Universidade Federal do Espírito Santo
Núcleo de Processamento de Dados

Documento POSIC/2011

Política de Segurança da Informação e Comunicações

Vitória, 5 de Dezembro de 2011

A Comissão de Elaboração desta Política de Segurança da Informação e Comunicações foi designada pela Portarias nº 602 de 18 de Abril de 2011, nº 1.508 de 27 de Setembro de 2011 e nº 1.775 de 24 de Setembro de 2011. Os membros da Comissão são:

- Hans-Jorg Andreas Schneebeli
- Carlos Alberto Ceotto
- Danilo José Silva Oliveira Mendes
- Aline Souza Gaigher Ceravolo
- Roney Pignaton da Silva
- Paulo Alexandre Lobato
- Symone de Deus Miranda Gonçalves

Esta Política de Segurança de Informação e Comunicações (POSIC) foi aprovada pelo Comitê Gestor de Tecnologia de Informação e Comunicações (CGTIC) em 05/12/2011.

Índice

Glossário

ABNT – Associação Brasileira de Normas Técnicas

APF – Administração Pública Federal

CGTIC – Comitê Gestor de Tecnologia de Informação e Comunicações

CEPE – Conselho de Ensino, Pesquisa e Extensão

CSIC – Comitê de Segurança da Informação e Comunicações

CONARQ – Conselho Nacional de Arquivos

CUN – Conselho Universitário

DICA – Disponibilidade, Integridade, Confidencialidade e Autenticidade

DOU – Diário Oficial da União

DSIC – Departamento de Segurança da Informação e Comunicações

ETIR – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

GSIPR – Gabinete da Segurança Institucional de Presidência da República

HTTPS – HyperText Transfer Protocol Secure

HUCAM – Hospital Universitário Cassiano Antônio de Moraes

IDS – *Intrusion Detection System*

IPS – *Intrusion Prevention System*

IN – Instrução Normativa

MPOG – Ministério do Planejamento, Organização e Gestão

NC – Normas Complementares

NPD – Núcleo de Processamento de Dados

POSIC – Política de Segurança da Informação e Comunicação

SEGD – Sistema Eletrônico de Gerenciamento de Documentos

SIC – Segurança de Informação e Comunicação

SLTI – Secretaria de Logística e Tecnologia da Informação

TIC – Tecnologia da Informação e Comunicação

VLAN – *Virtual Local Area Network*

WiFi – Tecnologia de comunicação sem fio baseada nas normas IEEE-802.11 a/b/g/n

1 Introdução

É necessária a criação de um **processo de gestão da segurança da informação e comunicações** na Universidade, para viabilizar a implementação efetiva de controles de segurança. Para tanto, este processo deve considerar o incentivo à **definição de políticas de segurança da informação e comunicações**. As referidas políticas devem também compreender o gerenciamento de riscos, baseado em análise quantitativa e qualitativa, análises de custo versus benefício e programas de conscientização da comunidade universitária.

A gestão da segurança da informação inicia-se com a definição de **políticas, procedimentos, guias e padrões**.

As políticas estão colocadas no mais alto nível de documentação da segurança da informação e comunicações. Nos níveis seguintes, encontram-se os *procedimentos, guias e padrões*. Estes níveis são *complementares*, não significando que as políticas sejam mais importantes que os demais. O fato é que as políticas devem ser definidas em primeiro lugar por razões estratégicas, enquanto os demais níveis/documentos seguem as políticas, de forma consequente, como elementos táticos e operacionais. Portanto, as políticas, como documento base, devem conter o comprometimento da alta administração, explicitando de forma clara e abrangente, a importância da segurança da informação e comunicações, bem como dos recursos computacionais, para a missão institucional. Constitui assim, uma declaração que fundamenta a segurança da informação e comunicações na totalidade da instituição. Deve-se, ainda, conter as necessárias autorizações para a definição dos *procedimentos, guias e padrões* nos níveis subsequentes.

Distinguem-se as políticas de alertas e as políticas informativas. As políticas de alerta não são mandatórias em si mesmas, mas são fortemente incentivadas, bem como melhor explicitadas nos níveis subsequentes que, normalmente, incluirão as consequências da não conformidade com as mesmas. As políticas informativas são as que simplesmente informam aos usuários sobre um determinado ambiente. Não implicam necessariamente em requisitos específicos e seu público-alvo pode ser somente determinado ou, inclusive, parceiros externos ou terceiros. Como tem caráter genérico, podem ser distribuídas para parceiros externos ou terceiros que acessam as redes da instituição, sem que isso acarrete o comprometimento da informação interna.

Os regulamentos de segurança são aqueles que a instituição deve implementar em conformidade com legislação em vigor, garantindo aderência à padrões e procedimentos básicos de setores específicos.

Os padrões especificam o uso uniforme de determinadas tecnologias. Normalmente são mandatórios e implementados através de toda a instituição, objetivando maiores benefícios gerais.

Os fundamentos ou princípios são semelhantes aos padrões, com pequena diferença. Uma vez que um conjunto consistente de fundamentos seja definido, a arquitetura de segurança de uma instituição pode ser planejada e os padrões podem ser definidos. Os fundamentos devem levar em conta as diferenças entre as plataformas existentes, para garantir que a segurança seja implementada uniformemente em toda a Instituição. Quando adotados, são mandatórios.

Os guias consideram a natureza distinta de cada sistema de informação e são similares aos padrões, embora pouco mais flexíveis. Eles se referem, normalmente, a metodologias para os sistemas de segurança, contendo apenas ações recomendadas e não mandatórias. Podem e devem ser usados para especificar a maneira pela qual os padrões devem ser desenvolvidos, como quando indicam a conformidade com determinados princípios da segurança da informação.

Os procedimentos contêm os passos detalhados que devem ser seguidos para a execução de tarefas específicas. São ações detalhadas que devem ser seguidas. São considerados como inseridos no mais baixo nível em uma cadeia de políticas. Assim, seu propósito é fornecer os passos detalhados para a implementação das políticas, padrões e guias. Também podem ser chamados de boas práticas.

As responsabilidades devem estar relacionadas com o perfil de cada um que esteja envolvido no processo. Estes são exemplos:

- Gerentes do mais alto nível – Estão envolvidos com toda a responsabilidade da segurança da informação e comunicações. Podem delegar a função de segurança, mas são vistos como o principal foco quando são considerados os eventos relacionados com a segurança;
- Profissionais de segurança dos sistemas de informação – Recebem da gerência do mais alto nível a responsabilidade pela implementação e manutenção da segurança. Estão sob sua responsabilidade o projeto, a implementação, o gerenciamento e a revisão das políticas, padrões, guias e procedimentos;
- Possuidores de dados – São responsáveis pela classificação da informação. Podem também ser responsabilizados pela exatidão e integridade das informações;
- Usuários – Devem aderir às determinações definidas pelos profissionais de segurança da informação;
- Auditores de sistemas de informação – São responsáveis pelo fornecimento de relatórios para a gerência superior sobre a eficácia dos controles de segurança, consolidados através de auditorias independentes e periódicas. Também analisam se as políticas, padrões, guias e procedimentos são eficazes e estão em conformidade legal e com os objetivos de segurança definidos para a instituição.

A Segurança da Informação e Comunicações visa a preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade. A segurança compreende, assim, a proteção das informações em relação aos diversos tipos de ameaças para:

- garantir a continuidade do negócio
- minimizar o risco ao negócio
- maximizar o retorno sobre os investimentos e as oportunidades de negócio

Assim estabelecido, este documento descreve as Políticas de Segurança da Informação e Comunicações no âmbito da UFES, estando em vigor após sua aprovação pela alta administração. Ele deve ser publicado e comunicado para todos os servidores da Instituição e para as partes externas relevantes. Este documento deve sofrer revisões periódicas, devendo manter-se alinhado com a legislação pertinente, com as normas e padronizações brasileiras e com os objetivos do negócio.

As garantias que devem ser conferidas às informações, aos sistemas e aos ativos (qualquer coisa que tenha valor para a instituição) são:

- Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.
- Integridade: propriedade de salvaguarda da exatidão e completeza de ativos. A informação não pode ser alterada ou destruída sem a autorização adequada.
- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

- Autenticidade: propriedade que assegura que a informação é realmente da fonte que se declara ser.
- Não repúdio: propriedade que assegura que nem o o emissor nem o receptor de uma informação possam negar o fato, a autoria, a responsabilização.

Quanto à disponibilidade, deve-se garantir o acesso aos usuários autorizados sempre que necessário. A ausência dessa garantia pode gerar situações de negação de serviço (DoS), prejuízo em situações de urgência e danos à imagem da instituição.

Quanto a integridade deve-se garantir: a) a alteração de dados e informações apenas por usuários devidamente autorizados; b) o armazenamento, processamento e transmissão dos dados e informações de forma a preservar a exatidão e completeza dos registros. A ausência dessas garantias pode gerar perda ou falsificação de dados/informações.

Quanto à confidencialidade, deve-se garantir a) que o acesso aos dados e informações fiquem restritos às entidades devidamente autorizadas; b) a proteção em todas as fases: armazenamento, transmissão e processamento. A ausência dessas garantias pode resultar na quebra do sigilo.

Quanto à autenticidade, esta implica na certeza de que os dados/informações provêm das fontes anunciadas. Sobre o não-repúdio ou irretratabilidade, estes implicam na impossibilidade de negar a autoria, a responsabilização. A ausência dessa garantia pode resultar no uso de informações falsas.

Levando em conta a grande quantidade e variedade das ameaças à segurança da informação e comunicações, evidencia-se, entre outras, a necessidade de: normas específicas para a segurança física de instalações; de acesso de colaboradores, usuários e visitantes; de criação e manutenção de contas e senhas; de instalação e configuração de aplicações; de uso de redes, Internet, correio eletrônico e relativas a privacidade, etc. Todas estas necessidades deverão ser englobadas em uma política de segurança da informação e comunicações, cujas diretrizes são estabelecidas por este documento.

