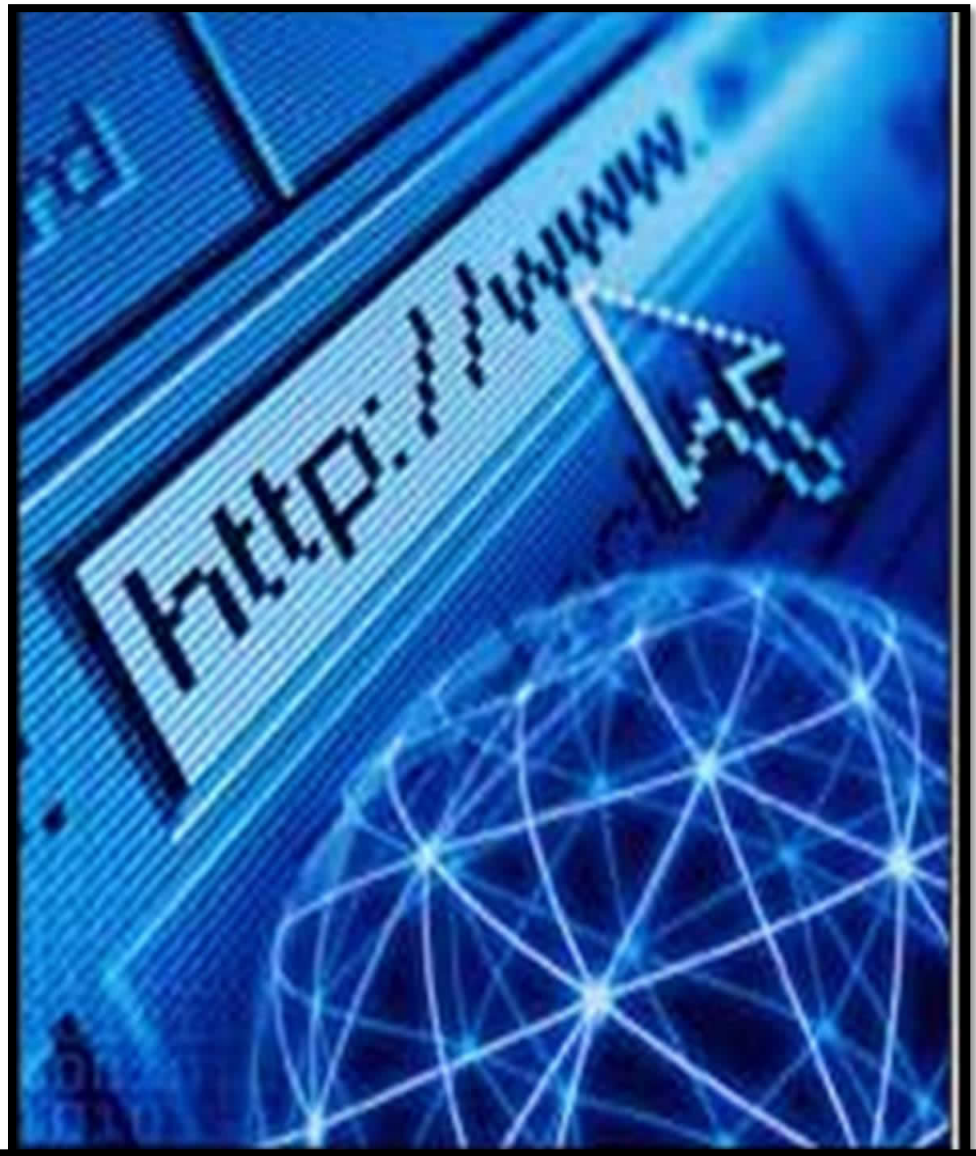
INTERNET: O PARADIGMA ATUAL

INFORMAÇÃO: O PRINCIPAL ATIVO

Qual a sensação que a frase "***SEM CONEXÃO COM A INTERNET***" provoca em você?

INFORMAÇÃO COMO UM ATIVO

Toda informação que seja valiosa e que possa causar dano ou prejuízo ao ser perdida ou extraviada **deve ser PROTEGIDA!**



O PANORAMA ATUAL DA INTERNET

Home - Segurança

Segurança cibernética: mundo gastou US$ 41,76 bilhões em 2012

:: Ana Paula Lobo*
:: Convergência Digital :: 19/06/2013

O mundo gastou US$ 41,76 bilhões com segurança cibernética em 2012 e esses gastos devem crescer progressivamente nos próximos cinco anos para proteção às infraestruturas consideradas críticas como telecom, energia, saúde e transporte público, projeta estudo da ABI Research. Na Europa, o presidente dos EUA, Barack Obama, enfrentou as críticas da chanceler da Alemanha, Angela Merkel, e disse que "o monitoramento é necessário e exige equilíbrio".

Fonte: Convergência Digital

Brasil registra mais de 2,2 milhões de tentativas de fraudes

:: Da redação
:: Convergência Digital :: 28/01/2014

Em 2013, foram registradas 2.204.158 tentativas de fraude conhecida como roubo de identidade, em que dados pessoais são usados por criminosos para firmar negócios sob falsidade ideológica ou mesmo obter crédito com a intenção de não honrar os pagamentos, de acordo com o Indicador Serasa Experian de Tentativas de Fraudes – Consumidor, divulgado nesta terça-feira, 28/01.

Isso representa uma tentativa de fraude a cada 14,5 segundos no país. Esse resultado é o recorde histórico registrado pelo indicador, apresentado alta de 3,04% em comparação a 2012, em que foram registrados 2,1 milhões de tentativas; alta de 12,39% em relação a 2011, que teve 1,9 milhão e, alta de 17,56% em relação a 2010, com 1,8 milhão. Telefonia respondeu pelo maior número de registros em 2013, com 951.360, 43,16% do total de tentativas de fraude registradas no ano.

Aumentam ataques malware a contas bancárias no Brasil

:: Da redação
:: Convergência Digital :: 28/01/2014

A Trend Micro, empresa especializada em segurança, alerta para uma forma de ataque a operações bancárias que vem crescendo no Brasil, representando mais de 40% de todos os crimes dessa espécie em 2013.

26/01/2012 19h23 - Atualizado em 27/01/2012 13h00

Universidade do RS se desculpa por vazar dados de 23 mil alunos

Objetivo era divulgar vaga de estágio, mas arquivo com dados foi anexado. Unisinos diz que lamenta ocorrido e que responsável foi demitido.

