**Segurança de Dados: A importância de investimentos na segurança de dados**

**Anderson Silva da Conceição**IFSP, Cubatão, SP, Brasil

**Angelo Evangelista dos Santos**

IFSP, Praia Grande, SP, Brasil

**Grazielle da Silva Ribeiro**

IFSP, São Vicente, SP, Brasil

**Renato de Araújo Santos**

IFSP, Cubatão, SP, Brasil

**Resumo:** O presente artigo, possui o objetivo principal de alertar instituições públicas e privadas sobre a importância de investimentos financeiros e humanos na segurança dos dados de seus sistemas e aplicações, todos dados coletados foram extraídos de blogs ou empresas especializadas em segurança digital, incluindo a kaspersky, renomada empresa russa dona do antivírus de mesmo nome. Como resultado, conclui-se que devido falta de fortes medidas disciplinares por parte de seus colaboradores, empresas e instituições públicas investem poucos recursos financeiros e humanos em segurança.

**Palavras-Chave:** Tecnologia. Segurança da Informação. Segurança de Dados.

**Abstract:** This article has the main objective of alerting public and private institutions about the importance of financial and human investments in the data security of their systems and applications, all data collected were extracted from blogs or companies specialized in digital security, including kaspersky, renowned Russian company that owns the antivirus of the same name. As a result, it is concluded that the lack of strong disciplinary measures on the part of it’s employees, companies and public institutions invest little financial and human resources in security.

Keywords: Technology. Information Security. Data Security.

**INTRODUÇÃO**

Os ciberataques cresceram exponencialmente na última década, somente no ano de 2020, segundo dados da divisão de cibersegurança da Cisco(CISCO, 2020), revelam que ataques ransomwares, aumentaram de 33% nos ataques registrados contra organizações entre maio e julho, para 43% entre agosto e outubro deste ano, em relação ao ano anterior,no mundo todo.

Em média, houve 560 tentativas de ataque a uma única organização no Brasil, em contraste com a média global de 533, no mesmo período, segundo dados da empresa de segurança Check Point(Checkpoint, 2020), baseada em uma análise de cerca de 100 mil clientes.

Casos como do sequestro de dados do Superior Tribunal de Justiça (BBC, 2020) e da fabricante brasileira de aviões Embraer(Camurça, 2020), bem como a sobrecarga de acessos ao sistema do Tribunal Superior Eleitoral estão dentre estas estatísticas e são casos recentes e preocupantes de ciberataques a instituições brasileiras. De acordo com relatório da Kaspersky(Kaspersky, 2020), empresa russa especializada em segurança de dados, o Brasil foi o quinto país com o maior número de vítimas de dados confidenciais roubados entre os meses de abril e junho de 2020.

Em outro levantamento, também da Kaspersky, a empresa mostra que em março, abril e maio do mesmo ano, os ataques contra aparelhos celulares mais que dobraram em comparação ao período pré-pandemia. Em fevereiro de 2020, quando o Brasil teve o primeiro caso confirmado de Sars-Cov-2, as tentativas de phishing contra celulares eram de 10 por minuto; nos três meses seguintes, houve um salto para 23 tentativas por minuto.

Também houve alta no número de ataques de Phishing neste período(Kaspersky, 2020), em um dos casos o antivírus da Kaspersky, interceptou um e-mail que ofertava um kit gratuito de álcool gel e outro de máscaras. Em outro caso, o link oferecia cadastro para uma suposta isenção de tarifa de energia concedida pelo governo federal.

Segundo o portal Cio(Cio, 2020) em 2020, mais da metade das empresas sofreram ataques-phishing durante a pandemia. Em um estudo com 1.000 empresas(Barracuda, 2020), realizado pela IT Barracuda Networks, descobriu-se que 46% delas já haviam sofrido pelo menos um incidente de segurança desde o início do Lockdown. Mais da metade (51%) identificou um aumento no número de ataques de phishing por e-mail.

Apesar deste cenário, as ações do governo se mostram raras e insuficientes, visto que em seu caso mais recente, deixou que informações de mais de 200 milhões de brasileiros fossem divulgadas por conta de uma falha no código do site do órgão, os cadastramentos ficaram disponíveis para visualização de qualquer pessoa durante seis meses, um erro primário por parte da instituição, e que Demonstra ações insuficientes ou aponta para necessidade de revisão de protocolos., o caso também , escancara o perigo iminente que o cidadão brasileiro corre indiretamente com estes ataques ou falhas de segurança, pois, os dados de qualquer pessoa física ou jurídica podem estar entre estes vazamentos ou roubos de arquivos hospedados por órgãos públicos.

Esse ambiente que comporta vulnerabilidades requer uma atenção cautelosa das autoridades responsáveis, pois está sujeito a ataques e ao acesso indevido às informações armazenadas em redes corporativas e governamentais. Para evitar esses ataques cibernéticos e a perda de dados relevantes que podem prejudicar financeiramente à instituição, ou as decisões da justiça, ou até contratos com prestadores de serviços, por exemplo, é necessário investir em sistemas e serviços de TI que integrem as informações, evitem falhas e garantam a segurança dos dados(Paiva, 2020).

