Ementa: Propõe os termos da Política de

Segurança da Faculdade Delta.

A Política de Segurança da Informação da Faculdade Delta tem seus termos propostos, conforme segue:

Art. 1 - As questões relativas à Segurança da Informação, bem como, a administração e

gestão da Segurança da Informação em Ambiente Computacional da Faculdade Delta ficarão única e exclusivamente a cargo da Área de Segurança da

Informação do departamento de tecnologia.

Art. 2 - A Área de Segurança da Informação da STI será a responsável pela edição de

Políticas, Normas e Procedimentos Institucionais que se façam necessárias para a garantida Segurança e mitigação de riscos ao ambiente de Tecnologia da Informação – TI da Faculdade Delta.

Art. 3 - A aprovação e promulgação de Normas e Procedimentos de Segurança da

Informação Institucionais ficarão a cargo do Comitê de Tecnologia da Informação, enquanto para Políticas ficarão a cargo do Gabinete Reitor da Faculdade Delta.

Art. 4 - Esta Política se aplica a todos os colaboradores da Faculdade Delta e seus órgãos, nos diversos níveis hierárquicos e vínculos – servidores,

estagiários, trainees, temporários, fornecedores, clientes, terceirizados, etc – que a

qualquer momento tenham necessidade de utilizarem os recursos de TI.

Art. 5 - Esta Política deverá obrigatoriamente sofrer revisões, no mínimo uma vez a cada ano-calendário, visando à garantia de manutenção da mesma atualizada, e condizente com as melhores práticas de Segurança, as novas ameaças, a evolução tecnológica da Faculdade Delta, o crescimento da Instituição e suas constantes mudanças.

Art. 6 - A Área de Segurança da STI, juntamente com os Órgãos de Recursos Humanos, Jurídico da Faculdade Delta e o Comitê de Tecnologia da Informação, deverá definir uma matriz de responsabilidades referente às aprovações e aos aprovadores no âmbito de TI, devendo,esse documento ser revisado no mínimo uma vez em cada ano-calendário. Essa matriz

deverá obrigatoriamente contemplar os variados tipos e eventos de liberações de acesso e os respectivos responsáveis pela aprovação dos mesmos. Os usuários responsáveis deverão ser comunicados e estarem cientes que além da aprovação, poderão ser diretamente ou possuem corresponsabilidade acerca de eventos de mal-uso, descumprimento de normas ou ainda, infrações legais originadas de autorizações oferecidas pelos mesmos.

Art. 7 - Os processos, políticas, normas e procedimentos de Gestão de Riscos em

Segurança da Informação deverão ser definidos pela Área de Segurança da Informação da

STI e revisados periodicamente, no mínimo uma vez a cada ano-calendário.

Art. 8 - A Área de Segurança da Informação da STI será responsável pela edição e

aplicação dos planos de Gerenciamento e Reposta a Incidentes, devendo os mesmos ser suportados por Política, Norma ou Procedimento específicos para tal, bem como, chancelados pelo Comitê de Tecnologia da Informação.

Capítulo I

Das Definições

Art. 9 - Para efeito dessa política considere-se:

I) **Ambiente Computacional:** é o conjunto de recursos computacionais separado para uma determinada função. Subdivido em:

I.I) **Produção:** ambiente que possui os dados reais do sistema, aquele que os usuários utilizam para as funções diárias e que cujas informações possuem valores legais e são aproveitadas pela instituição. Por possuir dados reais, é considerado ambiente extremamente crítico para a Segurança das Informações da Instituição e por isso, seu acesso deve ser limitado e somente liberado a quem realmente possui necessidade de utilizá-lo em tarefas do dia-a-dia e de alimentação de informações para o sistema.

