PSI – Política de Segurança da Informação

Documento de Diretrizes e Normas Administrativas

V.1.0

Índice

1 Termos e Definições

TI: Tecnologia da Informação

Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.

Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Firewall: É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

Endpoint: Um endpoint, ou em Português ponto de extremidade, é um sinal de terminação ou conclusão. A terminologia se refere aos dispositivos que estão na ponta da rede, assim como: laptop, desktop, servidor e outros softwares ou dispositivos móveis e de rede.

Servidor: Um servidor é um computador equipado com um ou mais processadores, bancos de memória, portas de comunicação e, ocasionalmente, algum sistema para armazenamento de dados como hard disks internos ou memórias SSD. Capazes de executar um conjunto específico de programas ou protocolos para fornecer serviços para outras máquinas ou clientes, servidores são equipamentos dedicados a executar aplicações e serviços dentro de uma rede LAN ou WAN.

Rede: Conjunto de máquinas eletrônicas com processadores capazes de trocar informações e compartilhar recursos, interligados por um subsistema de comunicação, ou seja, é quando há pelo menos dois ou mais computadores, e outros dispositivos interligados entre si de modo a poderem compartilhar recursos físicos e lógicos

Dispositivo de saída: São dispositivos que exibem dados e informações processadas pelo computador. Por outras palavras, permitem a comunicação no sentido do computador para o utilizador. Exemplos: projetor de vídeo, impressora e monitor.

2 Objetivo da política de segurança

Este documento é destinado a garantir que os recursos de informática e a informação serão utilizadas de maneira adequada pelos colaboradores externos e internos da organização, visando a proteção dos ativos da empresa Atlântica Minas, sabendo-se que a informação é um dos principais patrimônios do mundo dos negócios, manter um fluxo de qualidade é determinante para o sucesso da empresa dentro do mundo dos negócios que é extremamente competitivo. Portanto estabelecer diretrizes estratégicas que visam garantir a disponibilidade, integridade, confidencialidade e autenticidade dos patrimônios da companhia é vital.

3 Requisitos sobre a PSI.

Para a uniformidade do documento, a PSI deverá ser comunicada a todos os colaboradores da Atlântica Minas a fim de que a política seja cumprida dentro e fora da empresa, preservando a missão, visão e valores da mesma.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos relacionados a vazamento de informações críticas para a empresa. Sendo necessário então, a assinatura de um termo de responsabilidade.

A PSI é correlacionada ao framework COBIT5 e um subprocesso especifico do mesmo definido como DSS05, o framework é estabelecido como um referencial em boas práticas de governança em TI (tecnologia e informação) e o seu subprocesso é especifico para a segurança da informação, protege informações da organização para manter o nível de risco aceitável para a segurança da informação de acordo com a política de segurança, portanto a PSI é atrelada aos princípios do DSS05, embasado com os processos que a empresa Atlântica Minas realiza.

Concluindo o tópico, a política está dividida em segurança da estrutura de informática e política de segurança física, sendo que a primeira trata do acesso aos recursos de rede, sistemas e correio eletrônico. A segunda aborda o acesso físico a sala de servidores e outros hardwares.

4 Responsabilidades

4.1 Colaboradores

Colaboradores é definido como qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a Atlântica Minas e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Aos colaboradores internos no período de contratação será apresentado o formulário de responsabilidade e sigilo das informações que poderá ser assinado posterior à leitura da PSI da Atlântica Minas.

4.2 Colaboradores Temporários

Os riscos associados à sua condição são descritos e explícitos na fase de contratação, visto que entender os riscos relacionados à condição especial do colaborador é essencial para o cumprimento de seus deveres.

O contrato poderá ser revogado caso após verificação, justificativa de motivo o colaborador não estiver cumprindo com as condições definidas no aceite.

4.3 Gestores de Pessoas e Processos

Apresentar postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, tanto temporários ou não, a responsabilidade do cumprimento da PSI da Atlântica Minas.

Antes de conceder acesso às informações da instituição, exigir a assinatura do acordo de confidencialidade dos colaboradores, com intuito de proteger as informações crucias da organização contra roubo, que mesmo que desligado da empresa o empregado deva cumprir com a assinatura de sigilo.

4.4 Colaboradores da área de segurança da informação

Tomar iniciativa em propor as metodologias e os processos específicos para a segurança da informação, com avaliações de riscos e classificação da importância da informação, além de apoiar quaisquer iniciativas relacionadas à segurança dos ativos de informação.

