VDM CORP

FACULDADE DE TECNOLOGIA SENAC GOIÁS

Segurança da Informação

Aldo Brito
Jordan Gladys
Liniker Lettierre
Rony Carneiro

POLÍTICA DE SEGURANÇA

Diego Guedes

GOIÂNIA,
2016

VDM CORP

Aldo Brito
Jordan Gladys
Liniker Lettierre
Rony Carneiro

POLÍTICA DE SEGURANÇA

Relatório apresentado como requisito parcial para obtenção de aprovação na disciplina de Implantação e Gestão de SI, no Curso de Segurança da Informação, na Faculdade de Tecnologia Senac Goiás.

Diego Guedes

GOIÂNIA,
2016

VDM CORP

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

VDM CORP
Goiânia/2016

VDM CORP

SUMÁRIO

VDM CORP

INTRODUÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da VDM CORP para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição. A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país. Com a intenção de aumentar a segurança da infraestrutura tecnológica visando a orientação de nossos funcionários para a utilização dos ativos de tecnologia da informação disponibilizados.

OBJETIVO

A Política de Segurança da Informação da VDM CORP é uma declaração formal da empresa acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores. Seu propósito é estabelecer as diretrizes a serem seguidas pela VDM CORP no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

A VDM CORP preserva as seguintes diretrizes:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Sistemas sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela VDM CORP pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços. A VDM CORP, por meio da Gerência de Sistemas, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

REQUISITOS DA PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da VDM CORP a fim de que a política seja cumprida dentro e fora da empresa.

Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação.

Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

Deverá constar em todos os contratos do VDM CORP o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

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. Eles devem assinar um termo de responsabilidade.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Gerência de Sistemas e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela VDM CORP ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A VDM CORP exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI será implementada na VDM CORP por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

REGRAS DE USO DOS COLABORADORES EM GERAL

Colaborador é qualquer pessoa física que exerça uma função nesta organização, interna ou externa, independente do regime de contratação.

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

Cabe a Área de Segurança da Informação:

- Desenvolver metodologias e processos específicos para a avaliação de riscos, classificação da informação.

- Divulgar a PSI e suas atualizações, assim que aprovadas pelo Comitê de Segurança da Informação.

- Trabalhar para a conscientização de todos os colaboradores sobre a importância da segurança da informação organizando palestras, treinamentos, campanhas, etc.., sempre que for julgado necessário pelo Comitê de Segurança da Informação.

- Ajudar na análise de incidentes de segurança da informação.

- Estar sempre em comunicação com o Comitê de Segurança da Informação, informando-o sobre novos eventos e incidentes de segurança da informação para que os mesmos possam ser avaliados.

CONTROLE DE ACESSO

O acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação.

As regras de controle de acesso levam em consideração as políticas para autorização e disseminação da informação. O registro daquilo que foi feito estará no nome do colaborador, logo, se alguém que não o colaborador, ainda que com boas intenções, fizer uso de sua senha e cometer algum ato ilícito, algum erro de no sistema, algum acesso não autorizado, a responsabilidade será do colaborador

- A Gerência Administrativa é o setor responsável por solicitar o cadastramento ou exclusão de funcionários e colaboradores, devendo proceder ao registro das informações básicas dos mesmos.
- Em caso de desligamento do funcionário ou colaborador, caberá à Gerência Administrativa a imediata solicitação de exclusão do acesso do mesmo.
- O cadastramento da senha será realizado pela Gerência Técnica, a qual fornecerá o nome de usuário e senha inicial ao colaborador presencialmente.
- A senha inicial só será fornecida ao próprio funcionário ou colaborador, sob nenhuma hipótese será informada a outra pessoa.
- A senha é de total responsabilidade do colaborador, sendo terminantemente proibida sua divulgação ou empréstimo a qualquer outra pessoa, nem mesmo da Gerência Técnica, devendo a mesma ser alterada imediatamente no caso de suspeita de sua divulgação.
- Em caso de esquecimento ou bloqueio de senha, o colaborador deverá entrar em contato com a Gerência Técnica que irá confirmar algumas informações de cadastro, gerar uma nova senha e encaminhá-la para um dos e-mails cadastrados do solicitante.
- Qualquer ato praticado com a utilização da senha será responsabilidade do seu respectivo colaborador. Não será aceita alegação de que outra pessoa utilizou algum recurso com a senha do colaborador

CORREIO ELETRÔNICO

O e-mail, seja pela sua agilidade, seja pela facilidade proporcionada, é tido como uma das principais formas de comunicação. Os servidores de e-mail da VDM CORP possuem software antivírus que são atualizados diariamente, mas, como o número de pragas virtuais cresce exponencialmente a cada dia, alguns cuidados por parte do usuário e outros mais profundos por parte da Gerência Técnica são necessários.