Notadamente, entre outras atividades institucionais, sendo a UFES uma instituição educacional pública de ensino superior, informações pessoais relativas a discentes, docentes e servidores técnico-administrativos devem ser armazenadas e processadas de modo adequado e seguro. Também, como a UFES é uma unidade de registro de diplomas de curso superior no Estado do Espírito Santo, informações de diplomação em cursos superiores ou em cursos de pós-graduação, devem ser processadas e armazenadas de modo adequado e seguro. Além disso, por haver um Hospital Universitário no âmbito da Instituição, devem ser consideradas as normas específicas para tanto e as informações relativas a pacientes, médicos, etc. devem ser processadas de modo adequado e seguro.

Observando o acima estabelecido, o Artigo 2 do Decreto 3505 de 13 de Junho de 2000, define:

> *Segurança da Informação é proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.*

Ainda, de acordo com o Decreto 3.505/2000, devem ser objetivos de uma Política de Segurança de Informação:

I. dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;

II. eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

III. promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;

IV. estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;

V. promover as ações necessárias à implementação e manutenção da segurança da informação;

VI. promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;

VII. promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação; e

VIII. assegurar a interoperabilidade entre os sistemas de segurança da informação.

Este documento trata da segurança da informação e comunicações de forma ampla, incluindo todas as formas de armazenamento, eletrônicas ou não. Devido a crescente sinergia entre as áreas, estão incluídos os aspectos relacionados a Tecnologia de Comunicações. Este documento deve servir de base para resoluções acadêmicas e administrativas que implementem as politicas nele contidas, inclusive as regras de uso de **Recursos de Tecnologia de Informação e Comunicações (RTIC)** e as **Normas Complementares.**

Em síntese, este documento institui diretrizes e princípios de Segurança da Informação e Comunicações (**POSIC**) no âmbito da Universidade Federal do Espírito Santo, com o propósito de limitar a exposição ao risco a níveis aceitáveis e garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade (**DICA**) das informações que suportam os objetivos estratégicos desta Universidade. Esta **POSIC** e suas Normas Complementares aplicam-se a todas as unidades e entidades vinculadas à Universidade Federal do Espírito Santo, bem como aos seus servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem de alguma forma tenha acesso aos ativos da organização.

2 Conceitos e Definições

Ativo: tudo aquilo que possui valor para o órgão ou entidade da Administração Pública Federal.

Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso [NC04/IN01/DSIC/GSIPR, 2009, p. 2].

Continuidade de Negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

Dados corporativos da UFES incluem, mas não estão restritos às informações sobre:

a) recursos humanos;

b) recursos financeiros;

c) recursos materiais;

c) equipamentos de qualquer natureza;

d) alunos;

e) cursos e disciplinas;

f) políticas, procedimentos e manuais;

g) páginas Web.

Recurso de Tecnologia da Informação e Comunicação (TIC): todos os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pelos setores administrativos e acadêmicos da UFES, tais como:

a) equipamentos de informática de qualquer espécie;

b) impressoras;

c) equipamentos de redes e de telecomunicações de qualquer espécie;

d) laboratórios de informática de qualquer espécie;

e) recursos de informação que incluem todas as informações eletrônicas, serviço de correio eletrônico, mensagens eletrônicas, dados corporativos, documentos, programas ou software que são armazenados, executados ou transmitidos através da infraestrutura computacional da UFES, redes ou outros sistemas de informação.

Informação: conjunto de dados corporativos da UFES que pode existir e ser manipulado de diversas formas seja por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados ou em meio impresso, verbalmente, em mídias de áudio e de vídeo, etc.

Informação Estratégica: toda a informação corporativa relativa à administração, planejamento, estrutura, gestão, relações internas e externas, novos produtos e tecnologias, serviços e contratos.

Segurança da informação (SI): Prioritariamente: preservação da confidencialidade, da integridade e da disponibilidade da informação. Sinteticamente, refere-se à proteção contra o uso ou acesso não autorizado à informação, bem como à proteção contra a negação do serviço a usuários autorizados, ao mesmo tempo em que a confidencialidade, integridade e a disponibilidade da informação são preservadas. Constitui-se, então, de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações [IN01/DSIC/GSIPR, 2008, p. 2];.

Segurança de Operações e Comunicações: responsável pela manutenção do funcionamento de serviços, sistemas e da infraestrutura de suporte dos mesmos.

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade [NC07/IN01/DSIC/GSIPR, 2010, p. 2].

Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso [NC07/DSIC/GSIPR, 2010, p. 3].

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade [IN01/DSIC/GSIPR, 2008, p. 2].

Confidencialidade: Garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas, ou seja: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado [IN01/DSIC/GSIPR, 2008, p. 2].

Integridade: Salvaguarda de exatidão e completude da informação e dos métodos de processamento, ou seja: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental [IN01/DSIC/GSIPR, 2008, p. 2];

Disponibilidade: Garantia de que usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessário, ou seja: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade [IN01/DSIC/GSIPR, 2008, p. 2];.

Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Evento: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação e comunicações ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação e comunicações [ISO/IEC TR 18044:2004].

Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

Riscos de Segurança da Informação e Comunicações: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização [NC04/IN01/DSIC/GSIPR, 2009, p.3].

Incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores [NC05/IN01/DSIC/GSIPR, 2009, p. 3].

Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação NC04/IN01/DSIC/GSIPR, 2009, p.3]

Capacitação: a aquisição de conhecimentos, capacidades, atitudes e formas de comportamento exigido para o exercício das funções;

Capacitação em SIC: fornecer conhecimentos em Segurança da Informação e Comunicações (**SIC**) com aplicação nas rotinas pessoais e profissionais, de forma a também multiplicar os conhecimentos sobre o tema, aplicando os conceitos e procedimentos na Organização, inclusive como gestor de SIC, quando for o caso. [DSIC/GSIPR]

Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pelo Conselho Universitário da UFES, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações [NC03/IN01/DSIC/GSIPR, 2009, p. 2].

Normas de Segurança da Informação (Normas): estabelecem obrigações e procedimentos definidos de acordo com a **POSIC**, a serem seguidos em diversas situações em que a informação é tratada;

Usuário: é qualquer pessoa, física ou jurídica, com vínculo oficial com a UFES ou em condição autorizada que utiliza informação de propriedade da UFES, em qualquer uma de suas formas, ou algum Recurso de TIC da UFES. São servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade [NC07/DSIC/GSIPR, 2010, p. 3].

Custodiante: responsável por armazenar e preservar as informações que não lhe pertencem, mas que estão sob sua custódia.

Terceiro: pessoas ou entidades envolvidas com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso, mas que não são integrantes do órgão ou entidade da APF [NC07/DSIC/GSIPR, 2010, p. 3].

Proprietário da Informação: pessoa ou setor que produz a informação.

Gestão de Incidentes: Conjunto de processos para a identificação, monitoração e comunicação e tratamento devido dos incidentes de segurança da informação, em tempo hábil, de forma a garantir a continuidade das atividades e a não intervenção no alcance dos objetivos estratégicos da Universidade.

Comitê de Segurança da Informação e Comunicações (CSIC): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações. [NC03/IN01/DSIC/GSIPR].

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

Administrador de Sistemas e Rede de um Órgão da UFES é pessoa designada formalmente pelo Dirigente deste Órgão e tem como atribuição principal o gerenciamento da rede local, bem como dos recursos de TIC do Órgão a ela conectados, direta ou indiretamente.

Gestor de Segurança da Informação e Comunicações: é responsável pelas ações de segurança da informação

e comunicações no âmbito do órgão ou entidade da APF [IN01/DSIC/GSIPR, 2008, p. 2].

Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicações [IN01/DSIC/GSIPR, 2008, p. 2];

Gestão de Riscos de Segurança da Informação e Comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos [NC04/IN01/DSIC/GSIPR, 2009, p.2].

Gestão de Continuidade do Negócio: A interrupção das atividades deste Ministério leva à suspensão de serviços críticos prestados ao cidadão e poderá resultar em grave dano à imagem da organização. Portanto, deverão ser instituídos normas e procedimentos que estabeleçam a Gestão de Continuidade do Negócio para minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços da Universidade, além de recuperar perdas de ativos de informação a um nível estabelecido, por intermédio de ações de prevenção, resposta e recuperação.

3 Referências Legais e Normativas

Constituição de República Federativa do Brasil. 1988.

Lei nº 8.112 de 11 de Dezembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

Lei nº 8.159 de 8 de Janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.

Lei nº 9.609 de 19 de Fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

Lei nº 9.610 de 19 de Fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.

Lei nº 9.507 de 12 de Novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data.

Lei no 9.609 de 19 de Fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

Lei no 9.610, de 19 de Fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.

Lei nº 10.406 de 10 de Janeiro de 2002. Institui o Código Civil.

Decreto nº 1.048 de 21 de janeiro de 1994. Dispõe sobre o Sistema de Administração dos Recursos de Informação e Informática, da Administração Pública Federal, e dá outras providências.

Decreto nº 1.171, de 22 de Junho de 1994. Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.

Decreto nº 3.505 de 13 de Junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

Decreto nº 4.073 de 3 de Janeiro de 2002. Regulamenta a Lei nº 8.159, de 8 de Janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.

Decreto não numerado de 18 de outubro de 2000. Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências.

Decreto nº 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 Pública Federal, e dá outras providências

Decreto nº 5.301 de 9 de Dezembro de 2004. Regulamenta o disposto na Medida Provisória nº **228, de 9 de dezembro de 2004, que dispõe sobre a ressalva prevista na parte final do disposto no Inciso XXXIII do Art. 5º** da Constituição, e dá outras providências.

ABNT ISO GUIA 73:2009. *Risk management -- Vocabulary*

NBR ISO/IEC 27000:2009. *Information Technology -- Security Techniques -- Information Security Management Systems - Overview and Vocabulary*.

NBR ISO/IEC 27001:2006. Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.

NBR ISO/IEC 27002:2005. Tecnologia da informação - Técnicas de segurança – Código de Prática para a Gestão de Segurança da Informação.

NBR ISO/IEC 27003:2010. *Information technology - Security Techniques -- Information Security Management System Implementation Guidance*.

NBR ISO/IEC 27004:2010. Tecnologia da informação - Técnicas de segurança – Medição.