Portanto, com todo este cenário em mente, o presente artigo tem por objetivo analisar o cenário da segurança de dados e como o mesmo afeta o cidadão.

**CONCEITOS**

**Segurança de Dados e Ataques Cibernéticos**

Os ataques cibernéticos, também conhecidos como crimes eletrônicos, cibercrimes ou ciberataques, são crimes efetuados em ambiente virtual por Crackers. Hackers e Crackers são termos que se referem a especialistas em Segurança de Dados, porém, o cracker utiliza desse conhecimento para efetuar crimes, enquanto o Hacker o utiliza para tornar sistemas e aplicações o mais seguras possíveis.

Segurança de dados consiste em proteger os dados de determinada aplicação ou sistema perante ameaças, intencionais ou acidentais, de alteração ou modificação não autorizada, roubo ou destruição. Ou seja, garantira preservação de informações e dados de valor para uma organização. Portanto, a segurança de dados envolve uma série de metodologias que visam assegurar a confidencialidade, a disponibilidade e a integridade dos dados, sejam eles virtuais ou físicos. Juntos, com mais ou menos intensidade, esses três atributos garantem a segurança da informação(Oficina da Net, 2008).

**Confidencialidade**

A confidencialidade visa impor limites de acesso à informação estritamente às pessoas e/ou entidades autorizadas por quem detém os direitos sobre a informação.  
Ou seja, somente pessoas e autorizadas, podem acessar, modificar e processar os dados(Oficina da Net, 2008).

**Integridade**

A integridade visa garantir as características originais de determinada informação. Ou seja, os dados se manterão íntegros, conforme criados ou mantidos pelo proprietário.

Portanto, este é um atributo que está diretamente ligado ao controle e manipulação e à preservação e manutenção do ciclo de vida dos dados - que compreende origem, manutenção e destruição(Oficina da Net, 2008).

### **Disponibilidade**

### Já a disponibilidade é a garantia de que as informações estarão sempre disponíveis para o uso legítimo. Ou seja, as pessoas e/ou entidades autorizadas pelo detentor dos direitos terão sempre garantido o acesso aos dados(Oficina da Net, 2008).

### 

### **Principais Tipos de Ataques Backdoor:** Backdoor é um Trojan (vírus de computador, o qual, quando infecta um usuário, é capaz de ter acesso a arquivos e funções do sistema de forma remota) que permite o controle e acesso do sistema do usuário infectado. Este tipo de ataque é extremamente perigoso, pois, uma vez infectado com este tipo de Malware, todos os arquivos e dados do sistema podem ser acessados pelo criminoso de forma remota e em sua grande maioria, imperceptivelmente(Unyleya, [s.d]).

**Ataque DDoS:** O Distributed Denial of Service, ou Ataque de Negação de Serviço Distribuído, consiste em um ataque, do qual, um determinado criminoso, utiliza-se de vários (milhares ou até milhões) de computadores infectados, chamados zumbis, para atacar o servidor de determinado serviço ou site, assim, todos os dispositivos zumbis acessam de forma ininterrupta o mesmo recurso de um servidor, fazendo com que o mesmo fique travado ou tenha de reiniciar inúmeras vezes(Unyleya, [s.d]).

**Port Scanning Attack:** Este Malware busca no sistema de determinada empresa ou instituição por alguma vulnerabilidade, por meio de possíveis portas abertas neste mesmo sistema, uma vez encontrada alguma brecha, os criminosos utilizam-na para roubar ou sequestrar informações(Unyleya, [s.d]).

**Ransomware:** Um tipo de “sequestro de dados”, o ransomware criptografa os arquivos do servidor atacado, e somente libera o acesso aos mesmos, após pagamento de um resgate em dinheiro, em sua maioria por meio de bitcoins, dada sua dificuldade de rastreio (Vega, 2017).Um exemplo deste ataque foi a recente invasão à Honda Motor. A empresa de automóveismultinacional suspendeu sua produção até que fosse resolvido o problema(Kaspersky,[s.d]).

**Spoofing:** Spoofing acontece quando um cibercriminoso se passa por um contato ou fonte confiável e conhecida. Podemos definir spoofing como uma variedade de táticas que dependem da capacidade do cibercriminoso se passar por outra pessoa, empresa ou instituição(Kaspersky,[s.d]).

Spoofing em segurança de rede envolve enganar um computador ou rede por meio de um endereço IP falso, redirecionando tráfego de internet no nível de DNS, ou falsificando dados ARP dentro de uma LAN(Kaspersky,[s.d]).

**Phishing:** Geralmente executado por e-mail, phishing é um ataque no qual os criminosos levam os usuários a expor informações pessoais ou sigilosas, como CPF, dados bancários e até mesmo senhas.

O ataque geralmente leva o usuário a uma cópia idêntica da página original, de uma agência bancária ou um site de compras, por exemplo.

Como sugere o nome da prática, os criminosos “pescam” os dados do usuário, assim que o mesmo os expõe nessas páginas fraudulentas. É um dos ataques mais comuns e que mais obtém sucesso(Unyleya, [s.d]).

**Manipulação de URL:** Neste caso, o Cracker manipula o site através de parâmetros na URL para ter acesso a recursos que somente administradores podem obter acesso(Unyleya, [s.d]).