- A VDM CORP disponibilizará uma caixa postal eletrônica (e-mail) para seus funcionários, a qual deverá ser utilizada exclusivamente para troca de mensagens relacionadas com a atividade desempenhada na empresa;
- A VDM CORP poderá impor limites de armazenamento e de banda utilizada de acordo com os recursos disponíveis, a fim de manter a continuidade dos serviços;
- A VDM CORP poderá monitorar a utilização do serviço de e-mail, inclusive analisar o conteúdo das mensagens, de forma a garantir a confidencialidade das informações transitadas;
- A VDM CORP não se responsabilizará por qualquer mensagem enviada por seus colaboradores que venham a ferir qualquer tipo de legislação vigente, ficando o emissor da mensagem responsabilizado por quaisquer danos causados;
- Não é permitida a utilização das contas de e-mail para envio de arquivos não relacionados com a atividade desempenhada, principalmente material fotográfico, vídeos, músicas e apresentações não relacionadas com os objetivos da empresa;
- Cada colaborador receberá uma conta cujo nome será gerado por sistema próprio, podendo esta conta possuir 1 (um) apelido - “alias”, escolhido pelo seu proprietário;
- A VDM CORP adotará mecanismos para evitar a disseminação de vírus, trojans, códigos maliciosos e demais pragas virtuais no envio ou recepção de e-mail. Esta medida não exime a responsabilidade e os cuidados que o colaborador devem adotar para evitar danos aos recursos disponibilizados e roubo de informações. Devido a estes mecanismos, algumas mensagens suspeitas poderão ser descartadas sem aviso;

INTERNET

A internet é a maior fonte de dados e a mais poderosa ferramenta de trabalho atual e assim deve ser considerada quando utilizada dentro da empresa, em horário de expediente

Como ferramenta de trabalho.

Cada colaborador realizara o cadastro na tela do HOTSPOT ao se conectar no Wi-Fi da empresa.

A VDM CORP disponibilizará acesso à internet aos colaboradores que necessitem deste recurso para execução de suas tarefas, ficando o colaborador responsável pelos acessos registrados em sua sessão de conexão com seu usuário de acesso

Visando a otimização dos canais (links) de acesso à internet, a proteção contra-ataques de vírus e hackers e, ainda, o aumento da produtividade dos colaboradores, é vedada a utilização do acesso à internet para os seguintes fins:

- Acesso a conteúdo não relacionado com a atividade desempenhada;
- Download de arquivos não relacionados com a atividade desempenhada;
- Utilização de redes de relacionamentos;
- Download de arquivos ou programas ilegais;
- Acesso a rádios on-line ou servidores de stream de áudio ou vídeo

- Utilização ou acesso de programas de rede P2P para compartilhamento de arquivos, músicas ou vídeos;
- Utilização de programas de mensagens instantâneas não homologados e autorizados pela Gerência Técnica;
- Utilização de qualquer programa não homologado pela Gerência Técnica que faça acesso à internet;
- Utilizar os recursos da empresa para fazer o download ou distribuição de software ou dados não legalizados
- A internet poderá ser utilizada no horário de almoço, ou fora de expediente, para acesso a conteúdo não relacionado com a atividade desempenhada pelo colaborador, desde que dentro das regras de uso definidas nesta política;
- Periodicamente são gerados relatórios de LOG, com as categorias e sites acessados por usuário e, se necessário, haverá a publicação destes relatórios;

A VDM CORP manterá softwares e sistemas que monitoram e gravam todos os usos de internet através da rede e das estações de trabalho da empresa;

DISPOSITIVOS MOVEIS

A VDM CORP deseja preservar a facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem alguns equipamentos portáteis disponibilizados pela empresa ou aprovado e permitido por sua Gerência de Sistemas, como: notebooks e smartphones.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

A VDM CORP, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na VDM CORP, mesmo depois de terminado o vínculo contratual mantido com a empresa.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da Gerência de Sistemas.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Gerência da VDM CORP.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela VDM CORP, notificar imediatamente seu gestor direto e a Gerência de Sistemas.

Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponibilizados pela organização para os colaboradores realizarem suas atividades corporativas são de propriedade da empresa e exclusivos para realização das mesmas.

