

**ÉTICA E SEGURANÇA EM SISTEMAS DE INFORMAÇÃO: estudo de caso na  
Prefeitura Municipal de Nova Andradina/MS**

**Raphael Augusto Perpétuo**  
Universidade Federal de Mato Grosso do Sul (CPNA)  
raphaelcenz@gmail.com

**Francieli Fernanda Eichinger**  
Universidade Federal de Mato Grosso do Sul (CPNA)  
francieli.ms.fernanda@gmail.com

**Aline Rodrigues Guisoni**  
Universidade Federal de Mato Grosso do Sul (CPNA)  
guisonialine@gmail.com

**Jamson Justi**  
Universidade Federal de Mato Grosso do Sul (CPNA)  
jamson.justi@ufms.br

**Edrilene Barbosa Lima Justi**  
Universidade Federal de Mato Grosso do Sul (CPNA)  
edrilene@gmail.com

**Jadson Justi**  
Universidade Federal do Amazonas (UFAM)  
jadsonjusti@hotmail.com

**RESUMO**

A proteção e a segurança dos dados, e demais informações de qualquer organização, é de crucial importância. O investimento neste processo deve ser contínuo, tanto em relação ao sistema remoto, bem como treinamento dos funcionários responsáveis pelo monitoramento e controle dessas informações. O presente trabalho tem como objetivo demonstrar algumas mudanças referentes à implantação de novos sistemas de segurança na Prefeitura Municipal de Nova Andradina/MS (PMNA), levando em consideração algumas medidas já existentes, e as melhorias percebidas após a implantação dos atuais sistemas de segurança. Metodologicamente, o trabalho se caracteriza como uma pesquisa qualitativa de grupo exploratório, classificado como pesquisa bibliográfica, e estudo de caso. É possível concluir que em relação a segurança dos dados e informações, a PMNA possui resultado satisfatório em relação ao sigilo e proteção de seus dados, pois além de altos investimentos, a Prefeitura possui uma equipe comprometida e responsável.

**Palavras-chave:** Banco de dados; Segurança; Inovação; Ética profissional.

De acordo com O'Brien (2013), o crime com o uso do computador é uma ameaça crescente à sociedade, provocada por ações irresponsáveis de indivíduos que estão tirando vantagem do uso generalizado e da vulnerabilidade de computadores, da *internet* e de outras redes. Percebe-se então, que há um importante desafio em relação ao uso ético de tecnologias de informação (TI). O crime com o uso do computador ameaça seriamente a integridade, a segurança, e a sobrevivência da maioria dos sistemas de *e-business*, tornando dessa forma, o desenvolvimento de métodos eficazes de segurança, uma prioridade.

A segurança é percebida como uma atitude inerente aos processos de gestão da informação, no sentido de oferecer às organizações um maior controle sobre os dados relevantes, e uma conformação maior com os mecanismos de tomada de decisão e confidencialidade dentro das instituições, incluindo o funcionário responsável como peça fundamental para o alcance desses objetivos.

Melo (2014) reforça a importância em ter um profissional altamente responsável dentro das organizações, e neste sentido, pode-se afirmar que o elo mais fraco de um processo de segurança é o funcionário responsável (ou grupos de pessoas) por garantir a fidelidade da informação. Portanto, a estratégia é analisar as pessoas que de alguma forma manipulam essas informações, verificando se são realmente aptas ao acesso de tais informações dentro da organização.

Um sistema de informação pode ser definido tecnicamente como um conjunto de componentes inter-relacionados que coletam, ou mesmo recuperam, processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização. Além de dar apoio à tomada de decisões, à coordenação e ao controle, esses sistemas também auxiliam os gerentes e trabalhadores a analisar problemas, visualizar assuntos complexos e criar novos produtos (LAUDON; LAUDON, 2014).

Foi realizada uma pesquisa junto à Prefeitura Municipal de Nova Andradina, detalhando alguns métodos de segurança, o que pode ou não ser mudado e quais melhorias podem ser realizadas, mostrando na prática a importância da segurança das informações e de se ter uma equipe eticamente responsável. O município conta hoje com algumas medidas de segurança, são elas:

**\*Firewall<sup>1</sup>:** o mesmo foi desenvolvido pelos servidores de TI, através dele é possível identificar e limitar acessos a páginas indevidas, *downloads* com potencial de risco, o uso de dados de cada máquina, ou até mesmo controlar o acesso de cada usuário da rede.

Como hoje o poder público deste município conta com uma rede muito ampla, o *firewall* dá um total controle de tudo o que acontece na infraestrutura de rede, visto que a prefeitura oferece um serviço de *internet* gratuita, ele consegue avaliar e apresentar gráficos em tempo real do uso da *internet* no paço, e suas ramificações no poder público, para assim relatar se há algum defeito, problema ou ataque em algum dos servidores.

**\*Antivírus<sup>2</sup>:** o *firewall* faz a parte de segurança externa do poder público, e na parte de segurança interna, conta-se com um antivírus gratuito da *Microsoft*, que provou incontáveis vezes ser útil no combate a pequenos vírus, inserido no parque tecnológico do poder público através de dispositivos móveis (*pendrives* e HD's externos) e com a licença do *Windows*, consegue mantê-lo sempre atualizado, eliminando o risco de sofrer perdas com softwares indesejados na rede (*worms*, cavalos de tróia, etc.).

