

**Disciplina: Segurança de Sistemas**

**Profa.: Rejane Cunha Freitas (**rejan.freitas@faculdadecdl.edu.br**)**

**Estudo de caso – Gestão Segurança da Informação**

Texto: Estudo de caso em Segurança da Informação

Referências: VENÂNCIO, Elaine Conceição. Um estudo de caso em Segurança da Informação. Monografia curso Gestão da Informação. Universidade Federal do Paraná, p. 30-34. Disponível em:

< <https://www.acervodigital.ufpr.br/bitstream/handle/1884/48297/TCC%20-%20Elaine%20Conceicao%20Venancio.pdf?sequence=1>>

A GEOPLUS GEOTECNOLOGIA E INFORMÁTICA LTDA

A GeoPlus Geotecnologia e Informática Ltda (inaugurada em 11 junho de 2003) é uma empresa especializada em soluções de informática, especialmente para Sistemas de Informações Geográficas. Com experiência no desenvolvimento de redes, *softwares*, bancos de dados e aplicações WEB – internet e intranet, atende empresas ou órgãos públicos em campos diversos, tais como agronegócio, logística, saneamento, meio ambiente, gestão municipal e setor florestal.

A empresa realiza análise de soluções necessárias para as organizações, desenvolve sistemas e treinamento técnico. Valoriza a infraestrutura e sistemas já existentes no cliente, com o objetivo de projetar soluções que atinjam os objetivos, mas que respeitem os recursos disponíveis.

Quanto à estrutura, a empresa possui escritório localizado em Curitiba-PR. A sua equipe é formada por engenheiros, cartógrafos, analistas de sistema, administradores, técnicos em cartografia, programadores e estagiários. Ao todo a empresa conta com sete colaboradores e estagiários e três diretores, totalizando dez funcionários. Especializada em desenvolvimento de sistemas para WEB, a empresa possui servidores destinados a hospedar aplicações dos clientes, cujo principal objetivo é primar pela segurança, confiabilidade, disponibilidade e velocidade de acesso às informações.

Alguns clientes da empresa e respectivos projetos:

a) Fundação ABC para Assistência e Divulgação Técnica Agropecuária: consultoria na elaboração do projeto da versão WEB do Banco de Dados Agronômicos e do Sistema de Informações Geográficas para o LIG, fornecendo subsídio para definição da tecnologia, *softwares* e linguagens de programação;

b) Associação Mico Leão Dourado/RJ: desenvolvimento de sistema para cadastro institucional de ONGS na área de atuação da associação e divulgação de dados espaciais;

c) Masisa: desenvolvimento de sistema de controle das operações florestais integrado ao cadastro da base florestal existente e do sistema de informações geográficas, possibilitando aos usuários visualizar todas as informações em ambiente WEB.

d) STCP Engenharia de Projetos Ltda: desenvolvimento de sistema de gestão de informações composto por documentos e mapas, desenvolvido com tecnologia WebMapping;

A seguir será apresentado um estudo realizado na empresa através de entrevista com um dos diretores da empresa, cuja área de atuação é o desenvolvimento de Sistemas Informações Geográficas e o suporte a bancos de dados.

A IMPORTÂNCIA DA INFORMAÇÃO E DA SUA PROTEÇÃO NA GEOPLUS

A GeoPlus é uma empresa focada fundamentalmente no uso da informação como ferramenta para desenvolvimento de suas atividades. Esta característica pode ser constatada nos projetos de consultoria, desenvolvimento e treinamento da qual a organização participa, onde a informação e/ ou a capacidade de transferência e/ou a capacidade de armazenar a informação são utilizadas amplamente. Muitos dos produtos entregues são compostos de documentos (mapas, memoriais descritivos, apostilas, etc) ou programas (código fonte, instaladores, etc).