A realização de manutenção em qualquer equipamento deve ser realizada apenas por colaboradores responsáveis por esta função ou por terceiro indicado pelos mesmos e aprovados pela gerencia. A solicitação de manutenção deve ser realizada por meio de chamado técnico no software

HelpDesk.

Todos as estações de trabalho devem possuir software antivírus instalado e atualizado. Em caso de suspeita de infecção por vírus de computador ou mau funcionamento do software, antivírus devem ser informadas imediatamente através do sistema helpdesk.

Arquivos pessoais como fotos, vídeos e músicas, não devem ser armazenados nos drivers de rede disponibilizados sob o risco de sobrecarregá-los. Caso esses arquivos sejam encontrados nesses drivers, são apagados sem aviso prévio.

Arquivos importantes para a empresa devem ser salvos nos drivers de redes disponibilizados da forma mais organizada possível. Esses arquivos devem possuir nomes que possibilitem sua fácil identificação.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Todas as estações de trabalho devem ter senha de BIOS conhecida apenas por quem faz a manutenção dos mesmos.
- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

- Qualquer mudança na configuração deve ser solicitada previamente ao departamento técnico, só podendo ser realizado pelo mesmo ou por colaborador autorizado pela gerencia.
- Toda estação de trabalho que não estiver em uso, deve ser bloqueada só podendo ser desbloqueada com o uso da senha de um colaborador com acesso a mesma.
- Todos os equipamentos devem ter sua senha padrão alterada imediatamente após sua aquisição.
- Todo equipamento deve gerar e armazenar logs para posterior auditoria.

DATACENTER

O acesso ao datacenter deve ser restringido por meio de biometria ou cartão magnético e horário. Esses acessos devem ser registrados com o uso de software e auditados semanalmente.

Colaboradores que não tenham acesso liberado ao datacenter, mas que precisem eventualmente acessá-lo, devem ser cadastrados como visitantes e o seu acesso registrado com os de colaboradores com acesso. Além disso, devem ser acompanhados todo o tempo por outro colaborador da área.

O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto famígero ou inflamável. Caso seja necessário retirar algum equipamento de dentro do datacenter, o procedimento só será realizado com prévia autorização do administrador do datacenter por escrito e devidamente identificada.

Em caso de demissão de um colaborador com acesso ao datacenter, a autorização do mesmo deve ser revogada imediatamente do sistema de autenticação.

BACKUP

Os backups devem ser realizados automaticamente com o uso de ferramentas de agendamento. Essas ferramentas devem ser verificadas diariamente para garantir o funcionamento, atualização e correção de erros. Os colaboradores responsáveis pelo backup devem analisar o desempenho do mesmo diariamente e sugerir melhorias sempre que for necessário. Também ficam responsáveis por verificar a necessidade de atualização dos softwares de backup, compra de mídias de armazenamento, fim da licença destes softwares e qualquer outra questão que venha a prejudicar a realização dos backups.

As mídias de backup devem ser armazenadas em ambientes seguros que impeçam a degradação das mesmas e mantendo a maior distância possível do datacenter. Essas mídias

também devem ser muito bem identificadas com o período e conteúdo e de forma não manuscrita para evitar que os dados fiquem ilegíveis.

Mídias que apresentam erros devem primeiramente ser inutilizadas.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

MONITORAMENTO

A VDM CORP realizara o monitoramento de tudo que acontece na empresa para detectar atividades não autorizadas de processamento da informação.

Todos os sistemas são monitorados e os eventos de segurança da informação serão registrados.

Os registros (log) de operador e registros (log) de falhas são utilizados para assegurar que os problemas de sistemas de informação são identificados.

Todo o monitoramento do sistema será utilizado para checar a eficácia dos controles adotados e para verificar a conformidade com o modelo de política de acesso.

14.1 Registros de auditoria

Os registros de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação são produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.

Os registros de auditoria incluem:

a. Identificação dos usuários;
b. Datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (log-on) e saída (log-off) no sistema;
c. Identidade do terminal ou, quando possível, a sua localização;
d. Registros das tentativas de acesso ao sistema aceitas e rejeitadas;
e. Registros das tentativas de acesso a outros recursos e dados aceitos e rejeitados;
f. Alterações na configuração do sistema;
g. Uso de privilégios;
h. Uso de aplicações e utilitários do sistema;
i. Arquivos acessados e tipo de acesso;
j. Endereços e protocolos de rede;
k. Alarmes provocados pelo sistema de controle de acesso;
l. Ativação e desativação dos sistemas de proteção, tais como sistemas de antivírus e sistemas de detecção de intrusos.

