Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

SERVIÇO PÚBLICO FEDERAL

UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

Gabinete do Reitor

PORTARIA Nº 1340/GR/UFFS/2013

O REITOR *PRO TEMPORE*, DA UNIVERSIDADE FEDERAL DA FRONTEIRA SUL, no uso de suas atribuições, resolve:

TÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1° ESTABELECER diretrizes, critérios, normas e procedimentos de Segurança da Informação e Comunicações no âmbito da Universidade Federal da Fronteira Sul (UFFS).

TÍTULO II
DO OBJETIVO E APLICAÇÃO

Art. 2° Política de Segurança da Informação e Comunicações da Universidade Federal da Fronteira Sul (POSIC/UFFS) visa assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas e/ou custodiadas pela UFFS.

Art. 3° A Política é aplicada a todos aqueles que, direta ou indiretamente, possuem acesso às informações da Universidade Federal da Fronteira Sul (UFFS).

TÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 4° Para os efeitos desta Política e das normas complementares e procedimentos operacionais de Segurança da Informação e Comunicações criados para o âmbito da UFFS, serão adotados os conceitos e definições descritos no "Dicionário de Referência da POSIC/UFFS", anexo I.

TÍTULO IV
DOS PRINCÍPIOS

Art. 5° A POSIC/UFFS deve obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal.

Art. 6° A POSIC/UFFS orienta-se pelos princípios de disponibilidade, de integridade, de confidencialidade e de autenticidade da Segurança da Informação e Comunicações.

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

TÍTULO V
DAS DIRETRIZES DE SEGURANÇA

Art. 7° A alta administração da Universidade Federal da Fronteira Sul cumprirá o disposto na Instrução Normativa GSI/PR N° 1, de 13 de junho de 2008 e suas complementares na implantação do POSIC/UFFS.

Art. 8° Adota-se o método PDCA (PLAN-DO-CHECK-ACT) como metodologia para implantação e implementação do Sistema de Gestão de Segurança da Informação e Comunicações como recomenda a Norma Complementar N° 02/IN01/DSIC/GSI/PR, do Gabinete de Segurança Institucional da Presidência da República e a norma ABNT NBR ISO/IEC 27001:2006.

CAPÍTULO I
DOS ATIVOS DE INFORMAÇÃO

Art. 9° Os ativos de informação da UFFS devem ser inventariados, classificados e protegidos, com a devida identificação de seus proprietários e custodiantes.

Parágrafo único: Utilizar os ativos da UFFS estritamente dentro do propósito institucional, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 10. Dispositivos móveis, de armazenamento, corporativos ou particulares, obedecerão às diretrizes da POSIC/UFFS e as recomendações da Norma Complementar N° 12/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional da Presidência da República.

CAPÍTULO II
DO TRATAMENTO DA INFORMAÇÃO

Art. 11. Toda informação é patrimônio da UFFS, devendo ser protegida no acesso, tráfego, uso, armazenamento e descarte de acordo com sua classificação em graus de sigilo à UFFS, ao Estado e as pessoas.

Parágrafo único: Preservar a integridade, a confidencialidade, a disponibilidade, a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela Universidade.

Art. 12. O armazenamento e o processamento de informações baseado em computação em nuvem devem obedecer às diretrizes e normas complementares dessa Política e a legislação brasileira, que deve prevalecer sobre qualquer outra, de modo a ter todas as garantias legais enquanto tomadora do serviço e proprietária das informações hospedadas na nuvem.

Art. 13. A informação hospedada na estrutura do *Data Center* da UFFS deve fazer uso de solução de *backup* (cópia de segurança) com locais, frequência e demais diretrizes previstas em norma complementar.

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

CAPÍTULO III
DO CONTROLE DE ACESSO

Art. 14. O controle de acesso observará as diretrizes e normas complementares dessa Política, as recomendações da Norma Complementar N° 07/IN01/DSIC/GSIPR do Gabinete de Segurança Institucional da Presidência da República e da ABNT NBR ISO/IEC 27002:2005.

Art. 15. Todos os usuários são responsáveis pela segurança dos ativos de informação e comunicações que estejam sob sua responsabilidade.