Altieres Rohr
Especial para o G1

Um arquivo contendo dados pessoais de alunos da Universidade do Vale do Rio dos Sinos (Unisinos) foi enviado por e-mail a estudantes da instituição gaúcha na tarde da última segunda-feira (23). A mensagem deveria apenas comunicar oportunidades de estágio a alunos do curso de arquitetura, mas o responsável pelo envio anexou o documento por engano, diz a Unisinos.

Enem: Twitter leva à eliminação de mais de 10 candidatos

Redação do IDG Now! Siga @idgnow 24/10/2011 - 08h23 - Atualizada em 24/10/2011 - 08h41

Durante o Exame Nacional do Ensino Médio, mais de dez pessoas foram eliminadas por acessarem a rede social durante as provas.

MEC confirma vazamento de dados de inscritos no site do Enem

Redação do IDG Now! Siga @idgnow 04/08/2010 - 10h14 - Atualizada em 15/03/2012 - 12h26

Informações como o nome do aluno, o número da inscrição, RG, o CPF e o nome completo da mãe do candidato ficaram com acesso livre na tarde de ontem.

Fonte: IDG Now!

Camelôs vendem CD com CPF e telefone por R$ 80 na Capital

CD contém informações sigilosas de empresas e pessoas físicas. Ministério Público investiga o caso. Há risco de os dados caírem nas mãos de criminosos

LUÍS ALFREDO DOLCI

Informações sigilosas de empresas e de pessoas físicas, que deveriam ser guardadas a sete chaves, são compradas livremente no centro da Capital. O DIÁRIO pagou R$ 80 por CDs que trazem milhares de dados como nome, endereço, telefone e até o número do Cadastro Pessoa Física (CPF) e Cadastro Nacional de Pessoa Jurídica (CNPJ) da Grande São Paulo e do Interior do estado.

Em mãos erradas e interessadas em bancos de dados, cadastros como estes podem ter inúmeras utilidades. As informações podem ser usadas para formação de clientela para empresas que trabalham com mala direta ou até mesmo servir como pontapé inicial para a ação de criminosos. A reportagem do DIÁRIO esteve na Rua Santa Ifigênia, região tradicionalmente conhecida pelo comércio de produtos de informática, e adquiriu em um camelô dois CDs, com um programa chamado Lista Brasil. "É o CD mais recente que a gente tem aqui. Vendo por R$ 100, mas faço um desconto e sai por R$ 80 se quiser comprar na hora", disse a vendedora que atendeu o repórter.

Sem fiscalização

"Isso que eu estou fazendo é errado, é cadeia na hora, mas espera aqui porque vou buscar com quem vende", comentou. Cinco minutos depois, a vendedora ambulante volta ao local com os dois CDs — um para a instalação do programa e outro que permitia acesso ao banco de dados. Outro camelô da Rua Santa Ifigênia ofereceu o mesmo CD por R$ 500. "Quanto você tem agora? Faço por R$ 200 e trago aqui amanhã", revelou o vendedor, mostrando que o comércio de bancos de dados sigilosos é uma prática comum e que ocorre sem qualquer tipo de fiscalização. Para atestar que o banco de dados trazia dados corretos, dois jornalistas do DIÁRIO consultaram o programa, e encontraram seu CPF, nome, endereço completo e telefone.

Logo após comprar os CDs, a reportagem do DIÁRIO entregou o material na sede do Grupo de Atuação Especial de Combate ao Crime Organizado (Gaeco), do Ministério Público Estadual, que fica em Higienópolis. O promotor José Reinaldo Carneiro, do Gaeco, informou que o material será anexado à investigação que já foi aberta pelo Ministério Público Estadual.

Segundo o promotor, a venda de informações deste tipo é ilegal e caracteriza violação de segredo profissional, previsto pelo artigo 154 do Código Penal, e que prevê de um a quatro anos de reclusão.

Estelionato

"O Ministério Público já investiga há alguns anos esse tipo de crime. Ao mesmo tempo em que as autoridades precisam passar por toda uma burocracia para obter algumas dessas informações durante uma investigação, camelôs revendem esses dados livremente", afirmou o promotor do Gaeco.

Carneiro lembrou que o comprador do CD pode ser investigado por estelionato e até mesmo falsidade ideológica. "Um banco de dados como esse, principalmente com dados de CPF e CNPJ, pode ser usado para produção de documentos falsos, por exemplo", explicou. O Gaeco já realiza uma investigação para apurar o comércio destes softwares na região central da Capital — principalmente na Rua Santa Ifigênia e também na Praça da Sé. "A investigação não pode ficar restrita apenas aos camelôs. Já iniciamos uma apuração bem mais detalhada para descobrir como funciona essa rede de comércio ilegal de bancos de dados", disse o promotor José Reinaldo Carneiro.

De acordo com a advogada Patricia Peck, especializada em direito digital, o funcionário de empresa ou órgão público que é flagrado vazando informações pode ser demitido por quebra de sigilo profissional, conforme prevê o artigo 482 da CLT.

Hoje, a instalação de jogos e programas no computador pela internet são uma das portas de entrada para vazamento de dados sigilosos de empresas e órgãos públicos. "Por isso é cada vez mais importante as empresas adotarem uma política de controle de dados. Um simples cupom preenchido em um posto de gasolina ou um formulário na internet podem cair em um desses bancos de dados e ser utilizado de forma indevida", explicou a advogada.

O Código de Defesa do Consumidor (CDC) também proíbe o comércio de dados de consumidores. Já o Código Civil prevê ressarcimento nos casos em que funcionários de empresas ou servidores são flagrados violando informações sigilosas.

frases

"É o CD mais recente que a gente tem aqui na rua. Vendo por R$ 100 mas faço um desconto e sai por R$ 80, mas só se quiser comprar na hora"
Camelô na Rua Santa Ifigênia

"Isso que eu estou fazendo é errado, dá cadeia na hora,

Vazamento de dados da Receita

Não são apenas informações como telefone, endereço, CPF e CNPJ que estão à venda no comércio ambulante da Capital. Dados ainda mais sigilosos, que são exclusivos da Receita Federal, também são revendidos pelos camelôs.

"Esse programa da Receita também tem para vender aqui, mas é bem mais caro. Custa uns R$ 15 mil. É caro mas vale a pena, tem tudo o que você possa imaginar", disse uma vendedora na Rua Santa Ifigênia.

A Receita Federal confirma que dados confidenciais de contribuintes pessoas físicas e preso durante as investigações, acusado de vazar os dados confidenciais dos contribuintes.