NBR ISO/IEC 27005:2008. Tecnologia da informação - Técnicas de segurança – Gestão de riscos de segurança da informação.

NBR ISO/IEC 27006:2007. *Information technology - Security Techniques -- Requirements for Bodies Providing Audit and Certification of Information Security Management Systems*.

NBR ISO/IEC 27011:2009. Tecnologia da informação - Técnicas de segurança - Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002.

ISO/IEC 31000:2009. *Risk management — Principles and guidelines*

ISO/IEC 31010:2009. *Risk management -- Risk assessment techniques*

Instrução Normativa nº 04 de 19 de Maio de 2008 da Secretaria de Logística e Tecnologia da Informação/MPOG. Dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional.

Instrução Normativa MP/SLTI nº 04, de 12 de Novembro de 2010 da Secretaria de Logística e Tecnologia da Informação/MPOG. Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.

e-PING – Padrões de Interoperabilidade de Governo Eletrônico. Documento de Referência. Versão 2011, de 3 de dezembro de 2010.

e-MAG – Modelo de Acessibilidade de Governo Eletrônico. Secretaria de Logística e Tecnologia da Informação. Versão 3.0. Agosto de 2011.

E-ARQ Brasil – Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. Conselho Nacional de Arquivos. Versão 1. Dezembro de 2006.

Norma Complementar nº 01/IN01/DSIC/GSIPR. Atividade de Normatização. Publicada no DOU nº 200, de 15 de Outubro de 2008 - Seção 1.

Norma Complementar nº 02/IN01/DSIC/GSIPR. Metodologia de Gestão de Segurança da Informação e Comunicações. Publicada no DOU nº 199, de 14 de Outubro de 2008 - Seção 1.

Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Publicada no DOU nº 125, de 3 de Julho de 2009 - Seção 1.

Norma Complementar nº 04/IN01/DSIC/GSIPR. Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. Publicada no DOU nº 156, de 17 de Agosto de 2009 - Seção 1.

Norma Complementar nº 05/IN01/DSIC/GSIPR. Disciplina a criação de Equipes de Tratamentos e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 156, de 17 de Agosto de 2009 - Seção 1.

Norma Complementar nº 06/IN01/DSIC/GSIPR. Estabelecem Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Publicada no DOU nº 223 de 23 Novembro de 2009 - Seção 1.

Norma Complementar nº 07/IN01/DSIC/GSIPR. Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Publicada no DOU nº 86, de 7 de Maio de 2010 - Seção 1.

Norma Complementar nº 08/IN01/DSIC/GSIPR. Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. Publicada no DOU nº 162, de 24 de Agosto de 2010 - Seção 1.

Norma Complementar nº 09/IN01/DSIC/GSIPR. Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta. Publicada no DOU nº 222, de 22 de Novembro de 2010 - Seção 1.

Resolução nº 25 do Conselho Nacional de Arquivos da Casa Civil da Presidência da Republica de 27 de Abril de 2007. Dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR.

Resolução nº 14 do Conselho Nacional de Arquivos da Casa Civil da Presidência da Republica de 24 de Outubro de 2001. Aprovam a versão revisada e ampliada da Resolução nº 4, **de 28 de março de 1996, que dispõe sobre o Código de Classificação de Documentos de Arquivo para a Administração Pública: Atividades-Meio, a ser adotado como modelo para os arquivos correntes dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR), e os prazos de guarda e a destinação de documentos estabelecidos na Tabela Básica de Temporalidade e Destinação de Documentos de Arquivo Relativos as Atividades-Meio da Administração Pública.**

Classificação, Temporalidade e Destinação de Documentos de Arquivo relativos às Atividades-meio da Administração Pública. **Conarq.** 2001.

Portaria nº 3 de 7 de Maio de 2007. Institucionaliza o Modelo de Acessibilidade do Governo Eletrônico – e-MAG – no âmbito do Sistema de Administração dos Recursos de Informação e Informática – SISP.

CAIXAS POSTAIS INDIVIDUAIS-FUNCIONAIS NA REDE GOVERNO. Regra de Formação de Nomes para a composição dos endereços eletrônicos (e-mail), com base na padronização aprovada pela *Worldwide Electronic Messaging Association-WEMA*.

Rede Ipê: Política de Uso . Comitê Gestor da RNP (Rede Nacional de Pesquisa. Documento doc0108. Outubro de 2007.

Segurança de informação no TCU: política corporativa comentada. 2008.

Boas práticas em Segurança da Informação. 2ª edição. TCU. 2007.

4 Princípios

Respeitando os princípios da publicidade estabelecidos na Constituição Federal, determinadas informações cuja guarda está a cargo da UFES devem ter circulação restrita (Art. 37 da Constituição Federal). Entre elas constam: informações pessoais sobre discentes, docentes, servidores técnico-administrativos e, no caso do Hospital Universitário (HUCAM), pacientes. Também existem informações cuja divulgação pode acarretar prejuízos a União como, por exemplo, entre outras, o preço esperado em licitações, questões de provas e exames, etc.

As diretrizes de Segurança da Informação e Comunicações (**SIC**) devem considerar, prioritariamente, os objetivos estratégicos, os requisitos legais, a estrutura e finalidade da Universidade Federal do Espírito Santo.

A segurança da informação e comunicações deve ser entendida como uma responsabilidade coletiva.

Sinteticamente, portanto, o conjunto de documentos que compõe esta **POSIC** guiar-se-á pelos seguintes princípios gerais:

1. **Menor privilégio:** Usuários e sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.
2. **Segregação de função:** Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos.
3. **Auditabilidade:** Todos os eventos significantes de sistemas e processos devem ser rastreáveis até o evento inicial.
4. **Mínima dependência de segredos:** Os controles deverão ser efetivos ainda que a ameaça saiba de suas existências e como eles funcionam.
5. **Controles automáticos:** Sempre que possível, controles de segurança automáticos deverão ser utilizados.
6. **Resiliência:** Os sistemas e processos devem ser projetados para que possam resistir ou se recuperarem dos efeitos de um desastre.
7. **Defesa em profundidade:** Controles devem ser desenhados em camadas de tal forma que quando uma camada de controle falhar, haja um tipo diferente de controle em outra camada para prevenir a brecha de segurança.
8. **Exceção aprovada:** Exceções à POSIC deverão sempre ter aprovação superior.
9. **Substituição da segurança em situações de emergência:** Controles somente devem ser desconsiderados de formas predeterminadas e seguras. Devem sempre existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência.
10. Esta **POSIC** deve estar também em **conformidade** com os princípios constitucionais e administrativos que regem a Administração Pública Federal, bem como com os demais dispositivos legais aplicáveis.

Para seu funcionamento, a UFES necessita receber, armazenar, processar e transmitir informações e comunicações. Estas, normalmente, estarão armazenadas em forma de documentos, em órgãos acadêmicos como secretarias de departamentos, colegiados de curso, enfermarias, laboratórios de pesquisa, órgãos administrativos, órgãos técnicos, etc. Elas também poderão estar armazenadas em meio eletrônico (magnético ou não), em computadores de órgãos da UFES ou nos servidores localizados no Núcleo de Processamento de Dados (NPD).

Deve ser objetivo da UFES ter um Sistema Eletrônico de Gerenciamento de Documentos (**SEGD**) e um sistema redundante de armazenamento que mantém cópias destas informações, replicadas em mais de um local. Assim, em caso de sinistro, a probabilidade de perda de informação é reduzida.

As Medidas de Segurança de Informação devem compreender, entre outros:

- Controle de Acesso
- Segurança de Materiais e Instalações
- Normatização dos Processos de Criação e Trânsito de Documentos
- Armazenamento da Informação
- Uso de Recursos de TIC
- Descarte de Meios de Suporte da Informação
- Acesso a Informação por Colaboradores Externos

Devido à natureza da universidade, a UFES **não implementará nenhum sistema de censura, devendo, por principio,** haver um livre fluxo de informação e intercambio de ideias dentro da comunidade universitária e com a comunidade externa, respeitando-se os preceitos éticos e a legislação vigente.

Portanto, os usuários são responsáveis pelas informações que distribuírem ou acessarem. Por haver a possibilidade de uso destes recursos de informação e comunicação para atos ilícitos, a UFES deverá implementar um sistema de controles que permitam identificar o(s) responsável(eis) por eventuais ilicitudes no âmbito da instituição. Para isto, o acesso pleno à Rede UFES deverá ser feito através da utilização de controles de acesso que identifiquem o usuário e o equipamento utilizado e a utilização de mecanismos que permitam o rastreamento das atividades.

Em caso de detecção de anormalidades no uso de algum serviço, o usuário e/ou o computador correspondentes terão o acesso bloqueado. O usuário deverá contatar o NPD para possibilitar a restauração do acesso de uma forma segura tanto para o usuário como para a UFES.

Ainda em relação ao TIC, devem ser estabelecidas políticas de uso que estejam em conformidades com as diretrizes estabelecidas por este documento

5 Diretrizes Gerais

5.1 Legislação existente

Práticas ilícitas já contempladas nas referencias legais e normativas usadas como base para o estabelecimento das políticas de segurança objeto desse documentos, bem como no Código Penal, no Código Civil, no Estatuto do Servidor Publico, no Código de Ética do Servidor Publico, não são objeto de aprofundamento neste Documento. Apenas a título de exemplo e de maneira não exaustiva estão listadas abaixo alguns atos considerados ilícitos na legislação federal:

No Código Penal estão listados os seguintes atos ilícitos:

- Divulgar sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública. (Art. 153, § 1º)
- Venda ou comercialização/doação de banco de dados – Revelar alguém, sem justa causa, segredo, de quem tem ciência em razão de função, ofício ou profissão, e cuja revelação possa produzir dano a outrem. (Art. 154).
- Utilizar usuário e senha de outra pessoa que não seja a própria (Art. 299). Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena de sexta parte.
- Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados nos sistemas informatizados ou banco de dados da Administração Pública com fim de obter vantagem indevida para si ou para outrem (Art. 313-A).
- Modificar ou alterar, o servidor, sistemas informatizados ou programas sem autorização ou solicitação de autoridade competente (Art. 313 – B).

No Código Civil, por sua vez, está listado que … aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito (Art. 186 do Código Civil - Lei 10.406/02).