Art. 16. Todos os sistemas de informação da UFFS, automatizados ou não, devem ter um gestor do ativo de informação, formalmente designado pela autoridade competente.

Art. 17. Os usuários que tenham acesso às informações com classificação de sigilo devem respeitar regras de proteção estabelecidas.

Art. 18. Os perímetros físicos de atuação da UFFS devem ser adequadamente protegidos, visando salvaguardar os ativos de informação, conforme a classificação de risco de cada ambiente.

CAPÍTULO IV
DO USO DE CORREIO ELETRÔNICO, DA INTERNET E DAS REDES SOCIAIS.

Art. 19. O uso da internet, e-mail corporativo e das redes sociais, no âmbito da UFFS, devem ser detalhados em normas específicas em conformidade com as diretrizes dessa Política.

Parágrafo único: Diretrizes para Gestão Arquivista do Correio Eletrônico devem se observadas através da Resolução N° 36 do Conselho Nacional de Arquivos (CONARQ).

CAPÍTULO V
DA AUDITORIA E CONFORMIDADE

Art. 20. O uso dos recursos computacionais e de informações da UFFS é passível de monitoramento, respeitando os princípios legais de acordo com a Norma Complementar N° 02/IN01/DSIC/GSI/PR, do Gabinete de Segurança Institucional da Presidência da República e a ABNT NBR ISO/IEC 27002:2005.

I - Mecanismos que permitam a rastreabilidade desse uso devem ser implementados e mantidos pela UFFS.

II - A entrada ou saída de equipamento computacional da UFFS deve ser autorizada e registrada.

Art. 21. As condições e termos de licenciamento de *software* e os direitos de propriedade intelectual devem ser respeitados.

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

Art. 22. O cumprimento das normas de Segurança da Informação e Comunicações da UFFS será auditado periodicamente.

Art. 23. A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

CAPÍTULO VI
DA GESTÃO DA CONTINUIDADE

Art. 24. A UFFS deve elaborar, implementar e instituir metodologias ou normas que estabeleçam a Gestão de Continuidade do Negócio.

CAPÍTULO VII
DOS CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES.

Art. 25. Todos os contratos, convênios, acordos e instrumentos congêneres devem:

I - Conter cláusulas que estabeleçam a obrigatoriedade de observância e aceitação desta Política de Segurança de Informação e Comunicações e de suas normas complementares.

II - Prever a obrigação da outra parte de divulgar esta Politica de Segurança de Informação e Comunicações e suas normas complementares aos seus colaboradores e prepostos envolvidos em atividades na UFFS.

III - A instalação, compra e uso de soluções de Tecnologia da Informação e Comunicação devem atender à Instrução Normativa N° 04 de 12 de novembro de 2010, do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Ministério de Planejamento, Orçamento e Gestão (MPOG).

CAPÍTULO VIII
DA GESTÃO DE RISCOS

Art. 26. A UFFS implementará e manterá processos de gestão de riscos para prevenir incidentes e proteger os ativos de informação e comunicações.

Parágrafo único: Os processos devem possibilitar a classificação de ordem de prioridade dos ativos e a definição e implementação de controles para identificação e tratamento de problemas de segurança.

CAPÍTULO IX
DO TRATAMENTO DE INCIDENTES DE REDE

Art. 27. Instituir e manter a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

Art. 28. Devem ser instituídas metodologias ou normas que estabeleçam processos de gestão para tratamento e respostas a incidentes de Segurança da Informação e Comunicações.

CAPÍTULO X
DO *SOFTWARE* SEGURO

Art. 29. A contratação e desenvolvimento de *software* seguirão as recomendações da Norma Complementar N° 16/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional da Presidência da República e normativas da UFFS.

CAPÍTULO XI
DA PUBLICIDADE E CAPACITAÇÃO

Art. 30. A POSIC/UFFS deve ser conhecida e seguida por todos os usuários do órgão sendo difundida na UFFS por meio de um processo permanente de conscientização e sensibilização em Segurança da Informação e Comunicações.