Ministério Público

O promotor José Reinaldo Carneiro, do Grupo de Atuação Especial de Combate ao Crime Organizado (Gaeco) do Ministério Público Estadual, disse que também há investigações sobre o comércio do banco de dados da Receita. "Estamos investigando para saber exatamente de onde saem essas informações e como esses dados chegam até o comércio ambulante da Capital", afirmou o

O outro lado

Empresa nega participação

Procurada pelo DIÁRIO, a TradeServ Empreendimentos e Serviços, que produz a Lista Brasil, informou que produziu em 2002 um sistema que permitia a leitura de banco de dados, com informações que traziam nome, endereço e telefone de consumidores de todo o país.

Os dados, segundo a empresa, eram extraídos a partir de listas telefônicas, e

ELIÁRIA ANDRADE/ DIÁRIO

IMPACTOS DE INCIDENTES DE SEGURANÇA SOBRE OS NEGÓCIOS

- ❑ Tempo necessário para recuperar o sistema
- ❑ Queda na produtividade
- ❑ Perda da credibilidade da empresa
- ❑ Perda de oportunidades de negócio
- ❑ Queda na competitividade

RISCOS DO EMPREGO DE MEIOS ELETRÔNICOS NO AMBIENTE CORPORATIVO

SEGURANÇA

ATAQUES E AMEAÇAS

Pesquisa: 59% dos ex-funcionários desviam dados corporativos

Empresas perderam mais de US$ 1 trilhão com roubo de dados em 2008

SEGURANÇA

ATAQUES E AMEAÇAS

Aumentam ataques a sites de empresas

Fonte: IDG Now!

"We don't pay much attention to information security.
We're hoping our competitors will steal our ideas
and become as unsuccessful as we are."

O PANORAMA ATUAL DA INTERNET

Empresas levam, em média, 10 horas para admitir uma falha de segurança

Convergência Digital - Hotsite Cloud Computing
:: Ana Paula Lobo* :: 01/07/2013

As empresas levam, em média, até 10 horas para reconhecer uma falha de segurança, mesmo que 35% digam que são capazes de fazer essa identificação num curto prazo de tempo, revela estudo divulgado pela McAfee. O levantamento, que ouviu CTOs nos EUA e na Europa, mostra ainda que mais de um quinto dos entrevistados (22%) afirmou que precisaria de um dia para identificar uma violação, enquanto 5% disseram que esse processo levaria até uma semana.

Fonte: Convergência Digital

Site do Tribunal de Justiça amanhece hackeado neste domingo

06/10/2013 - 10h06 - Atualizado em 06/10/2013 - 21h18

LER DEPOIS

Com uma imagem de uma mulher com a boca amordaçada, o site apresenta apenas uma mensagem em árabe

O site do Tribunal de Justiça do Espírito Santo (TJ-ES) amanheceu invadido por um hacker neste domingo (6). Com uma imagem de uma mulher com a boca amordaçada, o site apresenta apenas uma mensagem em árabe, que traduzida informa que o site foi hackeado por "Dr Anestesia".

Depois da invasão, a página do Tribunal de Justiça saiu do ar. Por volta das 18h, o site voltou ao funcionamento normal, informou a assessoria de comunicação.