Publicar e promover as versões da PSI, através da publicação realizar uma conscientização dos colaboradores em relação à relevância da segurança da informação para os negócios da Atlântica Minas, mediante campanhas, palestras, treinamentos e outros meios.

Analisar incidentes ocorridos na empresa e procurar soluções relacionadas aos tópicos descritos na PSI.

Procurar sempre manter os gestores cientes dos problemas envolvendo a segurança da informação.

Para que a PSI esteja em pleno funcionamento é de grande importância a utilização de sistemas de firewall, software de segurança (antivírus) e sistema de monitoramento de rede.

5 Proteger contra malware.

5.1 Aos responsáveis de TI:

Realizar treinamento periódico a cada 3 meses, aos colaboradores internos, sobre download de software maliciosos, malwares e spyware em e-mails, phishing, uso da internet e todos os principais riscos à Atlântica Minas demonstrando os possíveis prejuízos.

Para a ministração de treinamento será necessário rever e avaliar as potenciais ameaças que podem surgir ao longo do tempo, através de boletins e notícias de fabricantes e veículos seguros. A verificação periódica acontecerá todos em todos os dias de expediente na Atlântica, no primeiro horário da manhã. Exemplo de sites com boletins de segurança: https://www.securityfocus.com/.

Cabe ao responsável de TI instalar e manter atualizadas ferramentas de proteção contra software malicioso, tais como: Windows Defender e Kaspersky Anti-ransomware em todos os equipamentos end-points da Atlântica Minas.

6 Gerenciar a segurança da rede e conectividade.

6.1 Aos colaboradores:

Somente terá acesso à rede corporativa da Atlântica Minas, com acesso aos sistemas internos, informações e documentos sensíveis, colaboradores que necessitem desses mesmos serviços para a execução de suas tarefas, limitados a sua esfera de atribuições. Esse acesso só poderá ser feito por computadores pertencentes à Atlântica Minas.

Os equipamentos que não são de posse da Atlântica Minas, para a utilização de sistemas e arquivos contidos na rede interna, necessitará de autorização prévia do Diretor Administrativo e liberação do responsável de TI da organização.

Qualquer pessoa que não se enquadre em alguma das situações de necessidade de utilização da rede interna da Atlântica Minas, poderá utilizar a rede convidado para utilização dos recursos de internet.

6.2 Acesso à internet

Qualquer pessoa que não se enquadre em alguma das situações de necessidade de utilização da rede interna da Atlântica Minas, poderá utilizar a rede convidado para utilização dos recursos de internet.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio ou aplicação armazenadas na rede, estejam elas em qualquer lugar, visando assegurar o cumprimento da política de segurança da informação.

A internet disponibilizada aos colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos das respectivas unidades.

Os colaboradores com acesso à internet poderão fazer downloads somente através da permissão do administrador da rede e consciente de que o programa está ligado as atividades da Atlântica Minas, procurando sempre providenciar o que for necessário para regularizar a licença e o registro dos programas baixados.

Em hipótese alguma os colaboradores poderão utilizar os recursos da Atlântica Minas para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

7. Gerenciar a segurança dos endpoints (computadores e servidores).

7.1 Atlântica Minas:

É de responsabilidade da organização o fornecimento recursos tecnológicos que possibilitem a execução das tarefas de cada colaborador.

7.2 Ao responsável de TI:

Configurar os sistemas operacionais de maneira que o usuário Administrador seja de posse do responsável de TI, restringindo os colaboradores da instalação e desinstalação de programas sem a devida autorização, solicitada ao responsável de TI. Deverá também ser instalado e configurado em todas as maquinas um antivírus para a melhor proteção do sistema.

Manter todos os dispositivos atualizados, mantendo as atualizações do sistema e segurança sempre up-to-date.

O descarte de dispositivos deverá ser efetuado somente quando os dispositivos estiverem sem reparo, devendo ter toda sua parte de armazenamento inutilizada pelo responsável de TI, evitando vazamento de qualquer informação.

Segurança do servidor:

O ambiente em que serão alocados os servidores deve ter o tamanho adequado para todos os equipamentos, fios, cabos e também para a sua equipe de TI poder se movimentar quando precisar fazer algum ajuste ou manutenção. É extremamente necessário a utilização de ar refrigerado com a temperatura média do ambiente em 21ºC, pois o calor em excesso pode levar o servidor a superaquecimento afetando a vida útil do mesmo.