I.II) **Homologação:** ambiente no qual são feitos os testes de um sistema e que um

grupo restrito de usuários tem acesso para validação de funções de um novo sistema ou de novas funções para um sistema pré-existente. Possui cópias desatualizadas dos dados de produção. Por possuir dados reais, mesmo que desatualizados, possui razoável criticidade quando ao comprometimento da Segurança das Informações Institucionais.

I.III) **Desenvolvimento:** é o ambiente no qual os desenvolvedores de sistema possuem acesso para criar um novo sistema ou novas funções para um sistema pré-existente.

Obrigatoriamente possui esquemas reais (tabelas, campos em tabelas) porém,

preenchidos com dados falsos. Não compromete a Segurança das Informações da

Instituição.

II) **Perfil de acesso:** conjunto de regras de computação que liberam apenas determinadas operações em um sistema. É o perfil de acesso que determina as permissões de um usuário, ou seja, o que ele pode ou não fazer em um sistema.

III) **Usuário Normativo:** usuário de área, ou seja, não é necessariamente um Analista de TI, que possui conhecimento profundo da área operacional e recebe conhecimento acerca dos perfis de usuário de um determinado sistema. É ele o responsável por aprovar a liberação de acesso de um determinado perfil de acesso a um determinado usuário. Ou seja, é ele o responsável por afirmar que as funções de um determinado usuário são compatíveis com o perfil a ser liberado para o mesmo.

IV) **Área Normativa:** área da Instituição que é responsável pelas informações contidas em um sistema. O usuário normativo deve obrigatoriamente pertencer à Área Normativa.

Art. 10 - Compõem os recursos computacionais da Faculdade Delta equipamentos integrantes de quaisquer ambientes computacionais supracitados, sejam estes de quaisquer tipos ou com quaisquer finalidades (computadores, notebooks, telefones, switches, hubs, impressoras, periféricos, etc.), independente de terem sido adquiridos pela instituição; uma vez integrantes de algum ambiente computacional, estão sujeitos a esta Política.

Capitulo II

Das Diretrizes Gerais A Segurança da Informação deve ser responsabilidade de todos, não apenas da área de TI. Desta forma, deve refletir em hábitos, posturas, responsabilidade e cuidados constantes no momento do uso, solicitação de aprovação de recursos, etc.

Art. 12 - A Superintendência de Tecnologia da Informação irá providenciar os recursos humanos e materiais necessários para implementação das diretrizes estabelecidas nesta Política, bem como orientar todos os usuários quanto as suas ações que serão tomadas, além de divulgar os preceitos de segurança da informação a serem observados por todos, inclusive, nas divisões, órgãos e campi da Faculdade Delta que possuem ambiente de TI distinto, com

maior ou menor integração com o restante da instituição;

Art. 13 - A utilização de informação e dos recursos computacionais deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

Art. 14 - A utilização de recursos (sistemas, correio eletrônico, espaço em disco,

equipamentos, etc.) disponibilizados pela instituição ou integrados ao ambiente desta (rede e afins), deve ser feita segundo os padrões e procedimentos definidos pela STI, visando manter a disponibilidade e o desempenho das aplicações.

Art. 15 - A conexão de equipamentos de terceiros na rede da instituição somente será permitida se não apresentarem risco ao ambiente corporativo e estiverem de acordo as políticas da instituição aplicáveis aos demais equipamentos, bem como, houver sido analisada e declarada adequada pela STI.

Art. 16 - As informações classificadas como confidencial e/ou reservada requerem alto grau de controle e proteção contra acessos não autorizados, como também, aquelas que necessitem de sigilo por força de lei ou contrato são candidatas naturais à obtenção dessa classificação. O direito de acesso a estas informações requer autorização expressa do Usuário Normativo e é regida por política específica de Classificação da Informação.

Art. 17 - A utilização indevida dos recursos computacionais pode provocar sanções a serem definidas pela STI e a Área de Segurança da Informação da STI, dentre elas a suspensão dos acessos, e deve ser notificada à Área de Segurança da Informação.

