GESTÃO DE SEGURANÇA DA INFORMAÇÃO: POR QUE SUA PME PRECISA PARA CRESCER?[1]

Gabriel Motta de Souza

Resumo: Quando falamos em Gestão de Segurança da Informação (GSI), é normal que venha em nossas mentes invasão de hackers, de modo geral, nos sistemas das empresas. Como solução imediata, pensamos que um bom antivírus será o suficiente. Mas a questão pode ser mais extensa e complexa do que aparenta. Itens como pessoas, processos, ambientes e tecnologias podem contribuir para sérios problemas de segurança das informações nas empresas e influenciar diretamente no seu crescimento. A GSI possui como base a preocupação com 3 pilares básicos da informação: confidencialidade, integridade e disponibilidade. Deve manter o alinhamento estratégico e objetivos do negócio, visando reduzir os riscos às operações das organizações e garantir a capacidade de operação do negócio, fazendo com que desta forma o negócio e a reputação da empresa sejam protegidos. Vamos usá-la em favor de sua empresa?

Palavras-chave: Confidencialidade. Integridade. Disponibilidade. Gestão de Segurança da Informação para PME. Segurança da Informação. Crescimento Empresarial. Implantação SGSI.

1 INTRODUÇÃO

O presente artigo visa destacar como a Gestão da Segurança da Informação (GSI), hoje em dia tem se tornado fundamental para o sucesso do negócio, tendo em vista a constante variação das ameaças, o crescimento das Pequenas e Médias Empresas (PME), a velocidade em que as informações se propagam e a complexidade em que as infraestruturas se tornam.

As informações aqui contidas, foram obtidas através de análise teórica, com bases bibliográficas e estudo de caso, evidenciando o resultado da aplicação da GSI no âmbito das PMEs, demonstrando que a GSI pode alavancar o crescimento empresarial.

---

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gestão de Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão da Segurança da Informação.

Como base, foi utilizado o Livro Digital da Unisul, Governança e Gestão da Segurança da Informação, o site do Instituto de Tecnologia INFNET, o site da ARCON (Empresa do Grupo NEC) e o estudo de caso das duas empresas, que se disponibilizaram em serem visitadas e responder os questionários solicitados, que deram base para a comprovação do aumento de desempenho após a organização interna e desenvolvimento de políticas que fortaleceram os pilares da informação, tais como: confidencialidade, integridade e disponibilidade.

Espera-se desse artigo, que as Pequenas e Médias Empresas (PME) possam perceber que hoje em dia, a informação é um ativo estratégico essencial para o negócio da empresa e que se faz necessário o tratamento adequado desta, fazendo com que a existência da GSI alinhada ao negócio, possa trazer um diferencial competitivo fazendo com que a empresa cresça de forma organizada, demonstrando assim confiança aos stakeholders.

2 GSI ALINHADA AO NEGÓCIO

A GSI hoje em dia, tem se tornado fundamental para o sucesso do negócio, tendo em vista a constante variação das ameaças, o crescimento das Pequenas e Médias Empresas (PME), a velocidade em que as informações se propagam e a complexidade em que as infraestruturas se tornam.

Lento (2011), afirma que a GSI visa proteger os ativos, reduzir os riscos às operações das organizações a um nível aceitável, garantir a capacidade de operação do negócio, a implementação dos controles de segurança da informação e a reputação da empresa. Influencia diretamente na política de segurança da informação da empresa e deve estar consistente com as leis e normas em vigor, considerando também as políticas e controles internos. Como resultado a GSI deve proporcionar alinhamento estratégico, gestão de riscos, gestão de recursos, gestão de desempenho e entrega de valor (stakeholders por exemplo). Procura garantir a confidencialidade, integridade e disponibilidade das informações, fornecendo qualidade de serviço e maior retorno de investimento (ROI).

Segundo Lento (2011), Neste mundo virtual globalizado, e cada vez mais competitivo, a informação é o maior patrimônio que uma organização pode possuir, se deseja manter-se competitiva. Considerada um ativo estratégico para o negócio da organização, a informação deve receber uma maior atenção no que tange ao seu tratamento, devendo ser protegida e gerenciada quanto ao seu armazenamento e tramitação, evitando que pessoas indesejadas a acessem.

De acordo com o Instituto INFNET, a TI não se limita ao suporte às operações, ela é a salvaguarda dos dados que sustentam a estratégia de crescimento das empresas.