Fonte: GAZETA ONLINE

ESTATÍSTICAS

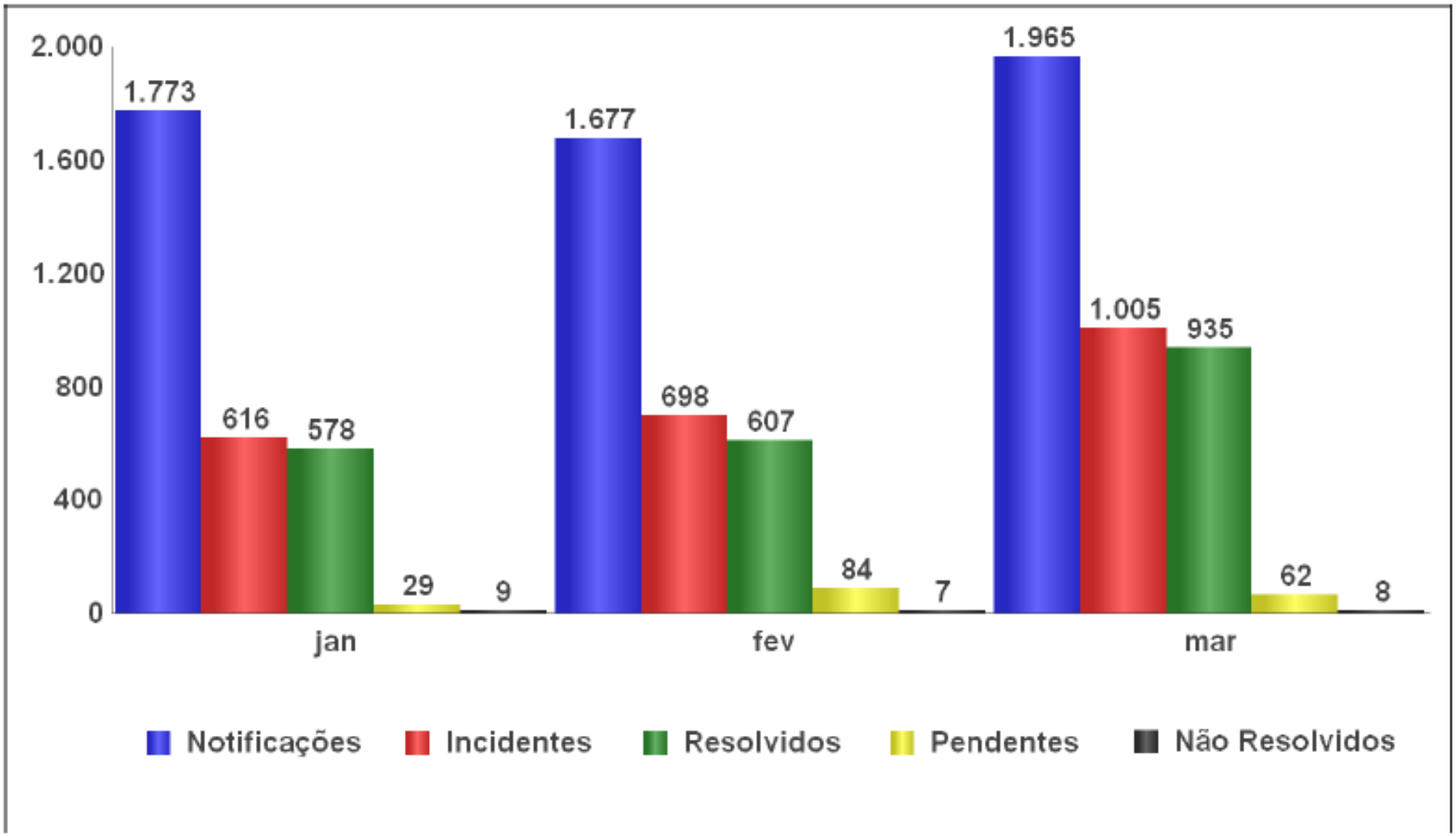
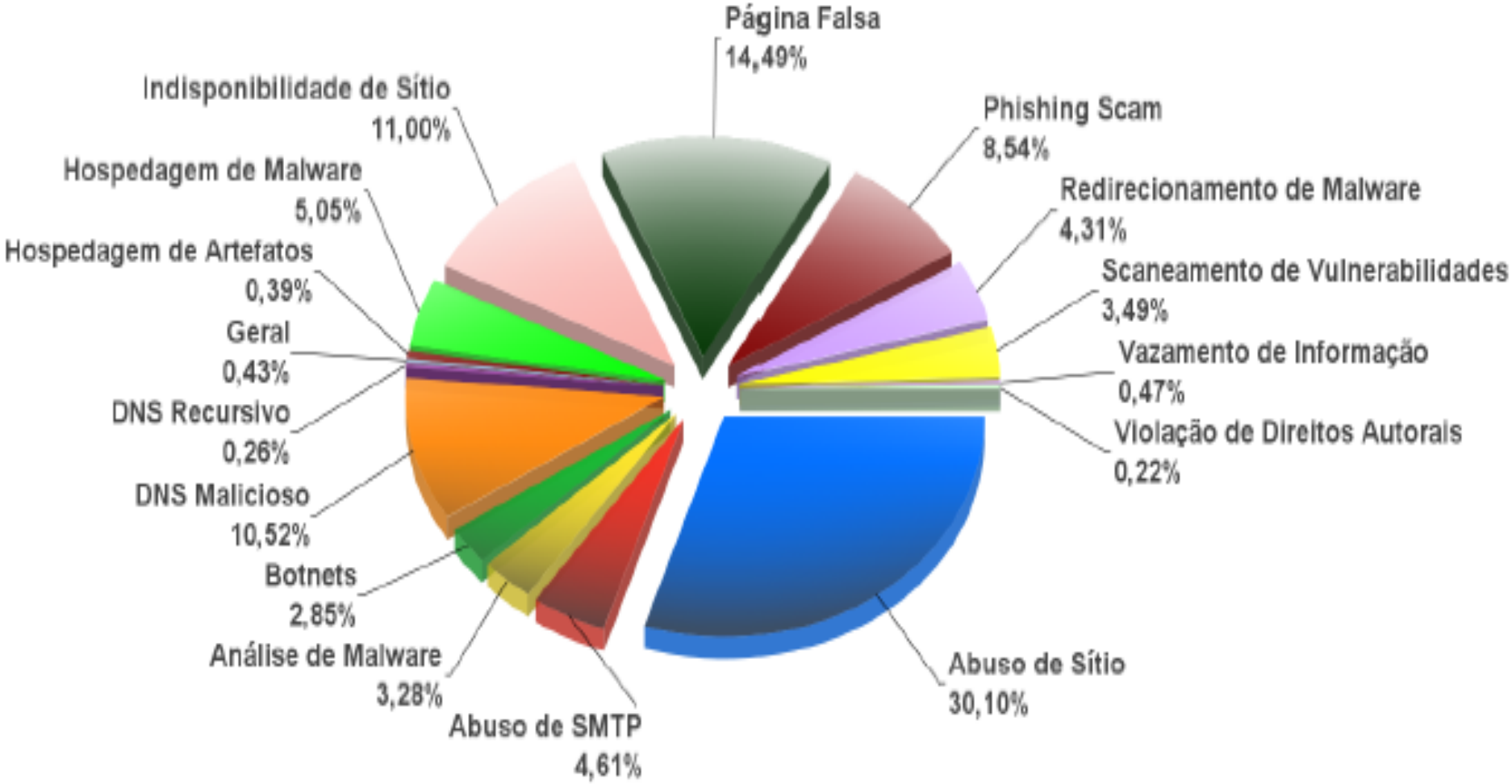