Art. 18 - Qualquer violação dessa política constitui base para uma medida disciplinar, inclusive o término do contrato empregatício, conforme Política Disciplinar, bem como, às sanções previstas por lei.

Capitulo III

Da Classificação das Informações A Classificação das Informações na UFF será regulamentada por política específica acompanhada de procedimentos específicos de manipulação, salvaguarda, transporte, criação e edição.

I) Toda informação criada no ambiente da Faculdade Delta não classificada explicitamente será considerada informação Reservada

Capítulo IV

Da gestão da Segurança das Informações e suas responsabilidades A

responsabilidade pela gestão da Segurança da Informação é atribuída aos agentes envolvidos no processo de criação, salvaguarda, transporte e destruição da informação, sendo assim caracterizados:

I) **Normativos:** responsáveis pela classificação da informação, pela definição de perfil do usuário e o tipo de acesso às informações;

II) **Usuários:** todos aqueles que utilizam os recursos de tecnologia da informação, sendo, portanto, responsáveis pelo conhecimento e aplicação dessa política;

III) **Custodiante**: responsável pela guarda da informação com segurança. Na Faculdade Delta e nos seus prédios anexos, esse agente é a Área de Segurança da Informação da STI, que terá a incumbência de implementar e controlar as autorizações de acesso à rede, correio/e-mail, internet, sistemas, servidores, etc.; monitorar o uso adequado dos recursos liberados, bem como, de implementar e operacionalizar os mecanismos de segurança da informação.

Art. 21 - Os usuários normativos de natureza específica serão designados pelos 1º nível de reporte das áreas usuárias.

Art. 22 - Os gestores das Unidades Organizacionais da Faculdade Delta são Usuários Normativos das informações pertencentes ao domínio de sua autoridade, e podem delegar as funções de concessão de direitos de acesso/homologação de alterações nos sistemas. Para tanto, devem formalizar estas delegações junto à Área de Segurança da Informação da STI.

Capitulo V

Da Segurança Física do Ambiente de TI

Art. 23 - Todos os equipamentos, incluindo suas movimentações, que compõem a estrutura do ambiente computacional da Faculdade Delta, tais como servidores, roteadores, switches, hubs, controladores, impressoras, meios óticos e magnéticos de backup, computadores, etc., devem ser devidamente autorizados e registrados pela Divisão de Atendimento Técnico da STI.

Art. 24 – A Faculdade Delta manterá dispositivos de proteção contra problemas de segurança física (condições ambientais adversas, desastres naturais, incêndios, etc.) e lógica (vírus, acesso não autorizado, invasões, etc.) compatíveis com os requisitos definidos nessa política.

Cabe à STI a definição de tais dispositivos de proteção, considerando características regionais, a criticidade das informações e os recursos tecnológicos envolvidos. Nenhum fluxo de informações poderá existir sem que passe pelas camadas de proteção lógica.

Art. 25 - Para os sistemas classificados como de missão crítica, será utilizado hardware que disponha de recursos de redundância de processador, disco, energia, etc., bem como, equipamentos de prevenção e combate a incêndios (SPCI), além de controle da corrente elétrica (rede estabilizada), temperatura e umidade e acesso físico e lógico restrito.

Capitulo VI

Da Segurança Lógica do Ambiente de TI

Art. 26 - Cabe à Área de Segurança da Informação da STI garantir que todos os ambientes lógicos (sistemas operacionais, SGDBs e sistemas de informação) tenham o seu acesso restrito por senhas, estando em conformidade com as diretrizes descritas nessa Política, salvo em situações nas quais existam restrições técnicas impeditivas que serão analisadas pela área de segurança.

Art. 27 - Todo programa ou transação desenvolvido ou adquirido para execução no

ambiente Faculdade Delta deve, obrigatoriamente, conter as verificações de autorização de execução em perfeita sintonia com o ambiente tecnológico em que será processado. Não haverá exceção à verificação de autorização para execução de qualquer programa ou transação.