É extremamente necessário a utilização de nobreak para eventuais quedas de energia que forçam o desligamento indevido do servidor.

Rotinas de backups são necessárias, devendo fazer o uso de 2 rotinas diferentes: Backup completo do sistema utilizando no mínimo 2 HDs externos de capacidade de armazenamento igual ou superior ao do servidor, fazendo a alternância dos mesmos diariamente, e a utilização de backup na nuvem. As rotinas devem estar programadas para a execução no horário superior a 1 hora após o término do expediente.

7.3 Aos colaboradores:

É proibido todo procedimento de abertura e manuseio dos computadores para reparo físico, de instalação, desinstalação e alterações de configurações de sistemas efetuado pelos colaboradores, devendo somente ser executados pelo responsável de TI.

Arquivos pessoais e/ou não pertinentes às atividades da Atlântica Minas não deverão ser nem copiados ou movidos para os drivers da rede, pois podem congestionar o tráfego de arquivos e sobrecarregar o armazenamento dos servidores. Caso verificado a existência desses arquivos, os mesmos se encontrarão sujeitos a exclusão permanentemente e sem aviso prévio.

Todo computador é entregue para o uso de somente de um (1) colaborador, que deverá cadastrar um usuário com senha e evitar sua utilização por partes não autorizadas. Todo computador deverá conter um bloqueio automático após 3 minutos de inutilização do mesmo.

É estreitamente proibido as seguintes práticas:

• Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;

• Burlar quaisquer sistemas de segurança;

• Acessar informações confidenciais ou não pertinentes sem explícita autorização do proprietário;

• Vigiar secretamente outrem por dispositivos eletrônicos ou softwares;

• Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

• Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

• Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;

• Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

Observações finais:

É vetada a entrada de terceiros em qualquer ambiente da Atlântica Minas sem o acompanhamento de um colaborador devidamente autorizado.

8 Gerenciar identidade de usuário e acesso lógico.

8.1 Ao responsável de TI:

Cabe ao administrador de rede da TI garantir que todos os usuários tenham acesso às informações, direitos de acesso de acordo com as suas necessidades e nível hierárquico de função dentro da empresa, sendo assim, é necessário que seja feita uma coordenação com as unidades de negócios que gerem os seus próprios direitos de acesso dentro dos processos, definindo explicitamente o acesso que cada pessoa deva ter dentro da rede.

Garantir que todos os usuários (internos, externos e temporários) cadastrados na rede possuam uma forma de serem identificados exclusivamente, e que suas respectivas funções em sistemas de TI sejam citadas também (desenvolvimento e manutenção, infraestrutura de TI, negócios).

Para a melhor procedência da prática, necessário o preenchimento de documentação com os campos de atuações e suas respectivas funções. Realizar análise de todas as contas de usuários periodicamente, para evitar que contas tenham privilégios desnecessários e utilização de contas de colaboradores que deixaram a organização, as desabilitando devidamente.

9 Gerenciar o acesso físico aos ativos de TI.

A infraestrutura de TI da Atlântica Minas é centralizada em um único espaço físico, cujo o acesso é totalmente restrito aos empregados a não ser o responsável pelo setor de TI.

Caso seja necessário a entrada de um funcionário de qualquer função nas instalações de TI, é preciso que seja monitorado pelo próprio responsável da TI.

10 Gerenciar documentos sensíveis e dispositivos de saída

10.1 Ao responsável de TI:

É função do responsável da TI realizar um inventario especificando todos os dispositivos de saída que fazem partes dos ativos da Atlântica Minas.

Realização de inventario de controle de todos os documentos sensíveis da Atlântica Minas que serão armazenados na sala de arquivo.

Em caso de descarte, dispositivos de saída deverão primeiro ser destruídos e inutilizados de forma que informação alguma possa ser extraída dos mesmos.

10.2 Aos colaboradores:

Documentos sensíveis devem ser armazenados na sala de arquivo. Todos os documentos devem ser catalogados, e por ocasião de sua retirada, deverá ser preenchida uma lista de controle com o nome do colaborador que esteja o utilizando.

Documentos sensíveis que perderam seu valor serão passados para a pasta de documentos de descarte, após 6 meses sem o uso dos mesmos, poderão ser devidamente destruídos e descartados, com a autorização prévia da diretoria pertinente ao assunto.

_____	_____
Responsável setor de Tecnologia da Informação	Diretor Administrativo