Art. 31. O Gestor de Segurança da Informação e Comunicações, os integrantes da Equipe de Segurança da Informação e Comunicações (ETIR) deverão receber regularmente, capacitação especializada em Segurança da Informação e Comunicações, a fim de garantir a adequada gestão, manutenção destas diretrizes e tratamento de incidentes como recomenda as Normas Complementares N° 08/IN01/DSIC/GSIPR, N° 17/IN01/DSIC/GSIPR e N° 18/IN01/DSIC/GSIPR do Gabinete de Segurança Institucional da Presidência da República.

Art. 32. A UFFS observará sempre melhores práticas e procedimentos de Segurança da Informação e Comunicações, recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 33. Demais requisitos de segurança, normas, procedimentos da Segurança da Informação e Comunicações serão estabelecidos em normas complementares especificas a essa Política.

TÍTULO VI
DAS COMPETÊNCIAS E REPONSABILIDADES

Art. 34. Todos os agentes públicos que necessitem ter acesso às informações devem assinar, antes do início de suas atribuições, termo de responsabilidade e confidencialidade, garantindo o conhecimento e zelo pelo adequado cumprimento desta Política de Segurança da Informação e Comunicações.

Art. 35. Ao Reitor, de acordo com a Instrução Normativa GSI/PR N° 1, de 13 de junho de 2008, compete:

a) Coordenar as ações de segurança da informação e comunicações;

b) Aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança;

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

c) Propor programa orçamentário específico para as ações de segurança da informação e comunicações;

d) Nomear Gestor de Segurança da Informação e Comunicações;

e) Instituir e implementar Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

f) Instituir Comitê de Segurança da Informação e Comunicações;

g) Aprovar Política de Segurança da Informação e Comunicações e demais normas de Segurança da Informação e Comunicações;

h) Remeter os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações, sempre que solicitado formalmente, ao GSI/PR.

i) Prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da ETIR e do Comitê de Segurança da Informação e Comunicações bem como prover a infraestrutura necessária;

Art. 36. Aos membros do Comitê de Segurança da Informação e Comunicações da UFFS, de acordo com a Instrução Normativa GSI/PR N° 1, de 13 de junho de 2008, compete:

a) Assessorar na implementação das ações de Segurança da Informação e Comunicações ;

b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

c) Propor alterações na Política de Segurança da Informação e Comunicações;

d) Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

Art. 37. Ao Gestor de Segurança da Informação e Comunicações, de acordo com a Instrução Normativa GSI/PR N° 1, de 13 de junho de 2008, compete:

a) Promover a cultura de segurança da informação e comunicações no âmbito da UFFS;

b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) Propor recursos necessários às ações de segurança da informação e comunicações;

d) Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

e) Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

f) 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;

g) Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do UFFS;

Art. 38. À Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais compete, em consonância com as Normas Complementares N° 05/IN01/DSIC/GSIPR e N° 08/IN01/DSIC/GSIPR do Gabinete de Segurança Institucional da Presidência da República:

a) Receber, analisar e responder a notificações e atividades relacionadas aos incidentes de segurança da informação e Comunicações;

b) Registrar todos os incidentes notificados ou detectados, com a finalidade de assegurar registro histórico das atividades da ETIR.

TÍTULO VII
DAS PENALIDADES

Art. 39. O não cumprimento das determinações da POSIC/UFFS, bem como de suas Normas Complementares e Procedimentos Técnicos, sujeitará o infrator às penalidades previstas na Constituição Federal, Código Civil, Código Penal, Lei 8.112, Decreto N° 1.171 e em regulamentos/normativos internos da Presidência da República e desta Instituição.

Art. 40. As violações das normas e regulamentos, ainda que não expressamente descritas, serão punidas com revisão temporária de privilégios de acesso aos recursos de Tecnologia da Informação e Comunicações da UFFS, após avaliação da gravidade da infração.

Art. 41. Em casos de risco ou quebra de Segurança da Informação e Comunicações por meios eletrônicos, o Gestor de SIC e a ETIR devem ser imediatamente acionados para adotar as providências necessárias, podendo inclusive determinar a restrição temporária do acesso às informações e/ou aos recursos computacionais da UFFS.

TÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 42. Os casos omissos serão analisados e deliberados pelo Comitê de Segurança da Informação e Comunicações da UFFS.

Art. 43. Os Instrumentos normativos gerados a partir da POSIC/UFFS, incluindo a própria POSIC devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.

TÍTULO IX
DA VIGÊNCIA

Art. 44. Esta portaria entra em vigor a partir de sua publicação no Boletim Oficial da UFFS.

Chapecó-SC, 11 de setembro de 2013.

Prof. Jaime Giolo
Reitor *pro tempore* da UFFS

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

ANEXO I

DICIONÁRIO DE REFERÊNCIA DA POSIC-UFFS

ABREVIATURAS

01. **CTIR GOV:** Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Publica Federal, subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da Republica - GSI.

02. **ETIR:** Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

03. **Gestor de SIC:** Gestor de Segurança da Informação e Comunicações.

04. **GSI/PR:** Gabinete de Segurança Institucional da Presidência da República.

05. **PDCA:** do inglês: *PLAN-DO-CHECK-ACT* (Planejar-Fazer-Checar-Agir).

06. **POSIC-UFFS:** Política de Segurança da Informação e Comunicações da Universidade Federal da Fronteira Sul-UFFS.

07. **POSIC:** Politica de Segurança da Informação e Comunicações.

08. **SIC:** Segurança da Informação e Comunicações.

CONCEITOS E DEFINIÇÕES

I - **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. Fonte: 07/IN01/DSIC/GSIPR.

II - **Administrador de Perfil Institucional:** agentes públicos que detenham autorização do responsável pela área interessada para administrar perfis institucionais de um órgão ou entidade da APF nas redes sociais. Fonte: 15/IN01/DSIC/GSIPR.

III - **Agente público:** Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta. Fonte: 18/IN01/DSIC/GSIPR.

IV - **Agente Responsável:** Servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta, incumbido de chefiar e gerenciar o processo de Inventário e Mapeamento de Ativos de Informação ou a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais. Fonte: 10/IN01/DSIC/GSIPR; 05/IN01/DSIC/GSIPR.

V - **Agentes públicos com dispositivos móveis corporativos:** servidores ou empregados da APF, que utilizam dispositivos móveis de computação de

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

propriedade dos órgãos ou entidade a que pertencem. Fonte: 12/IN01/DSIC/GSIPR.

VI - **Agentes públicos com dispositivos móveis particulares:** servidores ou empregados da APF que utilizam dispositivos móveis de computação de sua propriedade. Para fins desta Norma Complementar, os dispositivos particulares que se submetem aos padrões corporativos de software e controles de segurança, e que são incorporados à rede de dados do órgão, são considerados como dispositivos corporativos. Fonte: 12/IN01/DSIC/GSIPR.

VII - **Ambientação:** Evento que oferece informações sobre a missão organizacional do órgão ou instituição, bem como sobre o papel do agente público nesse contexto. Fonte: 18/IN01/DSIC/GSIPR.

VIII - **Ameaça:** conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. Fonte: 04/IN01/DSIC/GSI/PR.

IX - **Análise de Impacto nos Negócios (AIN):** visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos ou entidades da APF, bem como as técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos. Fonte: 06/IN01/DSIC/GSIPR.

X - **Análise de riscos:** uso sistemático de informações para identificar fontes e estimar o risco.

XI - **Análise dinâmica:** tipo de teste de software que verifica seu comportamento externo em busca de anomalias ou vulnerabilidades. A análise dinâmica ocorre por meio de interações com o software em execução. Fonte: 16/IN01/DSIC/GSIPR.

XII - **Análise estática:** tipo de teste de software que verifica sua lógica interna em busca de falhas ou vulnerabilidades. A análise estática ocorre por meio da verificação do código-fonte ou dos binários. Fonte: 16/IN01/DSIC/GSIPR.

XIII - **Análise/avaliação de riscos:** processo completo de análise e avaliação de riscos. Fonte: 04/IN01/DSIC/GSI/PR.

XIV - **Artefato malicioso:** é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores. Fonte: 05/IN01/DSIC/GSIPR.