A princípio, tudo que não for explicitamente permitido, está negado.

Art. 28 - Todo novo programa ou transação adquirido para execução no ambiente Faculdade Delta deverá ser submetido à análise da Área de Segurança da STI afim de verificar sua conformidade.

Art. 29 - Nenhuma senha pessoal será gravada no código-fonte de programas, tampouco em arquivos ou tabelas destinadas a outros fins, devendo o tratamento desse tipo de informação seguir norma específica da STI para desenvolvimento e/ou aquisição de sistemas, softwares e afins.

Art. 30 - O acesso – mesmo que de simples consulta – aos arquivos ou tabelas de senha não será permitido, em nenhuma circunstância, a nenhum colaborador. Tal restrição será provida por mecanismos de segurança lógica ou criptografia;

Art. 31 - Toda conta de acesso sem uso há mais de 60 dias até o limite de 180 dias poderá ser desabilitada pela Área de Segurança da STI, sem prévia autorização do proprietário ou da Gerência para isso, de modo a liberar recursos físicos e/ou licenças de softwares alocados.

A exceção dessa regra é para usuários com primeiro nível de reporte à Reitoria, que serão contatados antes do recurso ser desabilitado;

Art. 32 - É proibida a desinstalação, nas estações usuárias, de softwares ou hardwares, que são utilizadas para realizar controle físico e lógico dos recursos disponíveis. Caso isso ocorra por procedimento indevido, o fato será comunicado, imediatamente, ao Superior Imediato e à Divisão de Atendimento Técnico, que apurará as causas, corrigirá o problema e providenciará a reinstalação;

Art. 33 - Somente será permitido o uso de recursos homologados e autorizados pela Instituição, desde que sejam identificados individualmente, inventariados, com

documentação atualizada e atendendo a legislação pertinente em vigor. A utilização destes sem licenças correspondentes é crime, previsto na Lei 9.609, de 19 de Fevereiro de 1998. Portanto, qualquer usuário que exponha a Instituição a sansões jurídicas por utilização de softwares não homologados, independente de sua classificação (shareware, freeware, demo, etc.) sem respaldo das respectivas licenças, está sujeito às medidas disciplinares previstas, bem como, às sanções previstas por lei;

Art. 34 - A Homologação de recursos computacionais será de única e exclusiva

responsabilidade da STI, sendo regida por norma e procedimento específico de

Homologação de Software e Homologação de Hardware.

Art. 35 - Nenhum software, independente de suas condições comerciais, será instalado ou baixado para equipamentos Faculdade Delta pelo próprio usuário, cabendo esta tarefa exclusivamente aos usuários alocados nas gerências e divisões da STI, que tem essa atividade inclusa no seu papel funcional. A exceção a essa regra somente poderá ocorrer mediante aprovação expressa da área de Segurança da STI, respeitando-se as premissas do item 4 dessa política. Tais liberações terão sempre efeito pontual e nunca serão vistas

como permanentes e genéricas.

Art. 36 - A STI irá restringir as pessoas que poderão ser administradoras das respectivas estações de trabalho.

Art. 37 - No caso de contas de acesso standard e impossíveis de serem eliminadas ou alteradas, as senhas standard (que vem junto com o produto) serão, obrigatoriamente, modificadas imediatamente após a disponibilização do sistema e/ou ambiente, sem que haja solicitação específica sobre isso.

Art. 38 - É obrigatória e existência de planos de segurança e de infraestrutura para

implantação de sistemas de informação, sendo que não serão implementados se

trouxerem fragilidades que comprometam a segurança do ambiente Faculdade Delta.

Capitulo VII

Do uso e formação das senhas

Art. 39 - Uma senha segura possui ao menos oito caracteres, inclui uma combinação de letras, números e símbolos e é fácil de ser lembrada, mas difícil de ser “quebrada”. Para a formação das senhas, serão adotados os seguintes critérios:

I) Tamanho mínimo de 8 caracteres.