Os registros de auditoria contêm dados pessoais confidenciais e de intrusos. Para maior segurança os administradores de sistemas não têm permissão de exclusão ou desativação dos registros de suas próprias atividades.

14.2 Proteção das informações dos registros

Os recursos e informações de registros são protegidos contra falsificação e acesso não autorizado.

É implementado a proteção contra modificações não autorizadas e problemas operacionais com os recursos dos registros, como:

A. Alterações dos tipos de mensagens que são gravadas;
B. Arquivos de registros sendo editados ou excluídos;
C. Capacidade de armazenamento da mídia magnética do arquivo de registros excedida, resultando em falhas no registro de eventos ou sobreposição do registro de evento anterior.

Alguns registros de auditoria podem ser guardados como parte da política de retenção de registros ou devido aos requisitos para a coleta e retenção de registros de sistema normalmente contêm um grande volume de informações e muitos dos quais não dizem respeito ao monitoramento da segurança.

14.3 Registros de administrador e operador

A atividades dos administradores e operadores do sistema são registradas.

Esses registros incluem:

A. Na hora em que o evento ocorreu (sucesso ou falha);
B. Informações sobre o evento (exemplo: arquivos manuseados) ou falha (exemplo: erros ocorridos e ações corretivas adotadas);
C. Que conta e que administrador ou operador estava envolvido;
D. Que processos estavam envolvidos.

Os registros de atividades dos operadores e administradores dos sistemas são analisados criticamente em intervalos regulares.

14.4 Registros de falhas

As falhas ocorridas são registradas e analisadas, e que serão adotadas ações apropriadas.

As falhas informadas pelos usuários ou pelos programas de sistema relacionado a problemas com processamento da informação ou sistemas de comunicação serão registradas. Convém que existam regras claras para o tratamento das falhas informadas, incluindo:

A. Análise crítica dos registros de falha para assegurar que as falhas foram satisfatoriamente resolvidas;

B. Análise crítica das medidas corretivas para assegurar que os controles não foram comprometidos e que a ação tomada é completamente autorizada.

14.5 Sincronização dos relógios

Os relógios de todos os sistemas de processamento da informação relevantes, dentro da organização ou do domínio de segurança, são sincronizados de acordo com a hora oficial local.

A interpretação correta do formato data/hora é importante para assegurar que o timestamp reflete a data/hora real. Informações adicionais

O estabelecimento correto dos relógios dos computadores é importante para assegurar a exatidão dos registros de auditoria, que podem ser requeridos por investigações ou como evidências em casos legais ou disciplinares. Registros (log) de auditoria incorretos podem impedir tais investigações e causar danos à credibilidade das evidências.

GERENCIAMENTO DE ESPAÇO

A VDM CORP disponibilizar a cada colaborador um espaço de armazenamento na rede de tamanho padrão inicial.

Para se realizar o aumento da capacidade de espaços, o colaborador deverá solicitar a Gerência Técnica, para realizar a análise da solicitação do tamanho do espaço utilizado.

Todos colaboradores deverão ter o acesso ao espaço através do usuário disponibilizado pela VDM CORP.

O espaço reservado a cada colaborador deverá ser utilizado somente para fins de projetos relacionados da empresa. Cada colaborador será responsável pelo conteúdo salvo no espaço reservado ao mesmo.

CONTROLES DE CRIPTOGRAFIA

O controle de criptografia será usado em conformidade com todas as leis, acordos e regulamentações relevantes.

Os seguintes itens são considerados para conformidade com leis, acordos e regulamentações relevantes:

A. Restrições à importação e/ou exportação de hardware e software de computador para execução de funções criptográficas;
B. Restrições à importação e/ou exportação
C. Restrições no uso de criptografia;
D. Métodos mandatários ou discricionários de acesso pelas autoridades dos países à informação cifrada por hardware ou software para fornecer confidencialidade ao conteúdo.

Todas as pastas e/ou partições relacionadas a área de produção dos softwares, área financeira, administrativa e comercial serão criptografados por segurança, em caso de perda, furto ou roubo do equipamento da empresa.

VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e eventuais processos criminais, se aplicáveis.

REFERÊNCIAS BIBLIOGRÁFICAS

Baseado na política de segurança da informação Senac São Paulo;

Baseado na política de segurança da informação da empresa Mutua;

Baseado na norma ABNT NBR ISO/IEC 17799