O Código de Ética do Servidor Publico determina que é vedado ao servidor publico (Art. XV, Decreto Nº 1.171, de 22/06/1994):

- Alterar ou deturpar o teor de documentos que deva encaminhar para providencias;
- Fazer uso de informações privilegiadas obtidas no âmbito interno de seu serviço, em benefício próprio, de parentes, de amigos ou de terceiros;

5.2 Tratamento de Informação

O tratamento de informação está relacionado com aspectos como recepção, produção, reprodução, armazenamento, acesso, transporte, transmissão, distribuição, utilização e eliminação da informação. Neste documento somente são considerados os aspectos de segurança relacionados a estes tópicos, pois o tratamento de informação em si é objeto de normas especificas entre os quais se destacam a Lei 8.159/91, Decreto 4.073/2002, Resoluções do CONARQ e normas internas da UFES.

As informações e documentos apresentam diferentes níveis de confidencialidade e devem ser classificados em:

- acesso e divulgação irrestritos;
- reservados – incluem-se neste item as informações pessoais, que somente poderão ser acessada pelo interessado (ou por alguém por ele autorizado) ou por agente público no exercício de sua atividade. Também informações que comprometam planos, projetos ou operações (Decreto 4.553/2002) ou assim determinados por ordem judicial são consideradas reservadas;
- confidenciais – por ordem judicial ou legislação especifica. Neste caso, estão as provas e exames, em geral.

Informações, independente da forma, devem ser mantidos integrados e íntegros, permitindo que os seus usuários acessem as informações que necessitam, dentro de um ambiente controlado. Como exemplo de informações podem ser listadas:

I. Todos os dados em todos os formatos que dão suporte às necessidades administrativas,

acadêmicas e operacionais da Universidade;

II. Todos os softwares, aplicações e sistemas operacionais utilizados para o gerenciamento destes dados;

III. Atividades de processamento e comunicação de dados relacionados a atividades de ensino, pesquisa e extensão.

Para a manutenção da segurança no tratamento da informação, a UFES deverá proporcionar instrumentos para:

- Armazenamento e cópias de segurança: procedimentos para assegurar a integridade e segurança dos dados, sob responsabilidade dos diversos setores da UFES.
- Classificação da informação quanto ao assunto e nível de confidencialidade;
- Descarte seguro de informação e mídia;
- Definição de mecanismos que garantam a integridade dos dados;
- Acesso de acordo com o nível de confidencialidade.

A Universidade é proprietária de todos os seus dados corporativos e detém os direitos autorais de todas as políticas, manuais e compilações destes dados.

Devem existir restrições ao acesso às informações referentes à intimidade, vida privada, honra e imagem das pessoas. As restrições não serão aplicadas nos seguintes casos:

- Consentimento expresso do titular da informação;
- Tratamento e diagnóstico médico;
- Estatísticas e pesquisas científicas de evidente interesse público, vedada a identificação da pessoa;
- Cumprimento de ordem judicial;
- Proteção do interesse público e geral preponderante.

Observados os princípios da proporcionalidade e da responsabilidade, as restrições ao acesso a informação relativa a vida privada, honra, imagem das pessoas não poderão ser utilizadas com o intuito de prejudicar o processo de apuração de irregularidades e as ações para a recuperação de fatos históricos de maior relevância. A pessoa que tem acesso a informações pessoais responsabiliza-se pelo uso indevido.

5.3 Tratamento de Incidentes de Segurança

Tratamento de Incidentes de Segurança de Informação é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências [NC05/IN01/DSIC/GSIPR, 2009, p. 3]. O tratamento de Incidentes de Segurança de Informação deve consistir de um conjunto de atividades coordenadas capazes de promover o restabelecimento do serviço e a eliminação ou diminuição dos impactos provenientes de incidentes de segurança.

As diretrizes para estruturação de um plano de tratamento de incidentes de segurança incluem, mas não se limitam as seguintes etapas:

- Identificar as fragilidades e eventos de segurança e sua divulgação e conscientização como processo educacional;
- Estabelecer canais de comunicação desses eventos de maneira a permitir a tomada de ações em

tempo hábil;

- Gerenciar os incidentes de segurança com o objetivo que um enfoque consistente e efetivo seja aplicado para a sua solução. A gestão inclui, entre outras:
    - Definir as estratégias de monitoramento de sistemas, alertas e vulnerabilidades;
    - Definir procedimentos para manusear os diferentes tipos de incidentes de segurança (trilhas de auditoria, responsabilidades, etc);
    - Definir procedimentos para receber e tratar notificações internas ou externas, com o objetivo e detectar ou identificar de fato a existência de um incidente de segurança;
    - Levantar os impactos e determinação do diagnostico preliminar que possa guiar as acoes de solução do problema;
    - Estabelecer planos de contingência;
    - Documentar as ações como processo de realimentação educacional

Em particular, no que se refere a recursos de TIC, este tratamento deve incluir estratégias para restaurar os serviços de computação e comunicação após eles terem sofrido:

- falhas de sistemas de informação e perda de serviços;
- ataques cibernéticos;
- violações de confidencialidade e integridade;
- sinistros (inundações, incêndios, etc,)

5.4 Gestão de Risco

Gestão de Riscos consiste em atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos (ABNT ISO GUIA 73:2009). Risco deve ser entendido como perigo ou possibilidade de perigo, ou seja, a possibilidade de perda ou exposição à perda. Deve ser avaliado como uma combinação da probabilidade de um evento e a sua consequência, portanto um compromisso entre a probabilidade de um evento e o seu impacto.

A Gestão de Riscos implica na identificação, avaliação, prevenção, tratamento e no controle destes. Dentre as ações relacionadas a Gestão de Riscos estão:

- Identificação de riscos, eventos e vulnerabilidades técnicas que podem causar interrupção dos processos da Universidade;
- Identificação da probabilidade de ocorrência de tais eventos e dos impactos associados;
- Levantamento dos ativos pertencentes aos grupos de risco;
- Definição do valor dos ativos;
- Classificação dos riscos segundo a probabilidade e o impacto e as consequências para a segurança da informação;
- Determinação de ações de gestão e controle dos riscos, que podem incluir, mas não estão restritos, a aquisição de hardware, software, processos, pessoal, comunicações, documentação, serviços, instalações e equipamentos, entre outros.
- Determinação das responsabilidades sobre a gestão de riscos;

Para o controle de riscos, deve haver:

- Revisão periódica
- Utilização de indicadores
- Avaliação
- Auditoria
- Acompanhamento

5.5 Auditoria e Conformidade

O cumprimento desta política de segurança deverá ser avaliado periodicamente por meio de verificações de conformidade, que inclusive poderão ser feitas com o apoio de entidades externas e independentes. Devem ser instituídos processos de análise e tratamento de conformidade, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da Universidade, de forma a obter o absoluto cumprimento destes instrumentos legais e normativos.

O processo de auditoria deve identificar todos os controles que governam sistemas de informação e avalia sua efetividade. Para cumprir este objetivo o processo de auditoria deve compreender por completo as operações, instalações físicas, telecomunicações, sistemas de controle, objetivos de segurança de dados, estrutura organizacional, pessoal, procedimentos e manuais e aplicações da organização. As auditorias devem rever tecnologias, procedimentos, documentos, treinamento e recursos humanos.

A CGTIC deverá aprovar uma plano de Auditoria e Conformidades, que deverá incluir métodos, técnicas, procedimentos, normas, responsabilidades para o efetivo cumprimento do estabelecido por esta politica no âmbito da UFES.

5.6 Controle de Acesso

Devem ser instituídas normas ou procedimentos que garantam o controle de acesso às informações e instalações.

A concordância expressa aos preceitos desta **POSIC** é condição necessária para o acesso aos ativos da UFES.

Considerando que ambientes de computação móvel e de trabalho remoto são necessários para a consecução das atividades da Universidade e que podem consistir em pontos fracos do sistema de gestão de segurança, devem ser instituídas normas e procedimentos que garantam a segurança da informação em ambientes de computação móvel e de trabalho remoto.

No caso de ambientes físicos de armazenamento de informações, deve haver, quando necessário, um sistema de controle de acesso que o registre. Se possível, deve ser usado um método de autenticação baseado em cartão de identificação.

No caso particular de recursos de TIC, deve haver uma politica estabelecida de criação e manutenção de senhas. Deve haver um sistema único de autenticação e a autenticação deve ser de caráter pessoal (cada pessoa com uma única identificação, vinculada a ela e não ao cargo que ocupa). As informações para autenticação devem ser consideradas pessoais e intransferíveis, não podendo a UFES armazená-las de forma que permita a sua recuperação, nem o usuário divulgá-las sob qualquer pretexto.

5.7 Comportamento de usuário

Os recursos de informação disponibilizados são fornecidos com o propósito único de garantir o desempenho das atividades da Universidade e, portanto, seus usuários devem manter comportamento responsável e consistente com objetivos educacionais, de pesquisa e administração da UFES.

Para tal, o usuário deve conhecer as instruções, regras e penalidades de funcionamento do serviço que ele esteja usando, devendo ainda:

1. Concordar plenamente com as regras e responsabilidades definidas neste documento e demais normas internas da Universidade sobre o uso dos recursos de tratamento da informação, incluindo, em especial, os recursos de TIC, da Universidade;
2. Responder por atos que violem as regras de uso dos recursos computacionais, estando, portanto, sujeito às penalidades definidas na política de uso desses recursos e também, se for o caso, às penalidades impostas por outras instâncias (Estatutos e Regimentos da Universidade Federal do Espírito Santo, leis municipais, estaduais e federais);
3. Comunicar imediatamente ao responsável sobre qualquer falha identificada na segurança da informação para avaliação e determinação das ações que se fizerem necessária.
4. Não se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;
5. Responsabilizar-se pela sua identidade eletrônica, senha, credenciais de autenticação, autorização ou outro dispositivo de segurança, negando revelá-la a terceiros;
6. O titular da conta deverá responder pelo mau uso dos recursos computacionais em qualquer circunstância;
7. O usuário deve manter seus computadores pessoais com software (*patches*, erratas) e com antivírus atualizados, conforme orientação do administrador de rede e da Política de Segurança da Universidade;
8. Se necessário, os usuários devem procurar o administrador de rede para esclarecimentos.
9. Informações confidenciais ou reservadas não podem ser transportadas em qualquer meio (CD, DVD, disquete, pendrive, papel, disco rígido, etc) sem as devidas autorizações e proteções.
10. As informações da organização estão sob responsabilidade do usuário, mesmo que estejam em um computador em sua casa ou outro local que não o ambiente de trabalho. Assim, não é uma boa prática transportar informações para trabalho em casa ou em computadores de terceiros, salvo quando estritamente necessário.