XV - **Atividade:** processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços. Fonte: 06/IN01/DSIC/GSIPR.

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

XVI - **Atividades críticas:** atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo. Fonte: 06/IN01/DSIC/GSIPR.

XVII - **Atividades de ensino em segurança da informação e comunicações:** Eventos de orientação/instrução que abordam o tema SIC. Fonte: 18/IN01/DSIC/GSIPR.

XVIII - **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. Fonte: 04/IN01/DSIC/GSI/PR.

XIX - **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. Fonte: Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008.

XX - **Avaliação de conformidade em segurança da informação e comunicações:** exame sistemático do grau de atendimento dos requisitos relativos à SIC com as legislações específicas. Fonte: 11/IN01/DSIC/GSIPR.

XXI - **Avaliação de riscos:** processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco. Fonte: 04/IN01/DSIC/GSI/PR.

XXII - **Bloqueio de acesso:** processo que tem por finalidade suspender temporariamente o acesso. Fonte: 07/IN01/DSIC/GSIPR.

XXIII - **Capacitação:** Atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema, estando aptos para atuar em suas organizações como Gestores de SIC. Fonte: 18/IN01/DSIC/GSIPR.

XXIV - **Certificações profissionais:** processo negociado pelas representações dos setores sociais, pelo qual se identifica, avalia e valida formalmente os conhecimentos, saberes, competências, habilidades e aptidões profissionais desenvolvidos em programas educacionais ou na experiência de trabalho, com o objetivo de promover o acesso, permanência e progressão no mundo do trabalho e o prosseguimento ou conclusão de estudos. Fonte: 17/IN01/DSIC/GSIPR.

XXV - **Comitê de Segurança da Informação e Comunicações:** grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF. Fonte: 03/IN01/DSIC/GSIPR.

XXVI - **Computação em nuvem:** modelo computacional que permite acesso por demanda, e independente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores,

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços. Fonte: 14/IN01/DSIC/GSIPR.

XXVII - **Comunicação do risco:** troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas. Fonte: 04/IN01/DSIC/GSI/PR.

XXVIII - **Comunidade ou público alvo:** é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais. Fonte: 05/IN01/DSIC/GSIPR.

XXIX - **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado. Fonte: Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008.

XXX - **Conformidade em segurança da informação e comunicações:** cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação e Comunicações da organização. Fonte: 11/IN01/DSIC/GSIPR.

XXXI - **Conscientização:** Atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema. Fonte: 18/IN01/DSIC/GSIPR.

XXXII - **Contas de Serviço:** contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, script, etc.) sem qualquer intervenção humana no seu uso. Fonte: 07/IN01/DSIC/GSIPR.

XXXIII - **Contêineres dos ativos de informação:** o contêiner é o local onde "vive" o ativo de informação, onde está armazenado, como é transportado ou processado. Fonte: 10/IN01/DSIC/GSIPR.

XXXIV - **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. Fonte: 06/IN01/DSIC/GSIPR.

XXXV - **Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso. Fonte: 07/IN01/DSIC/GSIPR.

XXXVI - **Controles de segurança:** medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: a criptografia, as funções de "*hash*", a validação de entrada, o balanceamento de carga, as trilhas de auditoria, o controle de acesso, a expiração de sessão, os "*backups*", etc. Fonte: 16/IN01/DSIC/GSIPR.

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

XXXVII - **Credenciais ou contas de acesso:** permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha. Fonte: 07/IN01/DSIC/GSIPR.

XXXVIII - **Credenciamento:** processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer. Fonte: 07/IN01/DSIC/GSIPR.

XXXIX - **CTIR GOV:** Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República - GSI. Fonte: 05/IN01/DSIC/GSIPR.

XL - **Custodiante do ativo de informação:** refere-se a qualquer indivíduo ou estrutura do órgão ou entidade da APF que tenha a responsabilidade formal de proteger um ou mais ativos de informação, como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações comunicadas pelos proprietários dos ativos de informação. Fonte: 10/IN01/DSIC/GSIPR.

XLI - **Desastre:** Evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação. Fonte: 06/IN01/DSIC/GSIPR.