Lento (2011), afirma que o aumento da dependência da tecnologia nos processos da organização cresce a cada momento. A informação e os sistemas que a cuidam passaram a ser fundamentais para o funcionamento das organizações, de tal forma que o acesso à informação de maneira confiável tornou-se uma questão estratégica, um fator de sucesso para o negócio da organização.

A preocupação com a Segurança da Informação pode ser destacada através de diversos dados, como segue:

a. Brasil é um dos países com maior número de roubos pela internet. Reportagem de Michelle Barros (2014, G1).
b. Incidentes Reportados ao Cert.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) – Tipos de ataque – Janeiro a Dezembro de 2016.
c. Os 7 principais tipos de vulnerabilidades em uma empresa. Artigo de Rodrigo Oliveira (2017, ARCON).

Segundo Rodrigo Oliveira (2017), A fórmula mais importante quando falamos em segurança da informação é: **risco = impacto*probabilidade** (risco em segurança da informação é igual ao impacto vezes a sua probabilidade) e seu principal objetivo é mitigar e diminuir a probabilidade de que um ataque seja bem-sucedido de tal forma que o risco seja erradicado do ambiente. E no caso um ataque seja bem-sucedido, que o impacto seja mínimo. Por isso é fundamental conhecer os 7 principais tipos de vulnerabilidades: Físicas, Naturais, Humanas, Hardware, Software, Midias digitais e Comunicação.

Lento (2011), afirma que as organizações podem sobreviver à perda de ativos, incluindo facilidades de processamento, equipamentos e peopleware, mas poucas conseguem sobreviver com a perda das suas informações críticas (projetos, conhecimento das operações de negócio). Entretanto os riscos, benefícios e as oportunidades que estes recursos oferecem têm tornado a governança de segurança um componente fundamental de toda a governança na empresa.

2.1 CASE – Como a análise foi realizada?

Com visitas em clientes, foi possível perceber ao longo do tempo que ainda hoje, a grande maioria das empresas de pequeno e médio porte (PME), além de crescerem de forma desordenada, trabalham diariamente apagando verdadeiros incêndios em diversos setores e isso não é diferente na área de tecnologia. A informação é desencontrada e acaba se perdendo em diversas situações por não haver gestão e segurança da informação, visando garantir pelo menos os três pilares básicos que são: confidencialidade, disponibilidade e integridade, fazendo com que essa informação possa trazer um diferencial competitivo.

Devido a esta situação, comum entre estas empresas, foi realizado um estudo em 2 (duas) PMEs que iniciaram a implantação da GSI e assim demonstrar que uma PME, independentemente do tamanho, usando a GSI tende a ter um crescimento mais rápido e ordenado, devido a sua organização e utilização das tecnologias a seu favor, pois é mais fácil identificar os problemas, gerenciar seus riscos e assim mitiga-los a um nível aceitável, que garanta a entrega de seu produto com qualidade e transpareça confiança para os stakeholders.

Desta forma, a pesquisa nas PMEs foi pura e aplicada, tendo em vista que foi realizada uma análise teórica, com bases bibliográficas, sobre o objetivo da pesquisa fundamentando a aplicação no âmbito das PMEs em análise. Além da pesquisa ser teórica também foi empírica, devido ao estudo dos conceitos da GSI e como foram aplicados nas PMEs.

Já em relação ao aprofundamento da pesquisa, a mesma foi explicativa pois o objetivo foi esclarecer e evidenciar que a GSI pode alavancar o crescimento empresarial.

Em relação ao tipo de pesquisa, a mesma foi qualitativa baseada no estudo de caso das 2 (duas) PMEs, pois os dados foram coletados através de análise nos conceitos bibliográficos pesquisados e nos documentos das PMEs que iniciaram a implantação da GSI. Além da documentação analisada localmente, foi realizada entrevistas com os proprietários e os integrantes do setor de TI, envolvidos no processo de segurança, para melhor entendimento do funcionamento antigo da estrutura de cada PME, bem como as melhorias que foram efetivadas após a implantação da GSI. Após a análise individual das PMEs, foram realizadas comparações entre as empresas, dos pontos em comum no processo de implantação.