**\*Servidores<sup>3</sup>:** hoje a prefeitura conta com alguns servidores no poder público, sendo eles de dados, arquivos gerais para uso do poder público, aplicativos (acesso remoto a aplicativos, como compras, patrimônio, RH e outros), servidor de banco de dados (dos aplicativos), servidor de programas de saúde ( eSUS, flySAUDE, etc.) e alguns outros como BACKUP, CLOUD, MONITORAMENTO e DADOS de TI.A segurança dos mesmos é feita através de Login com usuário e senha, sendo estes liberados através de documentos enviados aos servidores de TI, e assinados pelos secretários das respectivas pastas.

**\*BACKUP<sup>4</sup>:** conta-se com um servidor de *backup*, o qual é programado para fazer *backup* diário nos demais servidores, e para garantir a total segurança é feito uso de um outro servidor que serve para fazer o *backup* no servidor de *backup*, e o mesmo se localiza em outro

---

<sup>1</sup> Firewall: É um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança". Disponível em: [https://www.cisco.com/c/pt\\_br/products/security/firewalls/what-is-a-firewall.html](https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html). Acesso em: 22/08/2020.

<sup>2</sup> Antivírus: São programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança ao usuário. Disponível em: <https://canaltech.com.br/antivirus/o-que-e-antivirus/>. Acesso em: 22/08/2020.

<sup>3</sup> Servidores: É um computador que centraliza serviços, oferecendo-os a outros computadores que estejam em sua rede. Tais serviços podem ter natureza diversa, como por exemplo, correio eletrônico, website, armazenamento de arquivos, dentre outros. Disponível em: <https://www.oi.com.br/faq/p/o-que-e-um-servidor>. Acesso em: 22/08/2020.

<sup>4</sup> BACKUP: É uma cópia de segurança dos dados (física ou em nuvem) de um dispositivo de armazenamento ou sistema. Disponível em: <https://tecnoblog.net/285077/o-que-e-backup/>. Acesso em: 22/08/2020.

ponto do paço municipal para evitar desastres (incêndios, alagamentos, etc.). Por fim, a equipe de TI também realiza armazenamento dos dados semanalmente, no intuito de mantê-los verdadeiramente protegidos.

Atualmente o que mais se busca é a informação, e poder ter essa informação disponível em qualquer lugar. No momento, a equipe de tecnologia trabalha para o desenvolvimento de um servidor chamado CLOUD<sup>5</sup>, pois através dele, os funcionários podem ter acesso onde estiverem.

Mas como liberar arquivos sem perder o controle sobre eles e também como fazer para manter essas informações longe dos olhos de pessoas as quais não devem ter acesso as mesmas? A equipe de TI da Prefeitura, após várias pesquisas sobre o caso, decidiu optar por um sistema de autenticação de dois fatores, com objetivo de armazenar com maior segurança suas informações.

O usuário será cadastrado por uma senha que será feita juntamente com a equipe e mediante apresentação de autorização de seus respectivos secretários, e após este procedimento, será instruído a baixar o aplicativo de autenticação para acessar e trabalhar como e onde estiver, lembrando que esse servidor ainda contará com um sistema de auditoria para assim saber quando o usuário “logou” e o que foi feito por ele, e também contará com um *backup* diário, assim como os outros. Portanto, mesmo que o usuário delete sem querer um arquivo, ainda haverá a possibilidade de ser restaurado.

Visto que um sistema de informação não é apenas algo baseado em computadores, tem-se levado em conta que a prefeitura hoje trabalha com processos, e os mesmos em sua forma física é anexado junto a vários volumes de inúmeras páginas. Pensando nisso, está sendo realizado um trabalho de desenvolvimento de um sistema chamado OPEN SOURCE<sup>6</sup> de comunicação institucional, e funciona da mesma forma como os processos de forma física, no entanto, sendo virtual, ou seja, o usuário cria um processo *online* e dá andamento para o mesmo. É perceptível que com este sistema consegue-se uma economia nos níveis de impressão, e também ajuda a manter seguro as informações contidas nos processos.

Com base nesses relatórios, conclui-se que apesar das infinitas formas de segurança que estão em andamento, e até mesmo as que estão sendo criadas, deve ser levado em

---

<sup>5</sup> CLOUD: é um termo utilizado para descrever uma rede global de servidores, cada um deles com uma função única. Disponível em: <https://azure.microsoft.com/pt-pt/overview/what-is-the-cloud/>. Acesso em: 22/08/2020.

<sup>6</sup> OPENSOURCE: Quer dizer código aberto. O termo é usado para designar os softwares livres, sem cobrança de licença de utilização pelo autor. Disponível em: <https://citrus7.com.br/artigo/o-que-e-tecnologia-open-source/>. Acesso em: 22/08/2020.

consideração que para a obtenção de tais resultados é de suma importância o comprometimento e fidelidade ética de cada funcionário que opera os diversos setores da empresa.

### REFERÊNCIAS

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerenciais**. 11. ed. São Paulo: Pearson Prentice Hall, 2014.

MELO, R. O.; SOUZA, R. S.; FURTADO, M. R. S. Ética e o Profissional de Tecnologia da Informação. **Revista Pensar Tecnologia**, v. 3, n. 2., 2014.

O'BRIEN, J. A.; MARAKAS, G. **Administração de Sistemas de Informação**. 15. ed. Porto Alegre: AMGH, 2013.

PMNA. **Prefeitura Municipal de Nova Andradina/MS**. Setor de tecnologia da informação, 2020.