XLII - **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade. Fonte: Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008.

XLIII - **Dispositivos móveis:** consiste em equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem não se limitando a estes: notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDs externos e cartões de memória. Fonte: 12/IN01/DSIC/GSIPR.

XLIV - **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR:** Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores. Fonte: 05/IN01/DSIC/GSIPR.

XLV - **Escolas de Governo:** Entidades de ensino da Administração Pública que trabalham com formação e aperfeiçoamento profissional dos servidores públicos dos três níveis de governo. Fonte: 18/IN01/DSIC/GSIPR.

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

XLVI - **Especialização:** Atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos p pessoal e profissional, além de servirem como multiplicadores sobre o tema, estando aptos para atuar em suas organizações como Gestores de SIC, além de tornarem-se referência na pesquisa de novas soluções e modelos de SIC. Fonte: 18/IN01/DSIC/GSIPR.

XLVII - **Estimativa de riscos:** processo utilizado para atribuir valores à probabilidade e consequências de um risco. Fonte: 04/IN01/DSIC/GSI/PR.

XLVIII - **Estratégia de continuidade de negócios:** abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior. Fonte: 06/IN01/DSIC/GSIPR.

XLIX - **Evitar risco:** uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco. Fonte: 04/IN01/DSIC/GSI/PR.

L - **Exclusão de acesso:** processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso. Fonte: 07/IN01/DSIC/GSIPR.

LI - **Formação continuada:** Evento de ensino que tem por finalidade desenvolver e ampliar a capacidade profissional dos servidores públicos. Fonte: 18/IN01/DSIC/GSIPR.

LII - **Formação inicial:** Evento de ensino que tem como finalidade formar os servidores públicos para a investidura em seus cargos. Fonte: 18/IN01/DSIC/GSIPR.

LIII - **Gestão de continuidade:** processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado. Fonte: 06/IN01/DSIC/GSIPR.

LIV - **Gestão de mudanças nos aspectos relativos à SIC:** é o processo de gerenciamento de mudanças, de modo que ela transcorra com mínimos impactos no âmbito do órgão ou entidade da APF, visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação. Fonte: 13/IN01/DSIC/GSIPR.

LV - **Gestão de riscos de segurança da informação e comunicações:** conjunto de processos que permitem 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. Fonte: 04/IN01/DSIC/GSI/PR.

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

LVI - **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. Fonte: Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008.

LVII - **Gestor de mudanças:** é o responsável pelo processo de mudanças no âmbito do órgão ou entidade da APF. Fonte: 13/IN01/DSIC/GSIPR.

LVIII - **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. Fonte: 03/IN01/DSIC/GSIPR.

LIX - **Identificação de riscos:** processo para localizar, listar e caracterizar elementos do risco. Fonte: 04/IN01/DSIC/GSI/PR.

LX - **Identificação e classificação de ativos de informação - é um processo composto por 6 (seis) etapas:**

a) coletar informações gerais

b) definir as informações dos ativos

c) identificar o$_{(s)}$ responsável$_{(is)}$

d) identificar os contêineres dos ativos

e) definir os requisitos de segurança

f) estabelecer o valor do ativo de informação. Fonte: 10/IN01/DSIC/GSIPR.

LXI - **Incidente de segurança:** é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;. Fonte: 05/IN01/DSIC/GSIPR.

LXII - **Incidente:** evento que tenha causado algum dano, colocado em risco, algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação. Fonte: 06/IN01/DSIC/GSIPR.

LXIII - **Infraestrutura crítica da informação:** são os meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso, que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade. Fonte: 10/IN01/DSIC/GSIPR.

LXIV - **Integridade:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. Fonte: Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008.

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

LXV - **Inventário e mapeamento de ativos de informação:** é um processo interativo e evolutivo, composto por 3 (três) etapas: (a) identificação e classificação de ativos de informação, (b) identificação de potenciais ameaças e vulnerabilidades e (c) avaliação de riscos. Fonte: 10/IN01/DSIC/GSIPR.