Gráfico 1 – Distribuição de notificações por *status* e mês de criação

ESTATÍSTICAS



ESTATÍSTICAS: Tempo de resolução

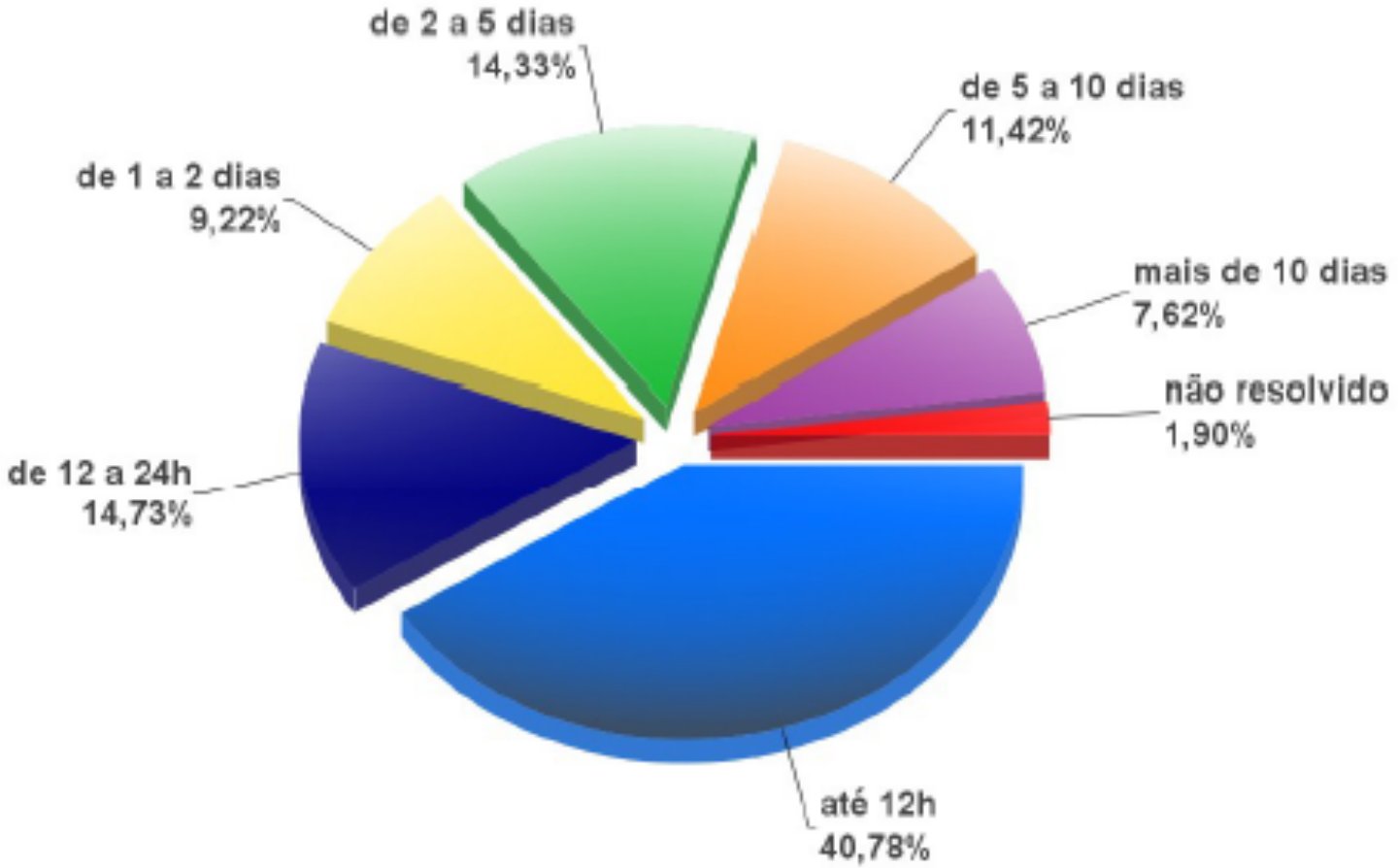


Gráfico 8 – Tempo de resolução

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O TRT13 definiu e criou sua ***Política de Segurança da Informação (PSI)*** *que define* responsabilidades, direitos e deveres que devem ser conhecidos e seguidos por todos os colaboradores da instituição.

A ***PSI*** visa promover a implementação e o bom funcionamento de uma cultura institucional de proteção às informações do TRT13.

OBJETIVOS

✓ **Estabelecer padrões** de procedimentos a serem adotados que visem a efetiva manutenção da segurança das informações do TRT13;

✓ Buscar, através da implementação de medidas de Segurança da Informação, **garantir a Disponibilidade, Integridade, Confidencialidade e Autenticidade das informações;**

✓ Assegurar que todos os procedimentos adotados pela instituição, que visem a efetivação da proteção às suas informações, estejam em conformidade com o quadro normativo vigente.

PÚBLICO ALVO

- ✓Magistrados,
- ✓Servidores (efetivos, requisitados e cedidos)
- ✓Terceirizados
- ✓Consultores,
- ✓Estagiários,
- ✓Pensionistas,
- ✓Jurisdicionados
- ✓Inativos

SEGURANÇA DA INFORMAÇÃO

Segurança da Informação busca ***garantir a proteção da informação*** *de vários tipos de ameaças, visando conferir a* ***continuidade do negócio****,* ***minimizando riscos*** *e* ***aumentando o retorno sobre os investimentos e oportunidades de negócio****.*

OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO

Confidencialidade

- Assegurar que a informação é acessível somente por aqueles devidamente autorizados

Integridade

- Salvaguardar a veracidade e complementariedade da informação bem como os seus métodos de processamento

Disponibilidade

- Assegurar a quem devidamente autorizado o acesso à informação sempre que necessário

OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO

Autenticidade

- Assegurar a identidade do emissor e do receptor das mensagens.

Não repúdio

- Impossibilidade de o emissor do documento negar sua autoria.

CONFIDENCIALIDADE

CONSTITUIÇÃO FEDERAL DE 1988 – art. 37

§ 7º **A lei disporá sobre** os requisitos e as restrições ao ocupante de cargo ou emprego da administração direta e indireta que possibilite o **acesso a informações privilegiadas**.

CÓDIGO PENAL – art .153

§ 1º-A. **Divulgar**, sem justa causa, **informações sigilosas ou reservadas**, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:

LEI 11.419/06

Art. 12 § 1º **Os autos** dos processos eletrônicos **deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados**, sendo dispensada a formação de autos suplementares.

CÓDIGO PENAL

Art. 154-A. **Invadir dispositivo informático** alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e **com o fim de obter, adulterar ou destruir dados ou informações** sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

DISPONIBILIDADE

CONSELHO NACIONAL DE JUSTIÇA - RESOLUÇÃO Nº 90/2009

Art. 8º. **As informações sobre processos, seus andamentos e o inteiro teor dos atos judiciais** neles praticados **devem ser disponibilizados na internet**, ressalvadas as exceções legais ou regulamentares.

CONSELHO NACIONAL DE JUSTIÇA - RESOLUÇÃO Nº 121/10

Art. 1º. **A consulta** aos dados básicos dos processos judiciais **será disponibilizada na rede mundial de computadores (internet)**, assegurado o direito de acesso a informações processuais a toda e qualquer pessoa, independentemente de prévio cadastramento ou de demonstração de interesse.

Parágrafo único: No caso de processo em sigilo ou segredo de justiça não se aplica o disposto neste artigo.

FUNDAMENTOS DA SEGURANÇA DA INFORMAÇÃO

Administração Pública

- Constituição Federal 1988: Princípios Constitucionais da Administração Pública (Legalidade, Impessoalidade, Moralidade, Publicidade, Eficiência)
- Legislação infraconstitucional (Código Civil, Código Penal, Consolidação das Leis do Trabalho, Lei 8.027/90, Lei 8.112/90, Lei 11.419/06, Lei 12.527/11, Lei 12.737/12, Lei 12.965/14)
- Medida Provisória Nº 2.200-2/2001
- Decreto Federal (Decreto 3505/2000 – Administração Pública Federal)
- Resoluções CNJ (Res. 90/11, Res. 121/10, Res 185/13)
- Resoluções CSJT (Res. 88/11, Res. 136/14, Res. 154/15)
- Regimento Interno TRT 13ª Região
- Regulamento Geral do TRT 13ª Região
- Resolução Administrativa 024/2015 TRT13ª Região
- Outros...