**Engenharia Social:** Consiste na exploração de erros humanos para obter informações. Geralmente o criminoso utiliza-se de persuasão, abusando da ingenuidade, confiança ou até mesmo ignorância do usuário para obter senhas ou outros dados confidenciais. Atualmente a engenharia social é um dos maiores riscos de segurança de dados, devido a falta da devida noção do ataque por parte dos usuários(Unyleya, [s.d]).

**DISCUSSÂO**

Tecnologias da informação e comunicação mudaram o mundo, barateando, agilizando e facilitando processos em todas as esferas da vida, mas, deram origem a um tipo novo de crime, os cyberataques.

Em maio de 2017, cerca de 150 países foram vítimas de ataques ransomware (Pastorino, 2020) criminosos movimentaram valores milionários em resgates de dados criptografados pelo malware.

Nessa onda de 2017, inúmeros sites e sistemas de órgãos públicos ficaram fora do ar devido ao mesmo ataque citado acima, órgãos importantes, como Tribunais de Justiça, Ministérios Públicos, INSS e até mesmo a Petrobras (Capelas, 2017), foram alvos de ataques Ransomware. Computadores e servidores, tiveram de ser desligados e removidos da rede para evitar a proliferação do vírus sobre em mais computadores e eventualmente sobre mais dados.

Casos mais recentes no Brasil estão vinculados a uma série de invasões de contas do aplicativo Telegram, do ex-ministro da Justiça, de procuradores da Lava-Jato, ministros do Supremo Tribunal Federal (STF) e parlamentares(G1, 2019).

Segundo especialistas(Souza, 2019), o governo brasileiro colhe agora o resultado de décadas de atraso no investimento em segurança de dados e em tecnologias para coibir a ação de hackers e crimes cibernéticos.

Essa situação mostra que a administração pública possui diversos desafios para mudar este cenário, os quais, exigem de imediato, uma ação efetiva, ou estaremos sujeitos a cenários onde, o estado brasileiro pode perder o controle e o poder de contenção de ataques cibernéticos

A padronização de normas de segurança, atualização de sistemas demasiadamente antigos, e a fiscalização do comportamento dos funcionários sobre as práticas necessárias para evitar as práticas destes crimes, são algumas destas ações que devem ser adotadas e priorizadas a curto prazo.

**DESAFIOS E SOLUÇÕES**

De modo geral, proteger as informações é dever do depositário, e mais ainda dos órgãos públicos que detém informações sensíveis, alvo constante de criminosos, portanto, os problemas e eventos que podem ocorrer devido a má gestão de segurança são catastróficos, não é sensato manter um sistema, ou uma organização, exposta para atacantes.

Em um estudo feito pela Diretoria de Estudos e Políticas Setoriais, de Inovação, Regulação e Infraestrutura do Ipea, destaca-se a necessidade do investimento em tecnologia, e isso é um fator crítico para a segurança de sistemas, e também um dos maiores desafios enfrentados atualmente(IPEA, 2013).

Por outro lado, o desenvolvimento tecnológico tornaria possível o uso dos chamados Security Operation Centers (SOC). Estes setores, que são responsáveis pela segurança de sistemas, monitoram constantemente as atividades, endpoints (portas de comunicação externa) abertos, acessos, estatísticas de servidores e tráfego em rede. Esta estratégia aumenta a confiabilidade e maturidade de um sistema de grande escala.  
Além do investimento em tecnologia, é importante a capacitação dos usuários destes sistemas. Em uma pesquisa da IBM e Ponemon Institute(IBM, 2018), identificou-se que, em grande parte dos incidentes, a falha do usuário foi crucial para o sucesso do ataque. Este fator de "falha humana" precisa ser levado em consideração ao se projetar um sistema de segurança. Ações como monitoramento de acesso, limites de contas parecem muitas vezes simples, mas podem evitar grandes problemas, que surgem de uma falha aparentemente minúscula.

Uma pesquisa realizada pela Symantec(Computer World, 2016), uma das maiores empresas de soluções em antivírus do mundo, mostrou que, ao longo de 2016, os brasileiros tiveram prejuízos financeiros de cerca de 33 milhões de reais somente com cibercrimes.

Ao analisar mais especificamente o universo corporativo, conclui-se que a preocupação é tão grande quanto no campo dos usuários individuais. De acordo com o Relatório Barômetro de Rede 2016, divulgado pela Dimension Data(Dimesion Data, 2016), o número de empresas vulneráveis no mundo aumentou cinco vezes em relação a 2015. O estudo, que abrange 28 países, constatou que, a cada 100 dispositivos em rede no continente americano, 66 contêm algum tipo de vulnerabilidade.

As empresas cometem inúmeros erros em relação à segurança da informação. Sendo os principais:

### **Não realizar um planejamento completo**

### Um dos maiores e mais triviais erros que as empresas cometem é não possuir um planejamento de segurança de dados. Ou seja, não planejar um levantamento de quais informações devem ser protegidas e de ações para garantir essa defesa. Com um planejamento frágil ou nulo, as empresas não sabem identificar qual é o valor dos seus dados e, consequentemente, não conhecem as suas próprias vulnerabilidades lógicas e físicas. Logo, também não conseguem administrar proativamente seus ambientes críticos. Por não efetuarem um monitoramento de seus bancos de dados, por exemplo, só percebem os incidentes depois que os mesmos já ocorreram. Por não praticarem [auditorias constantemente na infraestrutura](http://blog.diferencialti.com.br/entenda-a-importancia-da-auditoria-em-infraestrutura-de-ti/), não conseguem atuar para diminuir riscos e detectar o que foi mal estruturado e está sendo conduzido erroneamente.