As normas de uso de recursos de TIC devem ser objeto de resolução especifica, que deverá se basear nesta POSIC.

As chefias imediatas dos servidores e órgãos de recursos humanos, ao programar ou efetivar transferências ou desligamentos de servidores, deverão informar os fatos ao NPD para que sejam providenciada as reconfigurações ou remoção das contas e senhas individuais destes servidores.

Os colaboradores externos devem atuar em conformidade e concordância expressa com esta POSIC e normas complementares. Cláusulas específicas de concordância e de penalidades em caso de infração devem ser inseridas nos respectivos contratos entre a UFES e eventuais colaboradores. Especificamente, devem lhes ser aplicadas restrições de acesso à informações sensíveis ou não necessárias ao exercício de suas atividades.

A interação com os colaboradores externos, relativa à manutenção da segurança da informação deve compreender, mas não se limitar, a acordos de confidencialidade, que versem sobre os seguintes itens:

1. Definição da informação passível de ser acessada pelo colaborador;
2. Tempo de duração do acordo;
3. Ações para finalização do acordo;
4. Responsabilidades e ações dos signatários para evitar a divulgação não autorizada da informação;
5. Uso permitido da informação por parte do signatário;
6. Especificação do direito de auditar e monitorar as informações;
7. Termos para a informação ser retomada após a finalização do acordo;
8. Ações a serem tomadas em casos de violação do acordo;
9. Termos de uso de recursos de TIC da Universidade.

5.8 Acesso a Rede local

Devem existir, pelo menos, duas redes distintas: uma rede Administrativa e uma rede Acadêmica. Em ambas as redes, deverão ser obrigatórias o registro do usuário e da máquina para acesso e a utilização de serviço de sincronismo de tempo. Também devem ser satisfeitas exigências quanto a existência de ferramentas no equipamento com *antivirus* e *firewall*, atualizado e habilitados.

Na rede administrativa, as restrições de segurança são maiores, correspondente às suas necessidades, devendo haver grande estanqueidade e maior nível de monitoramento.

Devido a natureza da universidade, deve haver um livre fluxo de informação e intercambio de idéias. Por outro lado, existem impedimentos legais e éticos a determinadas ações, que implicam em responsabilidades atribuídas tanto a UFES quanto ao usuário. Por isso, a UFES poderá usar instrumentos para o rastreamento de tais ações.

Deverá haver uma rede acessível a visitantes e usuários ou máquinas não identificados, na qual haverá restrições para garantia da segurança e desempenho da rede.

Para acesso pleno a rede local, poderá ser obrigatória a participação no sistema de inventário. Neste sistema será identificada a configuração do equipamento, seu número de patrimônio (se for o caso) e o responsável por ele. Neste processo não serão coletadas informações pessoais de qualquer natureza.

A UFES deverá estabelecer às normas de acesso a rede local por meio de resolução específica.

5.9 Acesso à Internet

O acesso à Internet só poderá ser efetivado após o registro obrigatório de computadores e usuários, de acordo com os sistemas de registro implementados. A autenticação deverá se basear em um serviço global de diretório.

Devido a natureza da universidade, deve haver um livre fluxo de informação e intercambio de idéias. Portanto o acesso a Internet será, por principio, livre. No entanto, para garantir o desempenho adequado da rede, poderão ser impostas limitações de horário de uso de certos serviços.

Por outro lado, como existem impedimentos legais e éticos a determinadas ações, que implicam em responsabilidades atribuídas tanto a UFES quanto ao usuário, a UFES poderá usar mecanismos de registro das

ações realizadas por seus usuários.

Conforme estabelecido na Politica de Uso da Rede Ipê, a UFES pode utilizar os Serviços de Redes disponíveis, suas facilidades de trânsito nacional e internacional, bem como usufruir dos acordos de interconexão existentes entre a RNP e outras redes estaduais, regionais e internacionais para promoção de suas atividades de ensino e pesquisa, exceto nas seguintes condições:

- produção ou transmissão de dados ou materiais considerados ilegais, entre outros, por caracterizarem: transgressão dos direito do autor, de proteção à criança e ao meio-ambiente;
- atentado à privacidade ou promoção à discriminação racial ou religiosa;
- veiculação de propaganda comercial, política ou religiosa;
- transmissão de mensagens ou material de propaganda não solicitadas pelo destinatário;
- uso em atividades estritamente comerciais;
- atividades que contribuam para ineficiência ou esgotamento dos recursos na rede, sejam eles computacionais, comunicacionais ou humanos;
- atividades que promovam a corrupção ou destruição de dados de usuários;
- atividades que interrompam ou prejudiquem a utilização dos Serviços de Rede por outros usuários;
- interligação ou abrigo em seu espaço de endereçamento de uma terceira instituição sem qualificação obtida através da Política de Uso da Rede Ipê.

A UFES deverá implementar mecanismos de autenticação, conforme descrito no Item 5.6 Controle de Acesso, que ofereçam a possibilidade de verificação e rastreamento, quando necessário, dos acessos à Internet feitos por seus usuários. O Usuário é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso. Em particular, o usuário deverá observar os termos de licença de uso do material obtida através da internet.

É vedado o uso de serviços que trafeguem informação de senha sem proteção.

Como subsidio a elaboração da resolução que estabelece a política de uso de recurso de TIC, deve ser especificado que os usuários dos computadores e da rede da UFES não poderão:

I. Utilizar a Internet com objetivos ou meios para a prática de atos ilícitos, proibidos pela lei ou pela presente Norma, lesivos aos direitos e interesses da Universidade ou de terceiros.

II. Utilizar a Internet com objetivo de danificar, inutilizar, sobrecarregar ou deteriorar os Recursos de TIC e dados de qualquer tipo, de uso corporativo, pessoal ou de terceiros.

III. Obter ou disponibilizar material sem a licença adequada através da rede;

IV. Acesso a sites de proxy com o objetivo de burlar os mecanismos de segurança existentes;

V. Acesso a sites de pornografia, pedofilia e outros contrários à lei. O acesso à esses sites é terminantemente proibido, ainda que os mesmos não estejam sendo bloqueados no sistema de segurança da UFES.

5.10 Uso de Correio Eletrônico

Os serviços de correio eletrônico são oferecidos como um recurso profissional para apoiar alunos, docentes e servidores no cumprimento de seus objetivos nas áreas de educação, pesquisa, comunicação e serviços.

O uso pessoal poderá ser permitido, mas não priorizado, desde que não provoque efeitos negativos para qualquer outro usuário, não viole o sistema de mensagens, não interfira nas suas atividades, não interfira direta ou indiretamente nas operações dos recursos computacionais e serviços de correio eletrônico da UFES, não incorra em gastos adicionais para a UFES, não interfira nas suas obrigações internas e externas à UFES, não interfira na produtividade das atividades funcionais da UFES, não tenha propósitos comerciais ou viole qualquer outra lei ou norma vigente. Portanto, cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal.

Deve ser considerado que o correio eletrônico é inerentemente uma forma insegura de comunicação, não garantindo sigilo ou entrega. A UFES poderá fornecer recursos adequados para melhorar o nível de segurança no uso do correio eletrônico, como, por exemplo, chaves de criptografia e assinatura digital.

O acesso às mensagens nos servidores de correio eletrônico deve ser feito usando protocolos seguros.

A UFES deverá possuir um serviço de correio eletrônico único com os controles de segurança adequados. Os usuários da RedeUfes terão direito a uma conta de correio eletrônico com endereço da forma ***identtificação.usuário@ufes.br .*** A identificação do usuário será geradas de acordo com o documento Caixas Postais Individuais-Funcionais na Rede Governo (baseada na norma X-400).

A UFES deverá estabelecer normas de uso do correio eletrônico que caracterize as ações adequadas para a manutenção da segurança na troca de mensagens eletrônicas.

A UFES deverá possuir instrumentos para o bloqueio ou copia de mensagens de maneira a subsidiar processos internos de sindicância ou para atendimento de ordem judicial. O bloqueio poderá ser aplicado a recepção de mensagens provenientes de alguns locais, comerciais ou não, em caso de inconveniência e/ou possível ameaça contida em mensagens indesejáveis.

5.11 Serviços Web

O Portal da UFES, que inclui todos os subdomínios da UFES e outros domínios sob sua responsabilidade ou de algum de seus órgãos, é um repositório de informações relacionados a UFES, disponibilizadas para a comunidade universitária e para o público em geral. O Portal foi projetado para promover a publicação periódica de estudos, trabalhos, eventos e informações institucionais de forma geral. Também tem a finalidade de servir como veículo de apresentação da comunidade universitária e seus recursos.

Considerando o principio do livre fluxo de informação e intercambio de idéias não haverá processo de censura ou restrição de informações publicadas eletronicamente por seus membros (professores, técnico-administrativos e alunos), exceto nos casos de determinação legal. Sendo assim, os autores deverão ser identificados e têm a responsabilidade pelo conteúdo das informações publicadas e devem estar cientes das responsabilidades e consequências inerentes a estas publicações e das resoluções e normas de UFES.

Serviços que manipulem informações reservadas deverão ser previamente autorizados e devidamente homologados pela UFES e, sempre que possível, utilizar o serviço único de autenticação na RedeUfes.

A autorização e homologação de ambientes e serviços web deverão ser objeto de normas complementares.