II) Nunca podem ser nulas ou estar em branco.

III) Nunca visíveis na tela onde são informadas para atualização ou login.

IV) Nunca podem começar com os 3 caracteres iniciais do ID.

V) Mínimo de 2 dígitos numéricos.

VI) Mínimo de 2 caracteres alfanuméricos.

VII) Impedir a repetição de um mesmo caractere 3 vezes seguidamente.

VIII) Vetar a reutilização de ultimas 5 senhas utilizadas.

IX) Serem bloqueadas após 5 tentativas consecutivas e mal sucedidas de acesso.

X) Passar por rotinas de crítica que impeçam a utilização de senhas “fracas” ou “facilmente quebráveis”

XI) Evitar palavras dicionarizadas.

Art. 40 - Todas as senhas expirarão independentemente da vontade dos usuários, no máximo, a cada 45 dias. Além disso, todas as senhas iniciais – definidas pela Área de Segurança da Informação da STI quando da liberação do acesso – serão expiradas e, ao primeiro acesso de cada usuário, forçada a sua troca.

Art. 41 - As senhas pessoais podem ser trocadas pelo próprio usuário, independentemente da sua data de expiração. Porém, deverão ser impossibilitadas de serem trocadas mais de 1 vez no mesmo dia.

Art. 42 - Nenhum colaborador poderá usar de sua ascendência hierárquica ou funcional sobre outrem para determinar ou obrigar que este compartilhe sua senha pessoal de acesso com quem quer que seja. O usuário que porventura receba esse tipo de solicitação deve comunicar o fato à Área de Segurança da Informação da STI.

Art. 43 - O compartilhamento de senhas, individuais é proibido para todos os níveis da instituição. Da mesma forma, abrir uma conexão autenticada para deixar que outra pessoa a utilize. Em hipótese alguma, um usuário poderá passar sua senha pessoal de acesso para outrem. Tal ação, uma vez detectada, terá classificação de gravidade em função do ambiente em que ocorreu e será devidamente reportada aos superiores hierárquicos dos usuários e ao DDRH.

Art. 44 - Qualquer tentativa de “quebrar” (tentar descobrir) a senha pessoal de acesso de outra pessoal, ou mesmo invadir ambientes ou sistemas sujo acesso lhe é negado, serão notificadas aos superiores hierárquicos, e poderá resultar em medidas disciplinares apropriadas, conforme disposto na **Política Disciplinar**.

Art. 45 - É dever de todos, zelar pelo sigilo de suas senhas de autenticação, bem como escolher senhas fortes dificultando ser descoberta facilmente por outra pessoa.

Capitulo VIII

Da Segurança de Acessos

Art. 46 - A conta de acesso e a **senha** de cada pessoa são únicas, individuais e

intransferíveis, sendo reconhecidas como equivalentes à sua assinatura e representem nível de delegação concedida para o desempenho de suas funções.

Art. 47 - Os acessos externos a recursos da instituição (acesso remoto de colaboradores. terceiros, fornecedores, clientes, e outros casos que vierem a surgir) somente serão concedidos mediante autorização prévia, segundo instruções detalhadas caso a caso e realizadas por intermédio de soluções técnicas institucionais.

Art. 48 - O acesso à internet é permitido por intermédio de sistema de segurança

institucionais. É proibido o acesso direto à internet por intermédio de provedores externos estando conectado à rede Faculdade Delta.

Art. 49 - Eventuais interligações entre redes (de forma física e/ou lógica) envolvendo processo de automação e/ou informação somente deverão ocorrer utilizando soluções corporativas definidas pelo STI, de forma a garantir a disponibilidade, a integridade e a confidencialidade dos ambientes.

Capitulo IX

Do Controle de Acesso A Área de Segurança da Informação da STI deve assegurar que nenhum colaborador ou prestador de serviço obtenha direitos de acesso incompatíveis com a sua função, ou seja, cada usuário terá uma única conta de acesso por aplicação.