### 

### **Não treinar a equipe**

### No estudo da Dimension Data(Dimension Data, 2016), que citamos acima, descobriu-se que 37% dos incidentes de segurança de dados que ocorrem no mundo são frutos de erros humanos ou de configuração. Eis um erro que pode colocar qualquer estratégia de segurança de dados em xeque: não treinar a equipe. E aqui estamos falando tanto do time de TI quanto dos usuários, ou seja, dos colaboradores da empresa que não entendem sobre os detalhes técnicos. Quando não há treinamentos sobre segurança da informação, as pessoas tendem a relaxar na utilização das aplicações corporativas. Elas compartilham chaves de acesso, baixam arquivos não confiáveis, adquirem soluções SaaS(software as a service) sem solicitar auxílio do setor de TI. Enfim, provocam vulnerabilidades, muitas vezes, sem saber. E as brechas abertas podem ser fatais para o negócio.

### 

### **Não alinhar a política de segurança com a diretoria**

### O não alinhamento da política de proteção de dados com a diretoria costuma fazer com que a organização veja o assunto mais como gasto do que como investimento. Logo, os profissionais responsáveis vão se deparar com dificuldades de orçamento e baixa adesão dos usuários (em efeito cascata, desde a alta hierarquia até os colaboradores do dia a dia operacional, passando pelos líderes), por exemplo. E quando esses problemas aparecem, é natural que os esforços sejam sufocados por demandas mais corriqueiras. Se olharmos para os Estados Unidos, talvez a maior referencia em segurança dos dados, veremos essa realidade muito presente. De acordo com uma [pesquisa da Avaya](http://computerworld.com.br/so-25-profissionais-de-ti-tomam-medidas-eficazes-contra-ciberataques)(Computer World, 2017), somente 25% dos profissionais de TI tomam medidas eficazes para combater os cibercrimes. Para 35% dos profissionais entrevistados, ter uma política de segurança que contemple a segmentação de redes, por exemplo, é “muito complicado”. Outros 29% disseram que isso “requer muitos recursos”.

### 

### **Não possuir normas de proibição claras**

### Outro ponto importante, que ainda é muito negligenciado por várias empresas, é a existência de normas claras sobre o que é proibido fazer na rede interna. Sem limites claros, as pessoas tendem a manipular dados de diversos níveis de confiabilidade sem muita preocupação.

### Independentemente do tamanho da empresa, não é recomendável que todos os funcionários tenham acesso a todas as informações e documentos. É preciso delimitar os acessos com o uso de senhas e, mais do que isso, fazer o rastreamento baseado em hierarquias de responsabilidades — saber quem manipulou os dados, por exemplo.

**REVISÃO TEÓRICA**

Embora a população e a sociedade estejam cada vez mais atentas à importância da privacidade e da proteção de seus dados pessoais, é preciso que haja uma política que envolva governos, o mundo acadêmico e empresas privadas, com compartilhamento de informações estratégicas entre eles, para que a segurança de dados se torne mais eficiente. (Veja ,2019).

As tecnologias continuam a evoluir, e consequentemente a quantidade de informações armazenadas. Com o aumento dos dados, surge a necessidade de sistemas mais robustos para lidar com o volume e garantir a proteção eficiente dos dados, e é aí que muitas organizações falham, pois, a tecnologia herdada geralmente está desatualizada e incapaz de atender os novos requisitos (Filho, 2019).

Muitos governos e provedores estão se voltando para a criptografia. Tem sido uma das tecnologias de salvaguarda há mais tempo adotada e nós acreditamos que é uma das maneiras mais fortes de proteger dados que estão em trânsito. (Veja, 2019).

Porém, mesmo diante disso, ainda não vemos investimentos significativos em segurança da informação nos órgãos públicos. Frequentemente, vemos sistemas indisponíveis em função de ataques do tipo “wannacry” que “sequestram” os dados e os deixam indisponíveis por meio de criptografia. Ações simples, como backup de dados, ainda não são tratados de forma adequada (CIGEP, 2020).

O investimento, quando acontece, limita-se a equipamentos e não contempla o processo de segurança. Políticas, normas e campanhas de conscientização de usuários são deixadas em segundo plano (CIGEP, 2020).

Proteger os dados pessoais (de clientes e de funcionários) e a infraestrutura, dos setores público e privado, sempre foi relevante e, ainda mais agora, que é preciso estar em conformidade com regulações como a Lei Geral de Proteção de Dados no Brasil. (Romio, 2019)

No Brasil, apesar da preocupante morosidade legislativa e após quase uma década de discussões, foi criada a Lei Geral de Proteção de Dados (Lei 13.709/18), aprovada em 14 de agosto de 2018 e que encerrará seu prazo de adequação em 16 de fevereiro de 2020 (Filho, 2019).