Deverão ser utilizados protocolos web seguros (como, por exemplo, https), sempre que se lide com informações

reservadas

Como diretriz, existem restrições legais quanto a publicação e a criação de referências a:

a) material com conteúdo comercial de caráter publicitário;
b) empresas ou entidades externas com objetivos comerciais;
c) material calunioso ou difamatório;
d) material que infrinja a legislação sobre direitos autorais;
e) material ofensivo ou que faça uso de linguagem ofensiva;
f) material que incite a qualquer tipo de discriminação;
g) material que incite à violência;
h) material pornográfico de qualquer natureza;
i) imagens ou dados que possam ser considerados abusivos, profanos, incômodos;
j) ameaçadores ou sexualmente ofensivos a uma pessoa comum, considerados os padrões éticos e morais correntes na comunidade.

A instalação de servidores Web na rede da UFES fora do ambiente do NPD é condicionada a aprovação pelo CGTIC satisfeitas os requisitos de segurança e conformidade com as normas relativas ao uso de recursos de TIC e a existência de um responsável legal.

Quanto a utilização de servidores Web da UFES para a hospedagem de páginas de entidades não vinculadas a UFES, mesmo usando domínio específico e não subordinado ao domínio **ufes.br**, fica estabelecido que:

I. A autorização para hospedagem de sítios de entidades externas na rede da universidade será avaliada pela CGTIC com base no seu interesse institucional.
II. O pedido deverá ser encaminhado à CGTIC pelo Dirigente da Unidade que será responsável pela hospedagem, acompanhado de justificativa e relevância institucional desta hospedagem para a UFES.

5.12 Descarte de Mídia

No contexto deste documento, mídia é um meio de armazenamento ou tecnicamente um suporte para informação e inclui desde discos rígidos a registros em papel. O descarte de mídia não é descarte de informação, pois esta é objeto de legislação especifica. Informação somente pode ser descartada depois de devido processo e autorização. Mídias somente podem ser descartadas se a informação armazenada puder ser descartada ou tiver sido preservada em outro meio.

Portanto, o descarte de mídias deve compreender, entre outros:

I. Métodos de controle de classificação de documentos que permitam identificar mídias contendo informações sensíveis, de maneira que sejam guardadas e destruídas de maneira segura;
II. Procedimentos de autorização de descarte;
III. Métodos e procedimentos de coleta e descarte para cada tipo de mídia;
IV. Métodos e procedimentos para o controle do descarte de mídias sensíveis de maneira a manter, sempre que possível, uma trilha de auditoria.

Em caso de papel, devem ser usadas fragmentadoras de papel (excepcionalmente, pode ser fragmentado

manualmente). Existem diversos modelos e níveis de segurança para fragmentadoras de acordo com a possibilidade de reconstituição do material fragmentado. No caso de CD, DVD, cartões magnéticos, muitos modelos de fragmentadoras conseguem destruí-los. Recomenda-se, então, que sejam adquiridas fragmentadoras de papel capazes de destruir CD, DVD e cartões magnéticos e de PVC e que atendam, pelo menos, ao nível 2 de segurança (ver Anexo A) e que sejam resistentes a grampos e clips (metálicos ou não).

Em mídias magnéticas ainda em funcionamento, deve ser usado um software especifico (formatação não é suficiente!) para apagar fisicamente todo o conteúdo do disco rígido, antes da eliminação. No caso do equipamento não estar funcional, a unidade deve ser retirada para ser limpa em outro equipamento compatível com uso de software especifico. Se a unidade não estiver funcional ela deve ser destruída mecanicamente.

5.13 Licenciamento de software

Programas de computador ou software são propriedade intelectual, protegida por Lei nº 9.609/1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador, e pela Lei nº 9.610/1998 que trata dos direitos autorais.

Deve-se considerar que o uso de softwares não licenciados pode prejudicar a segurança dos dados por uma série de razões. Entre elas destacam-se:

- Desconhecimento da origem: o software pode conter *trojans*, *backdoors* ou outros *malwares*;
- Eventualmente, para uso destes softwares pode ser preciso desligar mecanismos de proteção ou, então, não fazer uso de determinados mecanismos de segurança.

Também deve ser considerado que o uso de software não licenciado é crime. E a penalidade pode chegar a multa proporcional ao valor comercial do software, segundo interpretações baseadas no Art. 56 da Lei 9.610/98.

Conforme legislação federal, principalmente a Lei de Direitos Autorais e na Lei de Software, nenhum membro da comunidade universitária deve se envolver em qualquer atividade que viole os direitos de propriedade intelectual referentes a licenças de software ou qualquer outra política relacionada a software de computador ou conteúdos em formato digital.

Obter, usar, copiar ou distribuir software para outros usuários ou computadores, caso tal hipótese não seja contemplada na sua licença, é ilegal e viola as leis de software e de direitos autorais, implicando nas sanções legais.

Fica estabelecido que para utilizar qualquer software ou hardware de propriedade ou licenciado pela UFES, os usuários:

I. Devem concordar com todos os termos do acordo de licença de software;

II. Devem estar cientes que todos os softwares são protegidos por direitos autorais, a menos que explicitamente rotulados como software livre ou de domínio público;

III. Não podem copiar software para qualquer propósito com exceção daqueles permitidos no acordo de licença de utilização;

IV. Não podem tornar o software disponível para outras pessoas usarem ou copiarem, se tal procedimento estiver em desacordo com os termos da licença de software e/ou procedimentos adotados pela UFES;

V. Não podem aceitar software não licenciado de terceiros;

VI. Não podem instalar, nem permitir ou induzir outros a instalarem, cópias ilegais de software, ou software sem as devidas licenças, em qualquer recurso computacional de propriedade ou operado pela UFES.

Toda aquisição de equipamento computacional deve incluir necessariamente a aquisição de licenças do software básico mínimo apropriado para o seu uso funcionamento.

Toda licença de software, de qualquer natureza, adquirida pela UFES deve ser obrigatoriamente registrada, assim como também as licenças de software incluídas na aquisição do equipamento.

A instalação de software nos equipamentos computacionais da UFES somente é autorizada mediante as formalizações de registro e arquivamento da licença de uso, em sistema centralizado no Órgão responsável pelo equipamento, excluídos os softwares abertos ou de uso gratuito.

Todas estas disposições se aplicam também aos equipamentos e licenças de softwares doados ou adquiridos por convênios ou projetos de pesquisa vinculados à UFES.

Dada a natureza da Universidade, onde existem laboratórios de ensino e pesquisa, não é recomendável a centralização da instalação de software. Portanto, os usuários podem ter livre acesso às máquinas sob sua responsabilidade, mas, claramente, devem responder por elas. Principalmente nos casos de laboratórios de ensino recomenda-se o uso de sistemas que permitem a restauração da máquina a um estado inicial preestabelecido.
Em caso de detecção de alguma violação dos direitos de uso de algum software, este deve ser removido imediatamente e o responsável deve ser notificado.

Em todo processo de contratação de software, deve haver um documento específico explicitando para cada exemplar, a autorização de uso e as suas condições. Sempre que possível, deve-se buscar a contratação de softwares sem restrições que possam impedir sua migração para outro equipamento.

5.14 Política de Mesa Limpa/Tela Limpa

Deve ser seguido o principio estabelecido na Norma ABNT NBR/ISO/IEC 27.001 da Mesa limpa/Tela limpa. Segundo este principio para se reduzirem os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente, a UFES deve considerar a adoção de uma política de "mesas limpas" para os papéis e mídias de armazenamento removível e, igualmente, uma política de "telas limpas", contra, por exemplo, o perigo de ter um usuário já autenticado/registrado, porém ausente e com sua sessão de trabalho aberta.

A política de Mesa Limpa/Tela Limpa busca resguardar a Universidade bem como o próprio usuário contra o acesso não autorizado a informações como, por exemplo, terceiros observando dados expostos em mesas ou telas.

Assim, sinteticamente, entre outros:

- Os papéis (relatórios) e mídia eletrônica devem ser armazenados em armários trancados adequados e/ou em outras formas de mobiliário de segurança, quando não estiverem em uso, especialmente

fora do horário do expediente.

- Informações sensíveis ou críticas devem ser trancadas em local separado (idealmente em um armário ou cofre à prova de fogo) quando não necessárias, especialmente quando o ambiente fica vazio.
- Computadores pessoais e terminais de computador e impressoras não devem ser deixados autenticados/registrados quando não houver um operador (usuário) junto e devem ser protegidos por *keylocks*, senhas e outros controles quando não estiverem em uso.
- Pontos de entrada e saída de correio e de conexão de aparelhos de fax devem ser protegidos contra acesso indevido.
- Fotocopiadoras devem ser trancadas ou protegidas contra uso não autorizado fora do horário de expediente.
- Informações sensíveis ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente;
- Papéis, anotações e lembretes da sua mesa de trabalho devem ser mantidas sempre que possível fora da superfície da mesa (mesa limpa).
- Ao final do dia, ou no caso de ausência prolongada, limpar a mesa de trabalho.
- Papéis, livros ou qualquer informação confidencial não devem ser deixados na mesa.
- Informações confidenciais devem ser mantidas em local apropriado (longe dos olhos de curiosos)
- Um protetor de tela que solicite uma senha para acesso deve ser usado.
- Todos os documentos e meios eletrônicos no final do dia de trabalho devem ser devidamente guardados/organizados, com proteção adequada.
- Documentos contendo informações pessoais deve ser mantidos trancados.

5.15 Cobertura de rede sem fio (WiFi)

A UFES deverá oferecer uma solução de cobertura de rede sem fio baseado no padrão 802.11 para todos os campi da UFES, devido à grande demanda atual. Esta substituirá as soluções decorrentes de iniciativas individuais e localizadas de instalação de Pontos de Acesso WiFi (Access Points - AP). Estas últimas, sem conexão ao controlador ou supervisão, e em alguns casos, funcionando sem a exigência de qualquer tipo de autenticação, deverão ser desligadas e removidas. Além de interferência mútua, esta solução sem controle permite o acesso de computadores diretamente à rede local, representando ameaça à segurança da informação.

A solução contratada exigirá autenticação para acesso e, com o uso de VLAN, haverá controle rígido para acesso as redes locais. As permissões serão dadas de acordo com o perfil do usuário (docente, técnico administrativo, aluno de graduação, aluno de pós-graduação, entre outros). Poderá haver permissão para acesso a rede por parte de visitantes depois de um processo simplificado de registro. No entanto, a capacidade disponibilizada e as permissões serão bastante restritas, para evitar riscos de invasões, ataques e outras ações e, também, para que a UFES não sirva como polo de atração para usuários não diretamente ligados a ela.