FUNDAMENTOS DA SEGURANÇA DA INFORMAÇÃO

Constituição Federal 1988:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, **garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito** à vida, à liberdade, à igualdade, à segurança e **à propriedade**, nos termos seguintes:

Art. 37. **A administração pública direta** e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios **obedecerá aos princípios de** legalidade, impessoalidade, moralidade, **publicidade e eficiência** e, também, ao seguinte:

§ 6º **As pessoas jurídicas de direito público** e as de direito privado prestadoras de serviços públicos **responderão pelos danos que** seus agentes, nessa qualidade, **causarem a terceiros**, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

Código Civil Brasileiro - Lei 10406/2002:

Art. 186. Aquele que, por **ação ou omissão voluntária, negligência, imprudência**, violar direito e **causar dano** a outrem, ainda que exclusivamente moral, **comete ato ilícito**.

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica **obrigado a repará-lo**.

Art. 932. São também responsáveis pela reparação civil:
III - **o empregador** ou comitente, **por seus empregados**, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele;

Art. 933. As pessoas indicadas nos incisos I a V do artigo antecedente, **ainda que não haja culpa de sua parte**, responderão pelos atos praticados pelos terceiros ali referidos.

FUNDAMENTOS DA SEGURANÇA DA INFORMAÇÃO

Política de Segurança da Informação da Administração Pública Federal – Decreto 3505/00:

Art. 1º Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos:
I - assegurar a **garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações**, nos termos previstos na Constituição;[...]
V - **criação, desenvolvimento e manutenção de mentalidade de segurança da informação**; [...]
VII - **conscientização** dos órgãos e das entidades da Administração Pública Federal **sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade**.

CONSELHO NACIONAL DE JUSTIÇA - RESOLUÇÃO Nº 90/2009
Art. 13. O **Tribunal deve elaborar e aplicar Política de Segurança da Informação**, por meio de um Comitê Gestor, alinhada com as diretrizes nacionais.

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO

- Propor e revisar as normas de SI
- Dirimir dúvidas e deliberar em casos omissos
- Propor e acompanhar planos de ação de SI
- Analisar as comunicações de descumprimento da política
- Solicitar a realização de auditorias de TIC, etc.

CLASSIFICAÇÃO DA INFORMAÇÃO

✓ Garantir seu **uso racional**;

✓ **Prevenir que informações restritas sejam reveladas a** público, violando os preceitos de proteção da confidencialidade estabelecidos em lei;

✓ **Evitar danos ou perda do conhecimento institucional**

CLASSIFICAÇÃO DA INFORMAÇÃO: Confidencialidade

INFORMAÇÃO PÚBLICA

- Informações que podem ser divulgadas a qualquer pessoa.

CLASSIFICAÇÃO DA INFORMAÇÃO: Confidencialidade

INFORMAÇÃO RESTRITA

- Informações que, em razão de Lei, devam ser de conhecimento reservado e, portanto, requeiram medidas especiais de segurança de salvaguarda.

CLASSIFICAÇÃO DA INFORMAÇÃO: Confidencialidade

INFORMAÇÃO RESTRITA

- Informações pessoais, relativas à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias fundamentais;
- Informações sigilosas nos termos da Lei 12.527/11;
- Informações de processos que tramitem em segredo de justiça;
- Informações protegidas por sigilo fiscal;
- Demais hipóteses do art. 22 Lei 12.527/11.

MANUSEIO DA INFORMAÇÃO

✓**Nunca deixe documentos** que não estão em uso **espalhados** sobre mesas ou bancadas de trabalho;

✓**Informações classificadas** como restritas **devem** sempre **ser armazenadas de forma controlada**.

✓**Mantenha documentos sempre em gavetas** ou armários com chaves.

✓**Para e-mail** e outros documentos eletrônicos, **faça o armazenamento em pastas seguras**.

MESA E TELA LIMPAS

✓Evite deixar **documentos ou mídias expostas sobre mesas** ou estações de trabalho;

✓Quando se ausentar de sua estação de trabalho, **verifique se seus documentos estão protegidos** e armazenados em gavetas ou armários, preferencialmente trancados com chave.

MESA E TELA LIMPAS

Dica: Na maioria dos sistemas operacionais **o bloqueio dos computadores pode ser** feito usando a combinação simultânea das teclas **Ctrl+Alt+Del** seguidas da opção "**Bloquear este computador".**

MANUSEIO DA INFORMAÇÃO

✓Não utilize a estrutura tecnológica do TRT13 para armazenamento de **material que infrinja direitos autorais**;

✓**Não é permitido o armazenamento de jogos eletrônicos**, material adulto ou de mau gosto, especialmente pornografia infantil (pedofilia);

✓**Nunca armazene material audiovisual** como músicas, vídeos, imagens, flash vídeo e qualquer outro similar, a menos, é claro, que se trate de informação autorizada pelo TRT13;

✓**Nunca tente ou permita que uma pessoa obtenha acesso não autorizado** a unidades de rede. Infrações deverão ser sempre comunicadas ao Comitê de Segurança.

POLÍTICA DE SENHAS

CREDENCIAIS E SENHAS DE ACESSO

✓**Nunca revele suas senhas** a outros usuários ou terceiros;

✓**Não tente obter acesso a sistemas** e a outros recursos com credenciais de outros usuários;

✓**Nunca se utilize de eventuais falhas em sistemas** para obter acesso não autorizado.

POLÍTICA DE SENHAS

✓Nunca utilize parte da credencial como base para sua senha;

✓**Nunca utilize nomes de familiares, amigos, colegas de** trabalho ou datas importantes, como aniversários;

✓**Não utilize palavras existentes em qualquer dicionário,** mesmo gírias ou jargões;

✓**Não use qualquer variação ou parte do nome Tribunal Regional do Trabalho;**

✓**Não utilize qualquer variação dos itens acima invertido ou** seguido por um número

POLÍTICA DE SENHAS

Para escolha de uma boa senha, siga as seguintes dicas:

✓**Utilize senhas com pelo menos 8 (oito) caracteres;**
✓**Utilize letras MAIUSCULAS e minúsculas;**
✓**Acrescente números (0-9) e caracteres especiais, como** !#$%&;

Dica: Nunca escreva ou anote sua senha. Caso você prefira uma senha fácil de lembrar, utilize um método para substituição de letras por similares ou caracteres especiais. Por exemplo, uma senha como ***Senha123! Pode ser escrita como 53nh@123!. Desta forma,*** você vai conseguir lembrar sua senha e ainda manter um bom nível de complexidade.