Hoje torna-se essencial confirmar se o fornecedor tem a preocupação com as atuais práticas no setor de segurança da informação, desde lawful of interception (intercepção legal) até backdoors (entradas secretas) e contrato de privacidade estabelecido com as organizações. Ou seja, devemos abolir a prática de escolher soluções por comparação de datasheets (Romio, 2019). De acordo com com o autor, os fornecedores de serviços de hospedagens, devem fornecer arquiteturas e a visão de investimento deve ser voltada à arquitetura do ambiente de TI e de segurança, contrapondo-se à visão de crescimento orgânico.

Construir uma arquitetura na qual as tecnologias cobrirão o máximo de possibilidades de vulnerabilidades ou brechas, em que tudo deve estar integrado para análises, conformidade e governança de segurança (Romio, 2019).

Uma forma de aprimorar a gestão da segurança de dados, é citada por Vinícius Durbano (Durbano, 2018) em 12 itens:

**Acompanhe as tendências e evoluções da área**

Uma realidade da área de tecnologia é: as tendências e evoluções são muito rápidas dentro deste setor. Soluções novas são criadas todos os dias pelas maiores empresas especializadas da área, o que já torna necessário que os responsáveis da área de TI se mantenham atentos.

Porém, a área de segurança da informação exige cuidados maiores neste aspecto. Isto porque os cibercriminosos também criam e investem em novos mecanismos de ação todos os dias. Um dos grandes exemplos foi o ransomware, que surpreendeu os especialistas em segurança de imediato, causando espanto em um primeiro momento, até a criação dos protocolos de mitigação de danos.

Por isso, é fundamental pesquisar e estar atento todos dias às inovações que são lançadas. Assim, caso apareça alguma novidade, você poderá implementar medidas de contenção o quanto antes.

**Mantenha softwares e drivers atualizados**

Um dos principais meios de acesso dos hackers aos sistemas é por meio de falhas encontradas em softwares, sistemas operacionais e drivers. Por isso as empresas fornecedoras estão sempre lançando novas atualizações, corrigindo as falhas que permitem esse tipo de ação e tornando os sistemas mais seguros.

Porém, não adianta este trabalho se os gestores de TI não atualizarem os sistemas regularmente. Desta forma, as brechas permanecem e os cibercriminosos continuam tendo seus mecanismos de ação facilitados.

**Estabeleça controle de acesso para os colaboradores**

Uma forma comum de facilitar os problemas de segurança da informação é por meio de ações inadequadas dos usuários. Vamos citar um exemplo bem corriqueiro: Um funcionário com acesso a informações não concernentes a sua área, sem querer, realiza uma exclusão de um arquivo importante, que não estava presente em nenhum backup feito anteriormente.Este tipo de falha humana é corriqueiro nas empresas. E pode ser dificultado por meio do controle de acesso para os colaboradores.

Quanto menos pessoas têm acessos aos dados, menores são os riscos de erros deste tipo. Além disso, diminui-se as chances de vazamento de informações confidenciais ou estratégicas.

**Estabeleça bloqueio de sistemas de saída**

Da mesma forma, é imprescindível investir em bloqueio de sistemas de saída, evitando que informações sejam vazadas sem o conhecimento dos funcionários de TI. Por exemplo, invista em bloqueios de aplicativos e sites que facilitem o recolhimento de arquivos e envio para fora da rede da empresa. Se há sistemas internos de e-mail, pode-se bloquear o uso de e-mails pessoais dentro do ambiente empresarial, bem como sites de redes sociais e aplicativos de conversação.

**Crie políticas de segurança na empresa**

Todos os colaboradores fazem parte do processo de segurança da informação. Afinal, em alguma medida eles interferem no acesso às informações, seja por meio da criação de documentos, acesso à dados, facilitando a entrada de malwares com usos inadequados, etc. Por isso é fundamental estabelecer normas de conduta e políticas de segurança que devem ser seguidas por todos. Esse tipo de documentação permite normatizar as regras utilizadas na empresa. Com isso, torna-se possível diminuir as facilidades que permitem a ação de cibercriminosos ou falhas que comprometam os arquivos.

Por meio disso, por exemplo, pode-se criar normas do que deve ser feito caso um funcionário encontre um problema em seu sistema: ao invés de tentar resolver por conta própria, ele deve entrar em contato com o setor responsável, que verificará o ocorrido.

**Alinhe os processos às políticas de segurança**

Após a criação das políticas de segurança, é necessário alinhar os processos da empresa ao que foi normatizado e documentado anteriormente. Algumas alterações podem ser sutis, enquanto outras podem exigir uma reestruturação de toda a empresa, tornando-se necessário realizar um planejamento prévio de implementação.

Por exemplo, caso opte-se por alterar o sistema operacional, é necessária uma mudança em todas as máquinas instaladas no ambiente empresarial. Demanda-se tempo e preparação. O mesmo ocorre com possíveis mudanças nas formas de hierarquia de arquivos, realização de backups recorrentes, entre outros.

Assim, deve ser estabelecida, junto aos diretores das outras áreas, a necessidade de adequação dos processos, de forma a colocar em prática o que foi documentado anteriormente. Caso contrário, as falhas anteriores permanecerão e poderão causar problemas que deverão ser resolvidos posteriormente.