Nos demais aspectos, o acesso à rede WiFi está sujeito aos mesmos mecanismos de controle de acesso, bem como às mesmas normas e diretrizes do acesso à rede local da Universidade.

5.16 Telefone e fax

Deve ser sempre considerado que telefone e fax não são meios seguros de comunicação. Sempre há a possibilidade de interceptação. Portanto, deve-se:

- Evitar ao máximo tratar de assuntos sigilosos através deles;
- Evitar dar o nome ao atender (aguardar a identificação do interlocutor);
- Não passar informações sensíveis;
- Solicitar o telefone para contato posterior e verificar o número, aumentando a garantia da identidade do interlocutor.

5.17 Mecanismos de segurança eletrônica

A Universidade deverá privilegiar, constantemente e de forma pró-ativa, o uso de mecanismos de segurança eletrônica, tais como IDS, IPS, Firewall, Certificados de Segurança, protocolos mais seguros (HTTPS, etc.).

6 Penalidades

Ações que violem a POSIC ou que quebrem os controles de segurança da informação e comunicações são passíveis de sanções civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isolada ou cumulativamente.

Docentes e técnico administrativos estão sujeitos a Lei nº 8.112/1990 que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. No Artigo 127 estão listadas as penalidades aplicáveis, a saber:

I. advertência;
II. suspensão;
III. demissão;
IV. cassação de aposentadoria ou disponibilidade;
V. destituição de cargo em comissão;
VI. destituição de função comissionada.

Especificamente em relação a informações o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal (Decreto nº 1171 /1994) estabelece que é vedado ao servidor público:

...

e) deixar de utilizar os avanços técnicos e científicos ao seu alcance ou do seu conhecimento para atendimento do seu mister;

...

h) alterar ou deturpar o teor de documentos que deva encaminhar para providências;

...

l) retirar da repartição pública, sem estar legalmente autorizado, qualquer documento, livro ou bem pertencente ao patrimônio público;

m) fazer uso de informações privilegiadas obtidas no âmbito interno de seu serviço, em benefício próprio, de parentes, de amigos ou de terceiros;

...

No caso de alunos, resoluções específicas devem ser aprovadas para que membros do corpo discente sofram punições em caso de violação das normas de segurança de informação. As penalidades devem variar de advertência ao desligamento da Universidade, sem prejuízo de outras sanções legais.

Para o caso de servidores de empresas terceirizadas, deve estar previsto no contrato o afastamento dos servidores envolvidos, sem prejuízo de outras sanções legais.

As penalidades devem ser gradativas e de acordo com a ação

- Uso indevido
- Disseminação de material proprietário (com *copyright*)
- Uso de material não adequadamente licenciado
- Produção e disseminação de material obsceno, racista, profana, obscena, intimidadora, difamatória, ilegal, ofensiva, abusiva.
- Quebra de sigilo
- Alteração de informações (falsidade ideológica)

Em todos os casos aplica-se o previsto no Código Penal e no Código Civil, bem como as normas e resoluções internas da UFES.

7 Competências e Responsabilidades

A responsabilidade pela Segurança da Informação e Comunicações deve ser vista como distribuída dentro da Instituição e todos os membros da instituição assumem corresponsabilidade quando usam estas informações.

Deverá ser instituído, por portaria específica, o Comitê de Segurança da Informação e Comunicações da Universidade, constituído por representantes, titular e suplente, indicados pelas respectivas áreas. O Comitê se reunirá no mínimo duas vezes ao ano e ficará vinculado ao Gabinete do Reitor. Sempre que necessário, poderão ser convidadas outras instituições ou especialistas para a reunião do Comitê.

O Comitê terá como atribuições mínimas:

a) assessorar na implementação das ações de SIC;

b) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre a SIC;

c) propor alterações na POSIC;

d) propor normas relativas à SIC.

O Comitê será a instância competente para dirimir eventuais dúvidas e deliberar sobre assuntos relativos à POSIC desta Universidade.

Os membros do Comitê deverão receber regularmente capacitação especializada em Segurança da Informação e Comunicações.

As Resoluções editadas pelo Comitê deverão ser cumpridas pelos servidores públicos, colaboradores e visitantes.

Assim estabelecido, a Gestão da Segurança de Informação e Comunicações ficará a cargo de um Comitê de Segurança de Informação e Comunicações (CSIC), que deverá ser integrado pelo Diretor do Núcleo de

Processamento de Dados (NPD), pelo Pró-Reitor de Planejamento, pelo Pró-Reitor de Administração, pelo Diretor Superintendente do Hospital Universitário e por um docente da Universidade indicado pelo Reitor. O coordenador da Comissão será definido pelo seus pares.

O Comitê de Segurança de Informação e Comunicações (CSIC) designará o Gestor de Segurança da Informação e Comunicações da UFES, que passará a compor o referido comitê a partir da sua designação. Este terá um mandato de dois anos, podendo ser renovado.

Caberá ao Comitê de Segurança da Informação e Comunicações:

I. Indicar o Gestor de Segurança da Informação e Comunicações;
II. Assessorar na implementação das ações de segurança da informação e comunicações no âmbito da UFES;
III. Constituir grupos de trabalho para tratar de temas e propor soluções especificas sobre segurança da informação e comunicações;
IV. Propor, analisar e aprovar Normas e Procedimentos internos sob forma de Instruções Normativas relativos a segurança da informação e comunicações, em conformidade com a legislação vigente;
V. Propor ajustes, aprimoramentos e modificações desta Política e submetê-las para aprovação pelo Conselho Universitário;
VI. Analisar os casos de violação desta Política e das Normas de Segurança da Informação, encaminhando-os ao Gestor de segurança da Informação quando for o caso;
VII. Propor projetos e iniciativas relacionados à melhoria da segurança da informação da UFES;
VIII. Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;
IX. Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;
X. Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação;
XI. Submeter ao Reitor proposta de abertura de processo de apuração de responsabilidade nos casos determinados por esta resolução.
XII. Propor outras normas e políticas, de acordo com as necessidades de se assegurar o cumprimento das diretrizes definidas pela POSIC;
XIII. Rever periodicamente esta política de segurança, bem como as normas e políticas relacionadas, sugerindo possíveis alterações;

Caberá ao Gestor de Segurança da Informação e Comunicações:

I. Promover cultura de segurança da informação e comunicações;
II. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança a partir dos relatórios encaminhados pela ETIR;
III. Propor recursos necessários às ações de segurança da informação e comunicações;
IV. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
V. Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;
VI. Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito

da Universidade e submetê-las à aprovação pelo Comitê de Segurança da Informação e Comunicações (CSIC).

VII. Dirimir dúvidas e deliberar sobre questões não contempladas nestas Diretrizes e em documentos relacionados;

VIII. Receber e analisar as comunicações de descumprimento das normas e políticas referentes à Política de Segurança da Informação e Comunicações - POSIC da UFES, apresentando parecer à CSIC para sua apreciação;

IX. Solicitar, sempre que necessário, a realização de auditorias pelo NPD/UFES, relacionadas ao uso dos recursos de Tecnologia da Informação e Comunicação no âmbito da UFES.

X. Tratar de Classificação de informações; Controle de acesso físico; Monitoração e auditoria de recursos tecnológicos; Descarte de equipamentos eletrônicos de armazenamento de informação; Plano de Gerencia de Riscos de recursos de TIC;

Haverá uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), composta pelo Gestor de Segurança da Informação e Comunicações e três servidores indicados pelo Diretor do Núcleo de Processamento de Dados. A coordenação do ETIR será indicada pelo Diretor do Núcleo de Processamento de Dados

Caberá à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR):

I. Tomar ações para mitigar os efeitos do incidente;.

II. Elaborar e submeter ao Gestor de Segurança da Informação propostas de normas e políticas especificas para diminuição do número de incidentes e para diminuir os seus efeitos.

III. Elaborar e submeter ao Gestor de Segurança da Informação relatórios relativos aos incidentes e em aspectos como:

- Gerenciamento de Identidade e acesso lógico;
- Contingência e continuidade das atividades relacionadas à TIC;
- Controle de acesso à Internet;
- Utilização de armazenamento lógico;
- Utilização de equipamentos de Tecnologia da Informação;
- Utilização de programas e aplicativos;
- Utilização do correio eletrônico.
- Utilização dos recursos Web;

Caberá aos Administradores de Sistemas e Redes:

I. Prover todas as informações de segurança da informação solicitadas pela Comissão de Segurança da Informação e Comunicações (CSIC);

II. Prover ampla divulgação da Política e das Normas de Segurança da Informação nos setores sob sua responsabilidade;

III. Oferecer orientação e treinamento sobre a Política de Segurança da Informação e suas Normas a todos os servidores e colaboradores de seu setor;

IV. Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da UFES, mantendo-se atualizada em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;

V. Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso as redes locais, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários,

sempre em conjunção com as normas regulatórias da UFES;

VI. Analisar os dados relacionados à segurança da informação do setor sob sua responsabilidade e apresentar relatórios periódicos sobre tais riscos ao CSIC, acompanhados de proposta de aperfeiçoamento do ambiente de controle, quando for o caso;

VII. Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações do seu setor;

VIII. Realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação;

IX. Estabelecer mecanismo de registro e controle de não-conformidade a esta Política e às Normas de Segurança da Informação, comunicando ao CSIC.

8 Atualização

Esta POSIC, bem como os documentos gerados a partir dela, sofrerá processo de avaliação e atualização ao final de dois anos de vigência. No entanto, em caso de necessidade, esta POSIC e os documentos relacionados poderão ser modificados a qualquer tempo.

9 Documentos complementares

Documentos complementares deverão ser propostos para que um ambiente seguro com relação a informação e comunicação seja efetivamente implementado na UFES. Caberá a CSIC determinar quais são esses documentos, as responsabilidades sobre sua elaboração e os encaminhamentos para sua aprovação no âmbito da UFES. Como exemplo, são listados:

- Resolução de política de uso de recursos de TIC;
- Cartilha/Apostila de Segurança de Informação.