Art. 51 - A Área de Segurança da Informação definirá e adotará um padrão de identificação de usuários que permitirá associar, de maneira única, cada direito de acesso à pessoa que o detém e concederá direitos de acesso compatíveis com as funções desempenhadas pelos usuários, através de perfis de acesso diferenciados. Tais perfis objetivam restringir os dados e operações disponíveis, e sua definição será realizada em conjunto com Usuários Normativos.

Art. 52 - No caso de fiscais de outros órgãos públicos, mesmo não existindo vínculo direto, as pessoas também poderão ser cadastradas nos sistemas de RH, associados a um colaborados responsável e também controlados por data de vigência lógica.

Capitulo X

Da Segregação de Ambientes e Funções

Art. 53 - A STI deve assegurar que todos os sistemas de informação da Instituição sejam aderentes as diretrizes a seguir:

I) Segregação de ambientes lógicos, de maneira que o ambiente de produção fique apartado dos demais.

II) Os ambientes que não sejam de produção – ou seja, de teste, de homologação, de desenvolvimento e outros – devem ser de acesso exclusivo dos usuários envolvidos com atividades de desenvolvimento e suporte a sistemas. Estes usuários, nos ambientes de produção, podem efetuar, no máximo, operações de consulta.

III) O acesso às bases de dados dos ambientes de produção será feito, unicamente, através dos sistemas de informação, estando completamente vetado qualquer tipo de acesso direto. Os casos extremos de necessidade de liberação serão aprovados pela Área de Segurança da STI em conjunto com o usuário com nível gerencial da área solicitante.

IV) Todo objeto, tais como programas, telas, funções, etc., que for transferido para o ambiente de produção, deverá ser originado do ambiente de desenvolvimento ou de homologação, mantendo nesses ambientes o arquivo fonte original.

V) Deve existir nos ambientes de produção, sempre que tecnologicamente possível, um controle automático das versões dos programas-fonte. Este controle possibilitará a recuperação de versões recentes (dentro dos 6 meses predecessores e das 6 ultimas

versões), assim como a identificação do responsável pela sua implantação. O acesso aos programas-fonte, principalmente de inclusão, exclusão e alteração nos seus códigos, será restrito, através de perfis de acesso específicos e registrado em trilhas de auditoria.

Capitulo XI

Do Plano de Contingência

Art. 54 - Para enfrentar situações de interrupção dos sistemas de informação, com

consequente paralisação das atividades da Faculdade Delta, a STI deverá manter um Plano de Contingência que permita operar os sistemas e recursos de forma que garanta um nível mínimo de operação.

Art. 55 - O Plano de Contingência deverá passar por revisões periódicas, no mínimo uma vez a cada ano-calendário.

Art. 56 - O Plano de Contingência deverá ser exercitado no mínimo 2 vezes ao ano.

Capitulo XII

Da Propriedade Intelectual

Art. 57 - Todos os sistemas, projetos e/ou configurações desenvolvidos para atender as necessidades e aos interesses da Instituição são de propriedade única e exclusiva da Faculdade Delta, e somente poderão ser cedidos, comercializados ou distribuídos mediante a aprovação do STI. Essa regra deve ser formalizada em todos os contratos com fornecedores e prestadores de serviço ou atividades de desenvolvimento realizadas pela equipe de desenvolvimento Faculdade Delta.