Por fim, os documentos que foram analisados e utilizados como base de pesquisa foram:

1. Política de Segurança da PME, no que tange os pilares da confidencialidade, integridade, autenticidade, disponibilidade e não repúdio;

2. Livro digital Unisul, Governança e Gestão da Segurança de Informação;
3. Questionário.

2.2 CASE – Quais foram os resultados ?

Nas visitas às empresas que iniciaram a implantação da GSI na sua infraestrutura a partir de um período determinado de sua existência no mercado, foi perceptível um padrão de organização e com isso um desempenho diferenciado dos colaboradores na execução de suas funções. Nas conversas que tivemos com seus proprietários, os mesmos relataram que após investimento para a aplicação de itens das políticas de segurança, tais como: servidores, filtros de conteúdo, políticas de senhas, rotinas de backup das informações, entre outras, as empresas passaram a ter mais tempo para planejar a execução do trabalho de seus clientes atuais, bem como adquirir novos clientes. O que não era possível pelo volume de trabalho, que achavam que possuíam, perceberam após a aplicação inicial de alguns itens da Política de Segurança da Informação, que a maioria do tempo tomado era para retrabalho por perda de dados ou por falta de foco do colaborador por ter total acesso aos itens pessoais como: e-mails, chats, redes sociais, entre outros, que não eram inerentes a finalidade do serviço a ser desenvolvido na empresa.

As empresas visitadas atuam no ramo de serviços, sendo uma na área de serviços de TI, manutenção de computadores, redes e servidores, e a outra como despachante executando serviços de transferências, emplacamentos e outros serviços vinculados a regularização de veículos junto ao DETRAN. Nos dois casos, anteriormente a implantação de itens da GSI, não se haviam documentos regulatórios, padronização nas tarefas, setores bem definidos, backup dos dados e nem identificação dos ativos de rede. As empresas alegaram que possuíam tanto serviço e falta de mão de obra especializada em determinadas funções, que acabava ocorrendo a sobrecarga de alguns de seus colaboradores. Desta forma, a falta de tempo era hábito dentro das organizações, impossibilitando o planejamento e aplicação de melhorias durante alguns anos. Informaram também que não tinham total conhecimento se a perda de dados constantes, era inerente a má manipulação dos dados pelos colaboradores, quer fosse de forma voluntária ou involuntária, ou se eram efetivamente alvos de ataques de hackers. Afirmaram que devido a isto, acabaram perdendo negócios e com isso consideráveis valores financeiros, o que os levou a buscar soluções para melhorias de suas infraestruturas.

A empresa de tecnologia, aplicou efetivamente a GSI em julho de 2016, já a empresa de despachante em janeiro de 2017 e perceberam que com itens básicos da Política de Segurança da Informação que complementam a GSI, houveram crescimentos de produtividades dos colaboradores de forma considerável, que

resultou ao término do primeiro ano de implantação na melhor gestão dos clientes existentes e um aumento de clientes em torno de 15%. Os itens implantados em comum da política de segurança da informação, criada nas duas empresas foram:

a. Termo de responsabilidade: Ao ser contratado o novo colaborador é instruído, mesmo que verbalmente na presença de outra pessoa que serve de testemunha das normas da empresa, e após isto assina um termo de responsabilidade dando ciência da informação recebida;

b. Política de senhas: foram implantadas no sistema interno, para que as senhas sejam criadas com um padrão de segurança mais elevado;

c. Nivel de acesso lógico: Um servidor foi adquirido visando a junção e organização das informações, implantando-se também controles de acesso aos arquivos. Cada departamento acessa somente os arquivos de seus respectivos interesses. Também foram instalados no servidor Antivírus e Firewall para minimizar acessos indesejados;

d. Bloqueio de conteúdo: Durante o período de trabalho, os colaboradores apenas utilizam os recursos fornecidos pela empresa que são inerentes ao trabalho a ser executado;

e. Bloqueio de Mídias: Pendrives e outros dispositivos, somente são utilizados os fornecidos pela empresa e estes devem permanecer no local combinado após o término do trabalho;

f. Rotina de backups: Com os dados no servidor, criou-se então a rotina de backups conforme necessidade, com uma mídia para recuperação rápida dentro da empresa e a outra que fica externa à empresa;

g. Redundâncias: Foi contratado nas duas empresas, um link de internet adicional e equipamentos adicionais com a finalidade de redundância, já que a grande maioria de seus trabalhos dependem do uso da internet.