Para se fazer cumprir as diretrizes estabelecidas por esta POSIC, este documento deverá ser complementado por Resolução especifica de aprovação desta norma e da estrutura responsável por sua aplicação.

Bibliografia Adicional

- Jaime Antunes da Silva, Seminário A Gestão de Documentos Arquivísticos na Administração Pública Federal. 22 de junho de 2010. Brasília. Link: http://www.siga.arquivonacional.gov.br/media/iii_encontro_siga_2010/apresentao_jaime_os__reflexos_do_projeto_de_lei_de_acesso.pdf. Acessado em 27/10/2011.
- Carol Templeton . Security in an Open Environment such as a University? December 21, 2004. Link:http://www.sans.org/reading_room/whitepapers/policyissues/security-open-environment-university_1570. Acessado em 27/10/2011.

Anexos

A Níveis de segurança para fragmentadoras de papel

O padrão internacional DIN 32757-1 determina o tamanho máximo das tiras ou partículas geradas pela fragmentadora. Estas são são classificadas em 5 níveis:

Nível 1: Largura máxima de tiras de 12 mm

Nível 2: Largura máxima de tiras de 6 mm

Nível 3: Largura máxima de Tiras de 2 Mm ou Fragmento máximo de 4 mm × 80 mm

Nível 4: Máximo de Fragmento 2 mm × 15 mm = 30 mm²

Nível 5: Máximo de Fragmento 0,8 mm × 13 mm = 10,40 mm²

B Normas ISO/IEC sobre segurança da informação

As normas internacionais (já parcialmente traduzidas para o português e devidamente chanceladas pela Associação Brasileira de Normas Técnicas (ABNT) da série ISO/IEC 27000 mostram os fundamentos e as melhores práticas a serem seguidas para a segurança de informação[1].

ISO/IEC 27000:2009	*Sistema de Gerenciamento de Segurança* Explicação da série de normas, objetivos e vocabulários;
ISO/IEC 27001:2005	*Sistema de Gestão de Segurança da Informação* Especifica requerimentos para estabelecer, implementar, monitorar e rever, além de manter e provisionar um sistema de gerenciamento completo. Utiliza o PDCA como prinípio da norma e é certificável para empresas.
ISO/IEC 27002:2005	*Código de Melhores Práticas para a Gestão de Segurança da Informação* Mostra o caminho de como alcanças os controles certificáveis na ISO 27001. Essa ISO é certificável para profissionais e não para empresas.
ISO/IEC 27003:2010	*Diretrizes para Implantação de um Sistema de Gestão da Segurança da Informação* Segundo a própria ISO/IEC 27003, "O propósito desta norma é fornecer diretrizes práticas para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), na organização, de acordo com a ABNT NBR ISO/IEC 27001:2005.
ISO/IEC 27004:2009	*Gerenciamento de Métricas e Relatórios para um Sistema de Gestão de Segurança da Informação* Mostra como medir a eficácia do sistema de gestão de SI na corporação.
ISO/IEC 27005:2008	*Gestão de Riscos de Segurança da Informação* Essa norma é responsável por todo ciclo de controle de riscos na organização, atuando junto à ISO 27001 em casos de certificação ou através da ISO 27002 em casos de somente implantação.
ISO/IEC 27006:2007	*Requisitos para auditorias externas em um Sistema de Gerenciamento de Segurança da Informação* - Especifica como o processo de auditoria de um sistema de gerenciamento de segurança da informação deve ocorrer.
ISO/IEC 27007	*Referências (guidelines) para auditorias em um Sistema de Gerenciamento de Segurança da Informação.*
ISO/IEC 27008	*Auditoria nos controles de um SGSI* O foco está nos controles para implementação da ISO 27001.
ISO/IEC 27010	*Gestão de Segurança da Informação para Comunicações Inter Empresariais* Foco nas melhores formas de comunicar, acompanhar, monitorar grandes incidentes e fazer com que isso seja feito de forma transparente entre empresas particulares e governamentais.

1 http://marcoacorreia.wordpress.com/2011/03/27/sera-que-voce-realmente-conhece-a-familia-iso-27000/

ISO/IEC 27011:2008	*Gestão de Segurança da Informação para empresa de Telecomunicações baseada na ISO 27002* Entende-se que toda parte de telecomunicação é vital e essencial para que um SGSI atinga seus objetivos plenos(claro que com outras áreas), para tanto era necessário normatizar os processos e procedimentos desta área objetivando a segurança da informação corporativa de uma maneira geral. A maneira como isso foi feito, foi tendo como base os controles e indicações da ISO 27002.

C Modelo de termo de responsabilidade

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, portador (a) da cédula de identidade n.º _____, expedida pelo _____, em _____ e inscrito no C.P.F. sob o n.º_____, e lotado no(a)_____deste (Nome do órgão ou entidade), DECLARO , sob pena das sanções cabíveis nos termos da _____ (legislação vigente) que assumo a responsabilidade por:

I) tratar o(s) ativo(s) de informação como patrimônio do UFES;

II) utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do (Nome do órgão ou entidade);

Nestes termos,

Vitória, _____
(data)

Assinatura e Nome do usuário e seu setor organizacional

Assinatura e Nome da autoridade responsável pela autorização do acesso

D Modelo de termo de ciência

TERMO DE CIÊNCIA

Pelo presente, eu, _____, portador (a) da cédula de identidade n.º _____ e inscrito no C.P.F. sob o n.º _____, residente e domiciliado na _____, nº _____, na cidade de _____, estado do _____, declaro ter ciência da Política de Segurança da Informação e Comunicação (POSIC), bem como suas normas complementares, comprometendo-me a cumprir o disposto no citado diploma.

Nestes termos,

Vitória, _____

(data)

Assinatura e Nome do usuário

E Modelo de checklist de segurança física

Item	Seção	Questões a auditar	Sim?	Não?
1 Segurança Física e do Ambiente				
1.1 Áreas de Segurança				
1.1.1	Perímetro da Segurança Física	Se barreiras físicas, como recursos de segurança, foram implementadas para proteger o serviço de processamento de informação		
		Alguns exemplos de tais recursos são o controle por cartão no portão de entrada, muros, presença de um funcionário na recepção, etc.		
1.1.2	Controles da Entrada Física	Se existem controles de entrada para permitir somente a entrada do pessoal autorizado dentro de várias áreas da organização.		
1.1.3	Segurança de escritórios, salas e instalações de processamento	Se as salas, que possuem o serviço de processamento de informação ou contém armários fechados ou cofres são trancadas		
		Se o serviço de processamento de informação é protegido contra desastres naturais ou causados pelo homem		
		Se existe alguma ameaça potencial de propriedades vizinhas		
1.1.4	Trabalhando em áreas seguras	Se existe algum controle de segurança para prestadores de serviço ou funcionários trabalhando em área de segurança. A informação deve ser fornecida quando necessário.		
1.1.5	Isolamento das áreas de expedição e cargas	Se as áreas expedição e carga e de processamento ode informação são isoladas uma da outra para evitar acesso não autorizado.		
		Se uma avaliação de risco foi realizada para determinar a segurança de tais áreas.		
1.2 Segurança dos equipamentos				
1.2.1	Instalação e proteção de equipamentos	Se o equipamento está instalado em local apropriado para minimizar o acesso não autorizado à área de trabalho.		
		Se os itens que requerem proteção especial foram isolados para aumentar o nível geral de proteção exigida.		
		Se os controles foram adotados para minimizar os riscos de ameças potenciais, como roubo, fogo, explosão, fumaça, água, poeira, vibração, efeitos químicos, interferências no fornecimento de energia, radiação eletromagnética, inundação.		
		Se existe uma politica especial para alimentação, bebida e fumo nas proximidades das instalações de processamento de informação		
		Se os aspectos ambientais são monitorados para evitar condições que possam afetas de maneira adversa a operação das instalações de processamento da informação		
1.2.2	Fornecimento de energia	Se o equipamento é protegido contra falhas de energia e outras anomalias na alimentação elétrica, utilizando fornecimento de energia permanente como alimentação múltipla, no-breaks, gerador de reserva.		
1.2.3.	Segurança de cabeamento	Se o cabeamento elétrico e de telecomunicações que transmitem dados ou suportam os serviços de informação são protegidos contra interceptação ou dano		
		Se existe algum controle de segurança adicional para informações sensíveis ou críticas.		
1.2.4	Manutenção de equipamentos	Se os equipamentos tem manutenção de acordo com os intervalos e especificações do fabricante.		
		Se a manutenção é realizada apenas pelo pessoal autorizado		
		Se são mantidos registros com todas as falhas suspeitas ou ocorridas e de toda a manutenção corretiva e preventiva		
		Se os controles apropriados são utilizados quando do envio de equipamentos fora da instalação física		
		Se todos os requisitos impostos pelas apólices de seguro são atendidas		
1.2.5	Segurança de equipamentos fora das dependências da organização	Se um equipamento é autorizado pela direção quando necessitar ser utilizado fora das instalações da organização		
1.2.6	Reutilização e alienação segura de equipamentos	Se dispositivos de armazenamento contendo informações sensíveis são fisicamente destruídos ou sobrescritos de maneira segura.		
1.3 Controles Gerais				
1.3.1	Política de Mesa limpa/Tela limpa	Se um serviço de bloqueio automático de tela de computador está ativo. Isso travará o computador sem que for deixado ocioso por um determinado tempo.		
		Se os empregados são avisados para deixar qualquer material confidencial de forma segura e trancada.		
1.3.2	Remoção de Propriedade	Se os equipamentos, informações ou software podem ser retirados em adequada proteção		
		Se inspeções regulares são realizadas para detectar remoção não autorizada de propriedade		
		Se as pessoas estão cientes que estas inspeções regulares são realizadas.		

Fonte: Francisco Marcelo Alencar de Matos. Proposta de um *Checklist* para Verificação da Segurança Física de uma Empresa

Baseada na Norma ANBT NBR/ISO/IEC 27002:2005. Monografia final de curso de Bacharelado em Ciências da Computação. Faculdade Lourenço Filho. Fortaleza. 2010.