POLÍTICA DE SENHAS

IMPORTANTE: Nunca utilize senhas encontradas em exemplos. O fato da senha *53nh@123! constar nesta cartilha automaticamente a* torna uma senha fraca!

E lembre-se! Se por qualquer motivo você achar que sua senha foi comprometida ou está sendo utilizada por outra pessoa, contate imediatamente a Comitê de Segurança da Informação. Desta forma, você não apenas está ajudando a identificar uma falha no sistema ou um uso indevido, mas também estará demonstrando que não está envolvido no incidente.

TRIBUNAL REGIONAL DO TRABALHO 10ª REGIÃO
Processo: **01005-2007-020-10-00-4 ROPS** (Acordão 1ª Turma)
Origem: 20ª Vara do Trabalho de BRASÍLIA/DF
Juíz(a) da Sentença: Thais Bernardes Camilo Rocha
Relatora: Desembargadora Maria Regina Machado Guimarães

EMENTA

DEMISSÃO MOTIVADA. **EMPREGADO QUE**, DETENDO SENHA DE ACESSO DO MAIS ALTO NÍVEL EM SISTEMA INFORMATIZADO, **FORNECE ESSA SENHA A TERCEIRO SEM AUTORIZAÇÃO PARA TANTO**. Se, de uma forma geral, a simples cessão de senhas de acesso a sistemas não representa "per se" ato necessariamente grave, tal gravidade pode bem emergir das circunstâncias específicas em que tal fato se dá. É o que ocorre "in casu", posto que a senha cedida a terceiro era do mais elevado nível nos sistemas da demandada, e possibilitava o mais amplo acesso a todos os sistemas informatizados. **A violação de seu sigilo poderia causar não apenas possíveis danos financeiros à empregadora, mas também - por força da natureza das atividades médico/hospitalares da ré - resultar em violação de informações protegidas pela confidencialidade médica.** Em caso extremo, tal acesso poderia até mesmo resultar no uso de dados errôneos que comprometessem negativamente os tratamentos prescritos a pacientes atendidos pela demandada. Por esse motivo é que **o obreiro não poderia, sem autorização expressa ou tácita da demandada, cedê-la a terceiro. Se o fez, sua demissão é motivada nos termos do art. 482, "g" e "h", da CLT.**

CÓDIGOS MALICIOSOS: COMO EVITAR INFECÇÕES?!

✓**Nunca execute arquivos não solicitados** recebidos por correio eletrônico ou outras fontes, mesmo que sejam de pessoas conhecidas. Caso seja necessário abrir o arquivo, esteja certo que o mesmo foi analisado pelo software de antivírus;

✓**Nunca utilize mídias de armazenamento removível** CDs, DVDs, cartões, pen drives e similares sem primeiro realizar uma varredura com o software de antivírus.

✓**Não utilize intencionalmente** softwares ou aplicativos que possuam ou possam conter vírus e outros códigos maliciosos.

ENGENHARIA SOCIAL

O termo **Engenharia Social é concebido como o ato de manipular** pessoas para que executem tarefas ou forneçam informações que podem ser utilizadas para obter acesso não autorizado a outros recursos e informações.

A Engenharia Social **abusa da ingenuidade e credulidade de usuários**, evitando um processo longo para quebrar senhas ou explorar vulnerabilidades e falhas existentes em sistemas.

ENGENHARIA SOCIAL

✓Esteja atento para **abordagens via telefone** ou qualquer outro meio de comunicação onde uma pessoa – geralmente falando em nome de uma instituição – solicita diversas informações, incluindo confidenciais;

✓O **Service Desk** do TRT13 **não solicita informações sigilosas ou credenciais** de acesso por telefone ou e-mail. Sob nenhuma hipótese forneça essas informações;

✓Instituições legítimas evitam enviar mensagens de correio eletrônico não solicitadas. **Desconfie de qualquer mensagem que solicite informações** e para tirar a dúvida, procure entrar em contato com o Comitê Gestor de Segurança da Informação.

USO DE SOFTWARES E APLICATIVOS

✓**O TRT13** respeita integralmente a lei de software e **trabalha exclusivamente com softwares licenciados**;

✓**Não instale ou utilize de forma portátil** softwares não homologados ou pessoais;

✓**Não use softwares que possam causar dano** ou comprometer a segurança do TRT13;

✓**Todas as instalações de software deverão ser feitas pelo Service Desk**. Nunca tente instalar ou utilizar um software não homologado.

USO DE SOFTWARES E APLICATIVOS

Dica:

Caso você acredite que necessite de um software que não se encontra disponível, entre em contato com o **Service Desk** ou com o **Comitê Gestor de Segurança da Informação**. Sua sugestão será bem vinda e cuidadosamente analisada.

DISPOSITIVOS MÓVEIS

✓Em locais movimentados como aeroportos, shoppings e similares esteja sempre atento ao seu ambiente. A pressa pode facilitar a ação de ladrões ou mesmo o esquecimento do equipamento;

✓Verifique o ambiente ao seu redor quando estiver acessando informações sigilosas. Lembre-se que em um ambiente público uma pessoa próxima pode observar furtivamente por cima do seu ombro enquanto você utiliza um arquivo ou digita uma senha;

✓Antes de viagens ou ausências prolongadas, solicite ao Service Desk uma revisão do seu backup. Desta forma, você estará resguardado no evento de um furto.

Quase 80% das empresas sofreram incidentes de segurança móvel em 2012

Da Redação Seguir @idgnow

13 de junho de 2013 - 09h00

Cerca de 50% das empresas participantes do estudo da Check Point reportaram que incidentes de segurança móvel custaram mais de US$ 100 mil

Fonte: IDG Now!

"We don't pay much attention to information security.
We're hoping our competitors will steal our ideas
and become as unsuccessful as we are."

ACESSO À INTERNET E REDES EXTERNAS

✓Sempre se autentique através de usuário e senha antes de obter acesso a internet;

✓O **acesso a internet não é um beneficio**. Utilize-o exclusivamente para realização de atividades profissionais ou aprovadas pelo TRT13;

✓Não acesse sites ou serviços na internet que possam resultar em falhas de segurança na infraestrutura computacional do TRT13.