As empresas informaram que itens da GSI vem sendo implantados mês a mês, de acordo com a necessidade de cada uma das empresas. Mas essas foram as primeiras 7 (sete) medidas adotadas no primeiro ano e que continuam a implementar outros itens da GSI, que vem a agregar ao bom desempenho já obtido com as implantações iniciais que geraram resultado.

3 SGSI – Como iniciar a implantação?

Embora não exista um passo a passo para uma implantação padrão, até porque isto depende da realidade de cada organização, existem fatores importantes para que se consiga melhores resultados com esforços melhor investidos na implantação do SGSI. Antes de iniciar a implantação do Sistema de Gestão de Segurança da Informação (SGSI), Lento (2011) afirma que precisa do apoio da alta direção na intenção fazer funcionar as atividades de segurança da informação. Se faz necessário também recursos humanos, a fim de criar uma equipe comprometida com a implantação e gerenciamento, recursos econômicos para realizar uma previsão financeira de gastos relativos à implantação e técnicos, com a finalidade de obter os conhecimentos necessários para a devida implantação do SGSI.

Cada empresa tem suas rotinas e particularidades, conforme vimos nas empresas visitadas. Devido a isto, percebe-se que a implantação do SGSI deve ocorrer por etapas, implantando-se o necessário que esteja de acordo com a realidade da organização e assim seguindo aos próximos passos, havendo treinamentos com os envolvidos e análises dos resultados de cada etapa. Porém é um processo que sempre deve ser acompanhado, de tempo em tempo revisado e se precisar readequado à realidade atual da organização, de acordo com as leis vigentes para a melhor efetividade.

Devem ser consultadas as normas vigentes da família ISO/IEC 27000 que se dividem da seguinte forma:

- **ISO/IEC 27000** – São informações básicas sobre as normas da série.
- **ISO/IEC 27001** – Bases para a implementação de um SGSI em uma organização.
- **ISO/IEC 27002** – Certificação profissional, traz códigos de práticas para profissionais.
- **ISO/IEC 27003** – Diretrizes mais específicas para implementação do SGSI.
- **ISO/IEC 27004** – Normas sobre as métricas e relatórios do SGSI.
- **ISO/IEC 27005** – Diretrizes para o processo de gestão de riscos de segurança da informação.

A norma ISO/IEC 27001:2005 por exemplo, tem como requisito geral que a organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta. Apresenta como facilitador para a aplicação de cada requisito do SGSI o modelo de processo PDCA, cujas fases são: Planejamento, Execução, Verificação e ações necessárias para à

Manutenção e Monitoramento do SGSI. Cada uma dessas fases tem suas funções específicas para a devida aplicação.

A fase do planejamento, por exemplo, define o escopo e os limites do SGSI, bem como a política, a abordagem do tratamento de risco da organização, identifica, analisa e avalia os riscos, escolhe os controles para o tratamento dos riscos, entre outros procedimentos. (ISO/IEC 27001:2005)

Na fase de execução, é implementada e operacionalizada a política, controles, processos e procedimentos do SGSI. É quando devemos implementar o plano de tratamento de riscos definido na fase de planejamento, implementar os controles escolhidos, implementar os programas de treinamentos, gerenciar as operações e recursos do SGSI. (ISO/IEC 27001:2005)

Já na fase de Verificação, avalia-se o desempenho dos processos, políticas, objetivos e a experiência prática, além de se reportarem os resultados ao gerenciamento para a revisão. Então faz parte desta fase, detectar erros nos resultados do processamento, identificar falhas e incidentes de segurança, medir a eficiência dos controles com a finalidade de verificar quais necessidades foram atendidas, registrar eventos que realmente causaram impacto no SGSI, entre outros. (ISO/IEC 27001:2005)

Na fase de Manutenção e Monitoramento, são realizadas ações preventivas e corretivas com base nos resultados obtidos da auditoria do SGSI. No entanto fazem parte desta etapa, identificar não conformidades e determinar suas causas, implementar as melhorias identificadas para que não ocorram não conformidades, garantir que as melhorias executadas estejam de acordo com os objetivos da organização, entre outras funções. (ISO/IEC 27001:2005)

4 CONCLUSÃO

Podemos notar nas bibliografias consultadas e nos estudos de caso mencionados, que a implantação da GSI nos dias atuais é de extrema importância para identificar os ativos da organização, mitigar os riscos e garantir os pilares da informação dando segurança para a organização e oferecendo um diferencial competitivo.