LXVI - **Modelo de Implementação:** são os modelos de implementação da computação em nuvem em geral: Nuvem Própria, Nuvem Comunitária, Nuvem Pública e Nuvem Híbrida. Fonte: 14/IN01/DSIC/GSIPR.

LXVII - **Mudança:** transição ou alteração de uma situação atual. Fonte: 13/IN01/DSIC/GSIPR.

LXVIII - **Necessidade de conhecer:** condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação. Fonte: 07/IN01/DSIC/GSIPR.

LXIX - **Padrões corporativos de sistemas e de controle:** conjunto de regras e procedimentos que compõem os normativos internos das corporações. Fonte: 12/IN01/DSIC/GSIPR.

LXX - **Perfil de acesso:** conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso. Fonte: 07/IN01/DSIC/GSIPR.

LXXI - **Perfil institucional:** cadastro de órgão ou entidade da APF como usuário em redes sociais, alinhado ao planejamento estratégico e à Política de Segurança da Informação e Comunicações (POSIC) da instituição, com observância de sua correlata atribuição e competência. Fonte: 15/IN01/DSIC/GSIPR.

LXXII - **Plano de continuidade de negócios:** documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes. Fonte: 06/IN01/DSIC/GSIPR.

LXXIII - **Plano de gerenciamento de incidentes:** plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes. Fonte: 06/IN01/DSIC/GSIPR.

LXXIV - **Plano de recuperação de negócios:** documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade. Fonte: 06/IN01/DSIC/GSIPR.

LXXV - **Política de Segurança da Informação e Comunicações (POSIC):** documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

segurança da informação e comunicações. Fonte: Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008.

LXXVI - **Prestador de serviço:** pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso. Fonte: 07/IN01/DSIC/GSIPR.

LXXVII - **Programa de gestão da continuidade de negócios:** processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção. Fonte: 06/IN01/DSIC/GSIPR.

LXXVIII - **Proprietário do ativo de informação ou gestor do ativo de informação:** refere-se à parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação, assumindo, no mínimo, as seguintes atividades: a) descrever o ativo de informação; b) definir as exigências de segurança da informação e comunicações do ativo de informação; c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários; d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento; e, e) indicar os riscos que podem afetar os ativos de informação. Fonte: 10/IN01/DSIC/GSIPR.

LXXIX - **Quebra de segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações. Fonte: Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008.

LXXX - **Redes sociais:** estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns. Fonte: 15/IN01/DSIC/GSIPR.

LXXXI - **Reduzir risco:** uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco. Fonte: 04/IN01/DSIC/GSI/PR.

LXXXII - **Requisitos de segurança:** conjunto de necessidades de segurança que o software deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da organização, compreendendo aspectos funcionais e não funcionais. Os aspectos funcionais descrevem comporta- mentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança como, por exemplo, controle de acesso baseado em papéis de usuários (administradores, usuários comuns, etc.), autenticação com o uso de credenciais (usuário e senha, certificados digitais, etc.), dentre outros. Os

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

aspectos não funcionais descrevem procedimentos necessários para que o software permaneça executando suas funções adequadamente mesmo quando sob uso indevido. São exemplos de requisitos não funcionais, dentre outros, a validação das entradas de dados e o registro de logs de auditoria com informações suficientes para análise forense. Fonte: 16/IN01/DSIC/GSIPR.

LXXXIII - **Resiliência:** poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre. Fonte: 06/IN01/DSIC/GSIPR.

LXXXIV - **Reter risco:** uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado. Fonte: 04/IN01/DSIC/GSI/PR.

LXXXV - **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. Fonte: 04/IN01/DSIC/GSI/PR.

LXXXVI - **Segurança da informação e comunicações:** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008.

LXXXVII - **Sensibilização:** Atividade de ensino que tem como objetivo orientar sobre o que é Segurança da Informação e Comunicações (SIC) fazendo com que os participantes possam perceber em sua rotina pessoal e profissional ações que precisam ser corrigidas. Fonte: 18/IN01/DSIC/GSIPR.

LXXXVIII - **Serviço:** é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais. Fonte: 05/IN01/DSIC/GSIPR.