ACESSO À INTERNET E REDES EXTERNAS

Usuários **não devem acessar** sites com conteúdo pertencente às seguintes categorias:

- ✓Material adulto ou de mau gosto;
- ✓Pornografia infantil (pedofilia);
- ✓Material que incite o uso de drogas, terrorismo, praticas subversivas, violência, aborto, práticas racistas, assim como qualquer outro que possa infringir a legislação vigente;
- ✓Sites de relacionamento e redes sociais;
- ✓Jogos e/ou qualquer tipo de recreação;
- ✓ Sites de streaming de áudio ou vídeo.

ACESSO REMOTO

✓A concessão do acesso remoto é feita com base no principio do mínimo recurso necessário, ou seja, você normalmente não terá acesso a toda rede, mas apenas ao recurso que precisa para trabalhar;

✓O **usuário é o único responsável por toda ação executada com suas credenciais.** Dessa forma, você é responsável por seguir todas as medidas de segurança que garantam que pessoas não autorizadas não obtenham acesso remoto;

✓Caso esteja usando dispositivos de autenticação como tokens ou smatcards, zele pelo bom uso e segurança dos mesmos;

✓Nunca tente obter acesso remoto a recursos aos quais não esteja autorizado.

CORREIO ELETRÔNICO

✓Utilize o sistema **unicamente para** transmissão e recebimento de mensagens relacionadas com **atividades profissionais**;

✓Seja cortês, utilize boas práticas de escrita e evite termos ou palavras de baixo calão;

✓**Nunca envie qualquer informação classificada** como de restrita através de endereços eletrônicos pessoais;

✓Não inscreva seu endereço de correio eletrônico em listas de distribuição que não tenham relacionamento com atividades profissionais;

CORREIO ELETRÔNICO

✓Nunca faça disseminação de informações de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;

✓Nunca tente utilizar o sistema de correio eletrônico para forjar ou simular falsa identidade;

✓Não utilize o sistema de correio eletrônico para disseminar mensagens caracterizadas como SPAM ou que possam conter vírus e outros softwares maliciosos;

✓Quanto estiver transmitindo informações sensíveis, lembre-se de atender as recomendações de confidencialidade

CUIDADOS COM SPAM

✓**Evite divulgar seu endereço de correio eletrônico (e-mail)** em sites da internet como listas de discussão, blogs e redes sociais;

✓**Nunca responda a mensagens de SPAM. Esta é uma forma** de garantir que seu endereço eletrônico é válido e ele certamente será utilizado durante o envio de novas mensagens;

✓**Nunca utilize a estrutura computacional do TRT13 para enviar mensagens não solicitadas,** especialmente em massa;

✓**Reporte** eventuais mensagens não solicitadas **ao Service Desk**.

CORREIO ELETRÔNICO

TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO
ACÓRDÃO 00285-2002-025-04-00-3 RO

EMENTA: INDENIZAÇÃO POR DANO MORAL. Correspondências eletrônicas de conteúdo ofensivo à honra do empregado enviada por colega de serviço. **Devida a indenização por dano moral pelos atos ilícitos praticados,** quer **porque a empregadora não tomou as medidas adequadas para apurar os fatos e punir o infrator**, quer por promover, por seus prepostos, uma comemoração exatamente no dia da despedida do empregado, em clara intenção de escárnio.

TRIBUNAL REGIONAL DO TRABALHO 2ª REGIÃO
ACÓRDÃO Nº 20060375633 RO

EMENTA: Endereço eletrônico fornecido pelo empregador se equipara a ferramenta de trabalho e não pode ter seu uso desvirtuado pelo empregado. Pertencendo a ferramenta ao empregador, a esse cabe o acesso irrestrito, já que o empregado detém apenas a sua posse.

TRIBUNAL REGIONAL DO TRABALHO 2ª REGIÃO
RO 0504/2002
ORIGEM: 13ª VARA DO TRABALHO DE BRASÍLIA – DF

EMENTA: JUSTA CAUSA. E-MAIL. PROVA PRODUZIDA POR MEIO ILÍCITO. NÃO-OCORRÊNCIA.

Envio de e-mail racista por superior hierárquico a seu subordinado

"OK Sr. XXXX, pelo tipo de pele entendo a sua colocação. Este é um fato típico da senzala!!! Nós que somos de cútis mais clara não compreendemos certas considerações até porque não possuímos correntes atadas aos pés ou sofremos qualquer tipo de chibatadas quando ocorremos em fatos errados, o que não é normal, para nós HUMANOS"

TRIBUNAL REGIONAL DO TRABALHO 10ª REGIÃO
PROCESSO Nº 012.0058.2008

SENTENÇA:

"... Por conseguinte, condeno o reclamado ao pagamento da indenização no importe de R$ 268.348,00 a título de danos morais em favor do autor, sem prejuízo das atualizações de direito."

E-MAIL PARTICULAR E MONITORAMENTO

✓O TRT13 resguarda-se o direito de **monitorar e registrar o uso do sistema de correio eletrônico corporativo**. Este monitoramento tem como único objetivo validar o respeito às normas da organização, bem como produzir evidências durante eventuais violações de conduta e/ou a legislação em vigor.

ACESSO FÍSICO A ÁREAS SEGURAS

- ✓Nunca tente obter acesso a uma área segura a menos que esteja devidamente autorizado;
- ✓Sempre se identifique e registre o seu acesso a áreas seguras;
- ✓Caso esteja acompanhando um terceiro, nunca permita que este fique sozinho em uma área segura;
- ✓Não utilize dispositivos para registros áudios-visuais como câmeras, webcams, celulares, gravadores e filmadoras sem estar devidamente autorizado;
- ✓Caso precise remover algum hardware ou outro ativo de uma área segura, sempre faça um registro incluindo data, horário e motivo da retirada;
- ✓Caso você identifique alguma irregularidade, comunique imediatamente ao Comitê de Segurança

REVISÕES E COMENTÁRIOS FINAIS

O TRT13 se reserva o direito de revisar, alterar ou adicionar novas disposições às diretrizes de segurança constantes na Política de Segurança da Informação e normas com a finalidade de aprimorar e garantir a perfeita aplicabilidade e observância das regras por ele definidas. Tais alterações serão notificadas aos usuários através de meios eletrônicos.

ENCERRAMENTO

Para garantir a publicidade necessária à devida implementação das diretrizes estabelecidas no Regulamento Interno de Segurança da Informação, o mesmo estará disponível para acesso na Rede Interna do TRT13.