No mundo globalizado de hoje, não há mais espaço para pequenas e médias empresas (PME) crescerem de forma desordenada como vinha ocorrendo ao longo dos anos. Estas devem buscar recursos e conhecimentos para que venham a se posicionar no mercado com competividade e inovações, que venham a despertar o interesse de investidores e clientes para alavancar o negócio. Sendo assim a GSI é parte essencial da empresa neste processo, pois vem a dar mais credibilidade da empresa perante os stakeholders. Além disso, A GSI faz com que a informação trafegue pela empresa de forma mais rápida e segura, minimizando também que seu concorrente tenha acesso as informações vitais da empresa, que são relativas ao negócio.

A GSI também vem garantir a continuidade do negócio que antigamente muitas empresas simplesmente encerravam suas atividades por ter havido alguma fatalidade como inundações, queima da informação, falecimento da pessoa que é o único conhecedor de toda a informação da empresa, entre outros casos. Todos os itens da GSI são importantes, itens como as normas vigentes devem ser analisadas para as corretas implantações.

Se analisarmos a GSI, veremos que faz parte da Gestão de Tecnologia da Informação (GTI), que de uma forma mais ampla está sob responsabilidade direta da alta gerência, para análises mais estratégicas de vantagem competitiva, por exemplo, de modo a se estabelecer claramente o processo de tomada de decisões e as diretrizes para o gerenciamento, monitoramento e uso da TI visando, por exemplo, otimizar o uso de recursos. Mas tanto a GTI quando a GSI, devem manter o alinhamento estratégico e objetivos do negócio e devem se preocupar com pessoas, processos e tecnologias.

De uma forma bem prática, o que devemos ter em mente quando pensamos em por que fazer a Gestão de TI, basicamente o que queremos é:

- Alinhar o objetivo de TI com o negócio;
- Automatizar, padronizar e unificar processos de TI;
- Otimizar o uso dos recursos;
- Gerenciar riscos de forma apropriada;
- Facilitar o trabalho de auditoria; e

- Estar em conformidade com partes externas (leis vigentes).

Já quando pensamos em por que Segurança da Informação, basicamente o que queremos é:

- Proteger os ativos, o negócio e a reputação da empresa;
- Alinhar o que proteger com o negócio;
- Gerenciar os riscos de forma a minimizá-los de forma apropriada pois quanto mais facilidade, mais ameaças que hoje são em sua maioria digitais;e
- Estar em conformidade com aspectos legais e regulatórios.

UNISUL

REFERÊNCIAS

BARROS, Michelle (2014). G1- Jornal da Globo. Disponível em: <http://g1.globo.com/jornal-da-globo/noticia/2014/07/brasil-e-um-dos-paises-com-o-maior-numero-de-roubos-pela-internet.html> . Edição do dia: 02 jul. 2014. Publicado em: 03 jul. 2014. Acesso em: 10 nov. 2017.

CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) – Incidentes Reportados, Janeiro a Dezembro de 2016 - Tipos de ataque. Disponível em: <https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html>. Publicado em 14 jul. 2017. Acesso em: 10 nov. 2017.

INFNET, Instituto. A importância da Segurança da Informação para pequenas e médias empresas – Infnet.edu.br. Disponível em: < http://www.infnet.edu.br/esti/a-importancia-da-seguranca-da-informacao-para-pequenas-e-medias-empresas >. Acesso em: 30 out. 2017.

LENTO, Luiz Otávio Botelho. Governança e Gestão da Segurança de Informação – Livro Digital. Unisul Virtual, 2011.

OLIVEIRA, Rodrigo. Analista de Segurança da Informação da ARCON (empresa do Grupo NEC) - Os 7 principais tipos de vulnerabilidades em uma empresa. Disponível em: https://www.arcon.com.br/blog/os-7-principais-tipos-de-vulnerabilidades-em-uma-empresa. Publicado em: 24 ago. 2017. Acesso em: 11 nov. 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2005 - Tecnologia da informação - técnicas de segurança - sistemas de gestão da segurança da informação – requisitos. Rio de Janeiro, 2006

ANEXOS

ANEXO A – Questionário coleta de dados da empresa Premium Tecnologia

ANEXO B – Questionário coleta de dados da empresa Despachante Macedo (ROCA)