Como os produtos que são desenvolvidos não possuem grande custo material, em geral é o custo dos CDs e papel, o valor está ligado à informação que estas mídias contêm. Portanto, a disponibilidade destas informações, sua segurança, o controle de acesso e a privacidade são fundamentais. Além disso, a empresa é contratada por diversas organizações para armazenar seus dados cartográficos e/ou seus sistemas de informação. Neste caso, existe uma obrigação contratual de garantir a segurança das informações que estão sob a guarda da GeoPlus.

GESTÃO DA SEGURANÇA DAS INFORMAÇÕES NA GEOPLUS

A Segurança da Informação dentro da organização é aplicada nos ambientes físico, lógico e nos aspectos humanos. No que se refere ao ambiente físico, a empresa está localizada em um prédio com portaria e câmeras de segurança 24 horas nos ambientes que dão acesso ao escritório. Referente aos aspectos humanos os funcionários recebem orientações verbais de utilização de senhas de acesso ao servidor e de e-mails para que estas sejam de difícil adivinhação, mas de fácil retenção na memória, para evitar a necessidade do registro em papel e da importância da troca periódica da senha (porém, o sistema não solicita automaticamente a troca em intervalos regulares). Os funcionários também são orientados a utilizarem antivírus e evitarem o acesso a arquivos suspeitos, mas não existe um procedimento de verificação que permita acompanhar se estas orientações estão sendo atendidas. Sendo que os acidentes com *malware* e perda de arquivos são tratados de forma pontual e os usuários são alertados das melhores práticas a serem observadas no uso dos computadores e do acesso às informações da empresa. Convém acrescentar que a empresa não possui uma norma de segurança ou política de segurança clara e formal e não segue nenhuma norma técnica de segurança da informação.

Sobre os aspectos lógicos a empresa possui um servidor para uso interno que está conectado à internet e um servidor de desenvolvimento fornecido por um cliente para uso exclusivo de seus sistemas. O acesso ao servidor é controlado e existem contas individuais para cada usuário. As permissões de acesso às pastas também são controladas e informações da empresa, dos projetos e dados de clientes são separados e controlados individualmente.

Mecanismos de Segurança voltados ao Aspecto Lógico

Como 95% das informações da empresa estão disponíveis digitalmente o foco maior da empresa para garantir a proteção das informações é no ambiente lógico, para isso são utilizados os seguintes mecanismos: antivírus, controle de acesso (citado anteriormente), criptografia, *backups*, certificados digitais e *firewall*, que será apresentado seu funcionamento.

O acesso remoto ao servidor só pode ser feito através de uma conexão SSH, que utiliza a tecnologia de criptografia para garantir a segurança e privacidade das senhas e dados trafegados na rede. Os sistemas hospedados no servidor em ambiente WEB utilizam certificados digitais SSL para garantir a autenticidade e privacidade da informação. Estes certificados são adquiridos por uma empresa que segundo o entrevistado é uma representante da maior empresa de certificação digital do mundo atualmente, a Verisign. Este tipo de certificado SSL é utilizado em praticamente todos os bancos e sítios de comércio eletrônico.

Para garantir a segurança das informações armazenadas no servidor, diariamente é feito um *backup* incremental, que é composto por todos os arquivos que foram alterados nas últimas 24 horas. Sendo que nos finais de semana é realizado um *backup* completo do servidor para garantir uma forma rápida de retornar os dados em caso de falha do sistema e equipamentos ou falha humana.

O servidor da GeoPlus utiliza um mecanismo de *firewall* nativo do Linux, o *iptables*. Este mecanismo permite que seja controlado o acesso do servidor tanto do lado externo (internet) quanto do lado interno (rede local). Este mecanismo é baseado em filtros e tentativas de quebrar ou contornar estas regras são armazenadas no servidor para posterior auditoria.

O acesso ao servidor é controlado e a senha do *root* (administrador do sistema) é alterada a cada 2 ou 3 semanas. A maior parte dos serviços que são executados no servidor só estão disponíveis para a rede local, ou quando estão abertos para a internet, é feita uma filtragem de quais endereços de origem podem acessar o servidor. Os *backups* diários são salvos em DVD e guardados dentro de um armário na empresa e ficam disponíveis para todos que precisam recuperar dados dentro de um determinado período e o *backup* semanal é feito em um outro disco rígido externo ao servidor.