**Treine os colaboradores para medidas de segurança**

Algumas questões elaboradas nas políticas de segurança podem não ser tão claras para os colaboradores, principalmente por envolverem questões específicas da área de tecnologia. Para evitar confusões, dúvidas e ações errôneas, é imprescindível realizar treinamento com todos os envolvidos, a fim de normatizar as condutas de todos, bem como ensinar medidas básicas de segurança. É por meio do treinamento, por exemplo, que pode ser explicado para todos as razões pelas quais as redes sociais são bloqueadas no ambiente empresarial, isso auxilia para que não busquem outros métodos de acesso que podem também comprometer a segurança das informações.O treinamento também auxilia na uniformização de procedimentos em caso de problemas.

Por exemplo, no caso de um ataque ransomware, todos os colaboradores terão a mesma conduta, evitando resolverem a situação por conta própria.

**Tenha ferramentas de monitoramento**

É imprescindível utilizar ferramentas de monitoramento de atividades no cotidiano da área de TI. Para que a segurança seja eficaz, é preciso saber o que está acontecendo em toda a rede. Qualquer tipo de conduta errada, vulnerabilidade, mudança nos padrões de acesso deve ser percebida imediatamente, de forma a ser contida e evitar um ataque digital gerado por hackers.

**Utilize a criptografia de dados**

A criptografia é uma importante aliada para a segurança da informação. Ela impede, por exemplo, que os arquivos sejam acessados caso sejam interceptados no meio do processo, só tendo as chaves de acesso, às pessoas que possuem a chave privada.

Este tipo de ferramenta pode — e deve — ser utilizado no envio de informações estratégicas e confidenciais, evitando que hackers possam interceptar os dados e ter acesso ao que foi encaminhado.

**Conte com ajuda de empresas especializadas em segurança da informação**

As empresas especializadas na área de segurança da informação podem ser estratégicas e essenciais para garantir a privacidade e integridade dos dados da sua corporação. Elas estão sempre atentos para as novidades, trazendo e desenvolvendo soluções importantes e inteligentes que ajudarão a potencializar os mecanismos de proteção.

Por exemplo, pode-se contar com essas empresas para o armazenamento de backups na nuvem de forma segura.

Assim, garante-se uma maior proteção para os dados e permitindo que sua equipe direcione os esforços para outras questões da área de TI. Além disso, em caso de desastres, como o ransomware, as empresas especializadas poderão auxiliar na resolução da situação com a aplicação de protocolos para mitigar os danos causados pela ação.

**Crie planos de contingência**

Não basta apenas pensar em medidas preventivas. Como falamos ao longo deste artigo, os cibercriminosos são engenhosos e criam constantemente novas formas de atuação para conseguirem seus objetivos. Muitas vezes eles surpreendem os especialistas em segurança da informação, de forma que, até descobrir formas de reverter a situação, pode-se ter prejuízos inestimáveis.

Além disso, os problemas não se limitam apenas aos casos de ataques feitos por hackers: desastres tecnológicos, falhas humanas, entre outros, são recorrentes. É preciso saber como agir nessas situações.

Assim, é necessário estipular ações padronizadas, já que a mitigação dos danos pode ser realizada por qualquer um dos membros responsáveis pela área de segurança da informação.

As ações podem variar de profissional para profissional, o que pode causar problemas posteriores. Portanto, é fundamental criar parâmetros de padronização.

Por isso, é importante ter um plano detalhado para eventuais situações, de forma que todos operem da mesma forma e evitem falhas de comunicação e procedimentos errados.

**Invista em backup**

Se tudo der errado e, assim, os dados encontrados em discos rígidos e servidores forem perdidos, é essencial ter uma espécie de “plano B” para não inviabilizar as funções cotidianas. O backup é a melhor opção nesses casos, provendo uma recuperação de dados eficiente, seja por meio de um servidor externo, um HD externo ou na nuvem. O essencial é não abrir mão dessa ferramenta.

Nota-se que os maiores investimentos acerca de segurança de dados, não se trata só na questão financeira, mas também de treinamento e preparação das pessoas que lidam diretamente com os dados. Dessa forma, não investimento em segurança de dados pode ser desastroso para a organização, levando problemas como vazamentos, fraudes bancárias, sequestros de dados, ataques DDoS, roubo de senhas, entre outros, identificam a fragilidade da segurança da organização, gerando um mal-estar no mercado(Durbano, 2018).

**METODOLOGIA**

O presente artigo é uma pesquisa bibliográfica demilitada pelos seguintes parâmetros: intervalo de tempo; no Brasil; Artigos em português, Notícias da mídia impressa e eletrônica.

A coleta dos dados ocorreu em duas fases: (i) pesquisa bibliográfica que teve por objetivo apresentar o referencial teórico sobre segurança de dados e levantar estatísticas acerca da segurança de sistemas e aplicações; (ii) análise de dados e ações levantados em artigos, notícias da mídia e blogs de empresas especializadas em segurança digital, e com base nestes dados, trazer ações e medidas de prevenção de cibercrimes e proteção de dados.