LXXXIX - **Tempo objetivo de recuperação:** é o tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente. Fonte: 06/IN01/DSIC/GSIPR.

XC - **Termo de responsabilidade:** termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso. Fonte: 07/IN01/DSIC/GSIPR.

XCI - **Transferir risco:** uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco. Fonte: 04/IN01/DSIC/GSI/PR.

XCII - **Tratamento da informação:** recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas. Fonte: Instrução Normativa GSI/PR n. 1, de 13 de junho de 2008.

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

XCIII - **Tratamento de incidentes de segurança em Redes Computacionais:** 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. Fonte: 05/IN01/DSIC/GSIPR.

XCIV - **Tratamento dos riscos:** processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco. Fonte: 04/IN01/DSIC/GSI/PR.

XCV - **Usuário:** 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. Fonte: 07/IN01/DSIC/GSIPR.

XCVI - **Usuários visitantes com dispositivos móveis:** agentes públicos ou não que utilizam dispositivos móveis de sua propriedade, ou do órgão ou entidade a que pertencem, dentro dos ambientes físicos e virtuais de órgãos ou entidades da APF, dos quais não fazem parte. Fonte: 12/IN01/DSIC/GSIPR.

XCVII - **Valor do ativo de informação:** valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos de um órgão ou entidade da APF, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado. Fonte: 10/IN01/DSIC/GSIPR.

XCVIII - **Verificação de conformidade em segurança da informação e comunicações:** procedimentos que fazem parte da avaliação de conformidade que visam identificar o cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação e Comunicações da organização. Fonte: 11/IN01/DSIC/GSIPR.

XCIX - **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. Fonte: 04/IN01/DSIC/GSI/PR.

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br

ANEXO II

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

I - Constituição da República Federativa do Brasil

II - Código Civil Brasileiro.

III - Código Penal Brasileiro.

IV - Código Civil, Art. 1.016.

V - LEI N° 9.983, de 14 de Julho de 2000.

VI - Lei N° 8.112, de 11 de Dezembro de 1990.

VII - Decreto N° 1.171, de 24 de junho de 1994.

VIII - Decreto N° 3.505, de 13 de junho de 2000.

IX - Instrução Normativa GSI/PR N° 01, de 13 de junho de 2008.

X - Instrução Normativa N° 4-SLTI/MPOG, de 12 de Novembro de 2010.

XI - Resolução N° 36, de 19 de Dezembro de 2012-CONARQ.

XII - Norma Complementar N° 02/IN01/DSIC/GSIPR

XIII - Norma Complementar N° 03/IN01/DSIC/GSIPR

XIV - Norma Complementar N° 04/IN01/DSIC/GSI/PR

XV - Norma Complementar N° 05/IN01/DSIC/GSIPR

XVI - Norma Complementar N° 06/IN01/DSIC/GSIPR

XVII - Norma Complementar N° 07/IN01/DSIC/GSIPR

XVIII - Norma Complementar N° 08/IN01/DSIC/GSIPR

XIX - Norma Complementar N° 10/IN01/DSIC/GSIPR

XX - Norma Complementar N° 11/IN01/DSIC/GSIPR

XXI - Norma Complementar N° 12/IN01/DSIC/GSIPR

XXII - Norma Complementar N° 13/IN01/DSIC/GSIPR

XXIII - Norma Complementar N° 14/IN01/DSIC/GSIPR

XXIV - Norma Complementar N° 15/IN01/DSIC/GSIPR

XXV - Norma Complementar N° 16/IN01/DSIC/GSIPR

XXVI - Norma Complementar N° 17/IN01/DSIC/GSIPR

XXVII - Norma Complementar N° 18/IN01/DSIC/GSIPR

XXVIII - ABNT NBR ISO/IEC 27001:2006

XXIX - ABNT NBR ISO/IEC 27002:2005

Ministério da Educação Universidade Federal da Fronteira Sul

Avenida Getúlio Vargas, 609-N Edifício
Engemede, 2º Andar
Chapecó - Santa Catarina
Brasil - CEP 89812-000

www.uffs.edu.br
contato@uffs.edu.br