O serviço de *firewall* é iniciado quando o servidor é ligado, garantindo desta forma que o sistema estará protegido neste aspecto. Os usuários que não estão mais ligados a empresa ou os serviços que não estão sendo mais utilizados são desativados para evitar falhas na segurança dos dados.

Atualmente, não existe um sistema ou processo de verificação rotineiro destes mecanismos, ou seja, os *backups* não são testados para verificar sua consistência e os arquivos de log não são lidos diariamente. No entanto, a empresa identifica que esta é uma prioridade nas atividades internas da área de informática da empresa e que, portanto, serão providenciados os testes destes mecanismos o mais breve possível.

**Responda:**

**Você deverá identificar assuntos relacionados à gestão de segurança da informação e relatar como tais assuntos são abordados no presente estudo de caso:**

1. **Quais são os controles do ponto de vista legal e de boas práticas que essa organização necessita? Justifique.**

Referente aos aspectos humanos os funcionários recebem orientações verbais de utilização de senhas de acesso ao servidor e de e-mails para que estas sejam de difícil adivinhação, mas de fácil retenção na memória, para evitar a necessidade do registro em papel e da importância da troca periódica da senha (porém, o sistema não solicita automaticamente a troca em intervalos regulares).

* Apesar de parecer eficaz, a memorização apenas por voz é falha, pois o indivíduo poderá dialogar e deixar “escapar” as senhas de acesso, fazendo com que esse sistema fique falho. Seria muito mais benéfico e inteligente que as senhas fossem registradas em uma documentação que não saísse da empresa, assim, os funcionários teriam acesso somente quando estivessem no ambiente corporativo. Não obstante, é necessário uma política que expire a senha a cada 15 dias (assim como a senha root), pois garante uma maior segurança.

Os funcionários também são orientados a utilizarem antivírus e evitarem o acesso a arquivos suspeitos, mas não existe um procedimento de verificação que permita acompanhar se estas orientações estão sendo atendidas. Sendo que os acidentes com malware e perda de arquivos são tratados de forma pontual e os usuários são alertados das melhores práticas a serem observadas no uso dos computadores e do acesso às informações da empresa.

* A princípio, é importante que a empresa verifique se todas as máquinas estão com antivírus ativo; por exemplo, antes de entregar a máquina pro contribuinte, é importante que tudo já esteja conforme requisitado. Com o antivírus instalado, arquivos suspeitos seriam automaticamente bloqueados, evitando a existência de contaminação por malwares.

Convém acrescentar que a empresa não possui uma norma de segurança ou política de segurança clara e formal e não segue nenhuma norma técnica de segurança da informação.

* Faz-se necessário a criação de um Protocolo de Políticas de Segurança da Informação GeoPlus, com o fito de padronizar processos clara e formalmente, para que a empresa siga as normas de segurança. Com essas informações claras, é possível evitar a desinformação de um funcionário.

Atualmente, não existe um sistema ou processo de verificação rotineiro destes mecanismos, ou seja, os backups não são testados para verificar sua consistência e os arquivos de log não são lidos diariamente.

* Com os backups rotineiros, é importante que seja criado um processo de verificação, pelo menos dos backups completos, pois assim dará mais segurança à integridade das informações, garantindo que nenhuma tenha sido perdida ou corrompida.

7 Acesso a um computador através da rede, em que não é necessário estar fisicamente próximo a este.

8 SSH - *Secure Shell*, programa que permite a execução de comandos em uma máquina remota.

9 SSL - *Secure Socket Layer*

10 *sites* de Internet

11 Neste caso é realizado o *backup* normal, que consiste em armazenar tudo que foi solicitado, visando o incremento da informação após a criação do *backup*.