A partir disso, desenvolvemos este artigo, e com base nos dados adquiridos, levantamos questões importantes e medidas que podem ser adotadas em todos os âmbitos, desde corporativos até mesmo pessoais. Os conceitos analisados foram falhas na segurança da informação de alguns órgãos públicos e instituições privadas, principais alvos de ataques, ações que propiciam ou facilitam as ações de crackers, e por fim as consequências da falta de investimento financeiro e de recursos humanos em prol da segurança de aplicações e dados.

**CONSIDERAÇÕES FINAIS**

Ao longo dos anos, a tecnologia evoluiu muito, sistemas que antes faziam operações simples, agora são responsáveis por gerenciar tarefas e operações muito importantes, principalmente nos sistemas públicos, abordados neste artigo.

Todos os eventos aqui estudados, como invasões, instabilidades e até mesmo vazamento de dados, alertam a necessidade de atenção que deve ser prestada a um sistema que possui grandes responsabilidades. Não dedicar os devidos cuidados à segurança, ou mesmo à resiliência do funcionamento destes perante a ataques, é irresponsabilidade.

Assim como os sistemas precisam de proteção, fica claro que nenhum sistema é sempre protegido e invulnerável quando há a interação humana e, neste tópico, toda a manipulação de sistemas é válida. Um usuário de um aplicativo de mensagens instantânea pode ter um arquivo de texto vazado por descuido, mas é esta mesma desatenção que pode dar brechas para um vazamento sobre uma investigação policial, localizações que não deveriam ser divulgadas ou mesmo dados de funcionários ou de pessoas cadastradas em um sistema. Isto tudo deve ser manipulado por pessoas que tenham noções de segurança, para que não cometam esses erros grotescos ou negligentes, que, por muitas vezes, acabam por descartar toda a segurança de um sistema bem construído.

**REFERÊNCIAS**

BARRACUDA**. Surge in security concerns due to remote working during COVID-19 crisis**.[S.l.] 2020. Disponivel em: <<https://blog.barracuda.com/2020/05/06/surge-in-security-concerns-due-to-remote-working-during-covid-19-crisis/>>. Acesso em 8 Jan. 2021.

BBC. **Alvo de ataque hacker, STJ gastou R$ 13,7 milhões com empresa de informática investigada**. [S.l.] 2020. Disponivel em:

<<https://www.bbc.com/portuguese/brasil-54847723#:~:text=O%20%27sequestro%27%20da%20base%20de%20dados&text="O%20Superior%20Tribunal%20de%20Justiça,quando%20ocorriam%20sessões%20de%20julgamento>.>. Acesso em 14 Jan. 2021.

CAMURÇA, Francisco**. Embraer sofre vazamento de dados e expõe documentos confidenciais**. We Live Security. [S.l.] 2020.Disponivel em:

<<https://www.welivesecurity.com/br/2020/12/09/embraer-sofre-vazamento-de-dados-e-expoe-documentos-confidenciais/>> Acesso em 14 Jan. de 2021.

CAPELAS, Bruno. **No Brasil, órgãos públicos foram os mais afetados pelo WannaCry.** Estadão. [S.l.] 2017. Disponível em:

<<https://link.estadao.com.br/noticias/cultura-digital,no-brasil-orgaos-publicos-foram-os-mais-afetados-pelo-wannacry,70001816480>>. Acesso em: 9 de jan. de 2021.

CHECKPOINT. **COVID-19 Pandemic Drives Criminal and Political Cyber-Attacks Across Networks, Cloud and Mobile in H1 2020**. [S.l.] 2020. Disponível em:

<<https://www.checkpoint.com/press/2020/check-point-research-covid-19-pandemic-drives-criminal-and-political-cyber-attacks-across-networks-cloud-and-mobile-in-h1-2020/>>. Acesso 14 Jan. de 2021.

CIGEP. **Segurança da informação no setor público aplicada à prática**. [S.l.] 2020. Disponível em: <<https://cigep.com.br/blog/seguranca-da-informacao-no-setor-publico-aplicada-a-pratica/>>. Acesso 2 de jan. de 2021.

# CIO. **Mais da metade das empresas sofreu ataques-phishing durante a pandemia**. [S.l.] 2020. Disponível em: <<https://cio.com.br/noticias/mais-da-metade-das-empresas-sofreu-ataques-phishing-durante-pandemia/>>. Acesso 9 jan. de 2021.

# CISCO. **What Are the Most Common Cyber Attacks**. [S.l.] 2020. Disponivel em: <<https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>> Acesso 14 Jan. de 2021.

Computer World. **Cibercrimes geram prejuízo de 33milhões aos brasileiros neste ano**.[S.l.] 2016. Disponível em: <<https://computerworld.com.br/cibercrime-gera-prejuizo-de-r-33-milhoes-aos-brasileiros-neste-ano-diz-estudo>>. Acesso em 25 Dez. 2020.

COMPUTER WORLD**.** **Só 25% dos profissionais de TI tomam medias eficazes contra ciberataques**.[S.l.] 2017. Disponivel em: <<https://computerworld.com.br/so-25-profissionais-de-ti-tomam-medidas-eficazes-contra-ciberataques>>. Acesso em 24 Dez. 2020.

DIMENSION DATA. **Network Barometer Report**. [S.l.] 2016. Disponivel em: <<http://www.dimensiondata.com/Global/Downloadable%20Documents/Network%20Barometer%20Report%202016.pdf>>. Acesso em 08 Jan. 2021.