Art. 58 - A documentação dos sistemas de informação e projetos desenvolvidos, devem ser disponibilizadas em meio ótico ou magnético, contendo:

I) Códigos fonte dos objetos (programas, telas, transações, etc.) desenvolvidos;

II) Manual do Usuário e/ou Help *On-Line*, desde que apresente explicações sobre

funcionalidades e não apenas preenchimento de campos;

III) Diagrama de Contexto e Especificação Funcional;

IV) Diagrama de Casos de Uso e Casos de Uso;

V) Dicionário de Dados (DD);

VI) Diagrama de Fluxo de Dados (DFD) ou Modelo de Transição de Dados (em projetos de automação, é indispensável os dois);

VII) Modelo de Entidade-Relacionamento (MER) ou Modelo de Objetos;

VIII) Diagrama de Classes

IX) E quaisquer outros artefatos de projeto e desenvolvimento gerados pela metodologia de projeto e desenvolvimento empregada no projeto.

Art. 59 - No caso dos sistemas de informação e automação desenvolvidos, implementados ou integrados por terceiros, a STI exigirá em contrato a disponibilização e atualização da documentação pertinente. Os pagamentos a serem efetuados ao fornecedor estarão condicionados à entrega de tal documentação, que poderá ser proporcional aos produtos entregues em cada fase do projeto.

Capitulo XIII

Da Auditoria e das Trilhas de Auditoria

Art. 60 - A Auditoria poderá ter acesso a qualquer informação que esteja armazenada em ambiente lógico (Sistemas Operacionais, SGDBs e Sistemas de Informação). Havendo evidência de qualquer atividade que possa comprometer a segurança do ambiente de TI, podendo a Auditoria auditar e monitorar as atividades de qualquer usuário, além de inspecionar seus arquivos e registros de acesso, sempre que julgar e comprovar necessidade.

Art. 61 - A STI deve providenciar os recursos tecnológicos para que as trilhas de auditoria sempre existam e fiquem disponíveis para uso, bem como definir o tempo de retenção e as informações que deverão sistematicamente e automaticamente compor os arquivos conhecidos como trilhas de auditoria.

Art. 62 - As trilhas de auditoria de um determinado sistema devem ser centralizadas evitando a sua dispersão em vários arquivos e ser de fácil acesso a quem de direito.

Art. 63 - As trilhas de auditoria devem registrar automaticamente todas as operações críticas efetuadas, e serão constituídas de, pelo menos, os seguintes campos: identificador do usuário (nominal, não podendo ser somente IP ou MAC Address), data da operação, horário da operação, operação realizada, dados antes da operação e dados após a operação.

Art. 64 - Sempre que surgir um novo ambiente lógico na instituição, a STI tomará a

iniciativa de reunir-se com os Usuários Normativos correspondentes para deliberar sobrea criação das trilhas de auditoria.

Art. 65 - As trilhas de auditoria devem estar disponíveis para consulta por um prazo

mínimo de 1 (um) ano, além de protegias contra inclusão, exclusão ou alteração de dados.

As únicas inclusões de dados admissíveis serão as oriundas das rotinas automáticas de registro.

Capitulo IVX

Referências Normativas

Art. 66 - Este documento se ampara e referencia pelos instrumentos normativos

apresentados conforme segue:

I) Decreto 3.505 de 13 de julho de 2000 – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Publica.

II) Decreto 4.553 de 27 de dezembro de 2002 – Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Publica Federal, e dá outras providências.

III) Lei 9.609 de 19 de fevereiro de 1998 – Dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país e dá providências.

IV) Instrução Normativa GSI/PR nº 01 de 01 de julho de 2008 – Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

V) Norma Complementar nº 03 de junho de 2009 à Instrução Normativa GSI/PR nº01 – Recomenda diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

VI) e-Ping – Padrões de Interoperabilidade do Governo Eletrônico, de 16 de dezembro de 2008.

VII) Portaria SLTI/MP nº05 de 14 de julho de 2005 – Institucionaliza os Padrões de

Interoperabilidade do Governo Eletrônico – e-Ping.

VIII) ABNT NBR ISO/IEC 27001:2006 – Sistema de Gestão de Segurança da

Informação.

IX) ABNT NBR ISO/IEC 27002:2005 – Código de Praticas para Gestão de Segurança da Informação.