ANEXO A – Questionário coleta de dados da empresa Premium Tecnologia

UNISUL

UnisulVirtual
A sua universidade a distância

Universidade do Sul de Santa Catarina – Unisul
Campus Virtual

Trabalho de Conclusão de Curso

Curso: **Gestão de Segurança da Informação**
Orientador: **Luiz Otávio B. Lento**
Nome do aluno: **Gabriel Motta de Souza**

Questionário:

1. Nome da Empresa
   Premium Soluções Tecnológicas
2. Área de Atuação
   Serviços TI
3. Quanto tempo de mercado
   5 anos. Desde 2013
4. A empresa possui uma Política de Segurança da Informação vigente? A partir de quando foi implantada?
   Sim. Julho 2016
5. Quando o funcionário é contratado, existe um termo de responsabilidade onde é assinado afirmando ter lido as políticas da empresa?
   Sim. Repassa as informações verbalmente e é assinado o termo de ciência das informações recebidas.
6. O que não pode parar dentro do seu ambiente de trabalho (tratando-se de tecnologia)? Por quê?
   Servidor, Ativos de rede.

UNISUL

7. A infraestrutura tecnológica da empresa é instável? Caso seja, com qual frequência (aproximadamente) o sistema/ambiente deixa de funcionar?
Antes da implantação das políticas normalmente havia quedas aproximadamente 3 vezes na semana. Após a implantação, o problema foi solucionado.
8. Existem rotinas de backup de dados bem definida?
Após a política sim. Diário, Semanal e Mensal.
9. Em relação ao local de armazenamento dos backups é interno, externo ou existem cópias dentro e fora da empresa?
Interno e Externo
10. Existem controles de acesso lógicos e físicos?
Sim. lógicos
11. Já houve invasão de hackers? Se sim, houve perda de dados? O sistema ficou fora? Por quanto tempo?
Sim. Antes da política houveram perdas de dados e a empresa sem sistema por aproximadamente 1 semana.
12. Responsável pelo preenchimento do questionário
Marcio Benincla

Assinatura

Entrevista realizada em 28/03/2018 às 16:00h.

ANEXO B – Questionário coleta de dados da empresa Despachante Macedo (ROCA)

UNISUL

UnisulVirtual
A sua universidade a distância

Universidade do Sul de Santa Catarina – Unisul
Campus Virtual

Trabalho de Conclusão de Curso

Curso: **Gestão de Segurança da Informação**

Orientador: **Luiz Otávio B. Lento**

Nome do aluno: **Gabriel Motta de Souza**

Questionário:

1. Nome da Empresa
   Despachante Macedo (Roca)
2. Área de Atuação
   Serviços de Licenciamento de documentações de veículos
3. Quanto tempo de mercado
   20 anos
4. A empresa possui uma Política de Segurança da Informação vigente? A partir de quando foi implantada?
   Sim. Em implantação por empresa terceirizada. Iniciou-se em JAN/2017.
5. Quando o funcionário é contratado, existe um termo de responsabilidade onde é assinado afirmando ter lido as políticas da empresa?
   Sim. Repassa as informações de forma verbal e solicita assinatura de ciência.
6. O que não pode parar dentro do seu ambiente de trabalho (tratando-se de tecnologia)? Por quê?
   Servidor, internet e ativos de rede.

UNISUL

7. A infraestrutura tecnológica da empresa é instável? Caso seja, com qual frequência (aproximadamente) o sistema/ambiente deixa de funcionar?

Antes das políticas Sim. Porém com a implantação delas, sanou-se os problemas que vinham ocorrendo em quase todos os dias, pelo menos 1 a 2 horas por dia.

8. Existem rotinas de backup de dados bem definida?

Sim. Diária, Semanal e Mensal.

9. Em relação ao local de armazenamento dos backups é interno, externo ou existem cópias dentro e fora da empresa?

Interno e externo.

10. Existem controles de acesso lógicos e físicos?

Sim. Lógicos

11. Já houve invasão de hackers? Se sim, houve perda de dados? O sistema ficou fora? Por quanto tempo?

Houve invasão no passado, parando a empresa pois dados foram perdidos. Desde as políticas implementadas os problemas foram solucionados.

12. Responsável pelo preenchimento do questionário

Lucia Macedo

Lúcia Macedo

Assinatura

Entrevista realizada em 12/04/2018.