DURBANO, Vinicius. **Segurança da informação: o que é e 12 dicas práticas para garantir**. [S.l.] 2018. Disponível em:

<<https://www.google.com/amp/s/blog.ecoit.com.br/seguranca-da-informacao/amp/>> Acesso 10 Jan. de 2021.

FILHO, José M. Araujo. **O Impacto da Lei Geral de Proteção de Dados na Administração Pública**. JUS. [S.l.] 2019. Disponível em:

<<https://jus.com.br/amp/artigos/77586/o-impacto-da-lei-geral-de-protecao-de-dados-na-administracao-publica>>. Acesso em 24 de dez. de 2020.

G1**. Honda é alvo de ataque hacker e suspende parte da produção, incluindo no Brasil**. [S.l.] 2020. Disponivel em:

<<https://g1.globo.com/carros/noticia/2020/06/09/honda-e-alvo-de-ataque-hacker-e-suspende-parte-da-producao-incluindo-no-brasil.ghtml>>. Acesso em 14 Jan. 2021.

IBM**. 2018 Cost of Data Breach Study: Impact of Business Continuity Management**. [S.l.] 2018. Disponivel em:

<<https://www.ibm.com/downloads/cas/ZYKLN2E3/>>. Acesso em 15 Jan. 2021.

IPEA. **Texto analisa a segurança cibernética no Brasil e nos EUA**. [S.l.] 2013. Disponivel em:

<<https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=19216:texto-analisa-a-seguranca-cibernetica-no-brasil-e-nos-eua&catid=9:diset&directory=1/>>  Acesso em 15 Jan. 2021.

# KASPERSKY. **Brasil foi o quinto país com maior proporção de vítimas de phishing após pandemia.** [S.l.] 2020. Disponivel em:<<https://www.kaspersky.com.br/about/press-releases/2020_brasil-foi-o-quinto-pais-com-maior-proporcao-de-vitimas-de-phishing-apos-pandemia>> Acesso em 14 Jan. 2021.

# KASPERSKY. **Ataques a dispositivos móveis crescem 124% em março**. [S.l.] 2020. Disponivel em: <<https://www.kaspersky.com.br/blog/phishing-covid-smartphone-pesquisa/14663/>> Acesso em 7 Jan. 2021.

# KASPERSKY. **Quais são os diferentes tipos de ransomware?**. [S.l.] [s.d]. Disponivel em:<<https://www.kaspersky.com.br/resource-center/threats/ransomware-examples>> Acesso em 08 Jan. 2021.

OFICINA DA NET. **Segurança da informação, conceitos e mecanismos**. [S.l.] 2008. Disponibilizado em:

<<https://www.oficinadanet.com.br/artigo/1307/seguranca_da_informacao_conceitos_e_mecanismos>> Acesso em 14 Jan. 2021.

PAIVA, Yaskara. **Conscientização sobre segurança cibernética na Administração Pública**. Conteúdo Juridico. [S.l.] [2020]. Disponivel em:

## <<https://www.conteudojuridico.com.br/consulta/Artigos/55351/conscientizao-sobre-segurana-ciberntica-na-administrao-pblica>>. Acesso em 13 Jan. 2021.

PASTORINO, Cecilia**. WannaCry: três anos depois, a ameaça ainda continua viva**. We Live Security, 2020. Disponivel em:

<<https://www.welivesecurity.com/br/2020/05/12/wannacry-tres-anos-depois-a-ameaca-ainda-continua-ativa/>> Acesso em 08 jan. 2021.

ROMIO, Daniel. **Como executivos devem investir em segurança da informação?**. Cio. [S.l.] 2019. Disponível em:

<<https://www.google.com/amp/s/cio.com.br/gestao/como-executivos-devem-investir-em-seguranca-da-informacao/amp/>> Acesso 10 Jan. de 2021.

SOUZA, Renato**. Ataque de hackers a autoridades desafia governo e empresas brasileiras**. Estado de Minas. [S.l.] 2019. Disponível em:

<<https://www.welivesecurity.com/br/2020/05/12/wannacry-tres-anos-depois-a-ameaca-ainda-continua-ativa/>>. Acesso em: 9 de jan. de 2021.

# UNYLEYA, Faculdade. **Conheça os 10 principais ataques cibernéticos da atualidade**. [S.l.] [s.d]. Disponivel em:

<<https://blog.unyleya.edu.br/bitbyte/ataques-ciberneticos/>>. Acesso em 14 Jan. 2021.

Veja. **‘Governo tem de ter papel de liderança na proteção de dado’, diz executivo**. [S.l.] 2019. Disponível em:

<<https://www.google.com/amp/s/veja.abril.com.br/economia/governo-tem-de-ter-papel-de-lideranca-na-protecao-de-dado-diz-executivo/amp/>>. Acesso 2 de jan. de 2021.

VEGA, Guillermo**. Por que nos ciberataques o resgate é pedido em bitcoins?**. El País. [S.l.] 2017. Disponível em:

<<https://brasil.elpais.com/brasil/2017/05/12/economia/1494621106_047933.html>>. Acesso em: 9 de jan. de 2021.