POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
URI - Campus de Frederico Westphalen

1. INTRODUÇÃO

A FuRI - Fundação Regional Integrada, mantenedora da URI - Universidade Regional Integrada do Alto Uruguai e das Missões - Campus de Frederico Westphalen, para proteger as suas informações, visando a redução dos riscos de falhas, danos e/ou os prejuízos que possam comprometer a imagem e a continuidade dos objetivos da instituição, estabelece esta Política de Segurança da Informação.

A Política de Segurança da Informação estabelece as diretrizes para a adoção de procedimentos e mecanismos relacionados à segurança da informação, de acordo com a NBR ISO/IEC 27002 - Código de Prática para a Gestão da Segurança da Informação, devendo ser cumprida por todos os seus professores, funcionários técnico-administrativos, alunos e prestadores de serviços terceirizados.

A informação é um ativo que possui grande valor, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, Internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo, etc.

Por princípio, a segurança da informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças, devendo abranger três aspectos básicos:

I) **Confidencialidade:** somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação.
II) **Integridade:** somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações.
III) **Disponibilidade:** a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Os equipamentos e sistemas que viabilizam a atividade de acesso eletrônico à rede corporativa e à conexão com a Internet, assim como as informações geradas, recebidas, armazenadas e transmitidas compõem patrimônio da Universidade e, como tal, devem ser entendidos e protegidos.

2. RESPONSABILIDADES

A Política de Segurança da Informação estabelece responsabilidades da FuRI, professores, funcionários técnico-administrativos, alunos e serviços terceirizados.

2.1 Da FuRI

Como mantenedora da URI - Universidade Regional Integrada do Alto Uruguai e das Missões - Campus de Frederico Westphalen, a FuRI - Fundação Regional Integrada, assume o compromisso de utilizar informações confiáveis e íntegras, devendo:

I) **Preservar a informação, confidencialidade, integridade e disponibilidade:** Garantindo que as informações sejam acessadas somente pelas pessoas devidamente autorizadas a qualquer momento, com a sua exatidão e integridade, salvando as informações em meios de armazenamentos seguros, em conformidade com estatutos, regimentos, regulamentos e a legislação pertinente.

II) **Reduzir os riscos de erro humano:** Conscientizando e treinando os usuários de modo a garantir a aplicação adequada dos recursos e o atendimento às normas e políticas de segurança da informação.

III) **Preservar e prevenir contra o uso indevido dos recursos de tecnologia da informação:** Garantindo que os recursos computacionais e de comunicação sejam utilizados somente para as atividades da instituição.

O cumprimento das diretrizes deverá ser atingido através de:

I) **Implementação da gestão da continuidade das atividades da Universidade:** Assegurar a continuidade dos processos vitais à Universidade, por meio da combinação de ação de prevenção e recuperação. Considerar prazos máximos de recuperação de sistemas de acordo com a criticidade dos processos. Contemplar planos de contingência e procedimentos para a prevenção, detecção e eliminação de vírus e *softwares* maliciosos.

II) **Salvaguarda de informações organizacionais:** Garantir a proteção das informações da Universidade contra perda, destruição ou falsificação, de maneira a atender os requisitos estatutários, regulamentares, de auditoria ou que possam assegurar a defesa adequada contra potenciais processos civis ou criminais. Contemplar cópias de segurança *(backup)* e tratamento adequado de mídias removíveis.

III) **Controle e gerenciamento da rede:** Garantir a segurança dos dados da rede, assim como a proteção dos serviços oferecidos contra acessos não autorizados, utilizando um conjunto de controles, considerando o uso de tecnologias que assegurem a confidencialidade e a integralidade dos dados que trafegam por redes públicas e privadas e coordenando as atividades de gerenciamento de forma a otimizar o serviço prestado para garantir a aplicação dos procedimentos de segurança em toda a infraestrutura de processamento da informação.

IV) **Estabelecimento de um gerenciamento de acesso:** Através de procedimentos de controle do acesso aos sistemas de informação e serviços que estabeleçam regras para a inclusão e exclusão de usuários. Divulgar as normas e procedimentos de segurança da informação adotados pela Universidade

V) **Monitoramento do uso e acesso ao sistema:** Adotar sistemas de monitoramento com a finalidade de detectar divergências entre a Norma de

Segurança Interna para a Utilização dos Recursos de TI e os eventos monitorados, fornecendo dessa maneira, evidências em caso de incidente de segurança da informação.

VI) **Corresponsabilidade dos usuários pela segurança da informação:** Implantar programas de conscientização e treinamento para os usuários dos recursos de tecnologia da informação, objetivando a redução do erro humano, roubo, fraude e o uso indevido das instalações e informações da Universidade.

VII) **Respeito aos direitos de propriedade intelectual:** Utilizar somente *softwares* adquiridos através de licenças, limitados a quantidade contratada, em respeito à legislação do direito autoral.

VIII) **Registro de incidentes de segurança:** Todos os incidentes de segurança relacionados à tecnologia da informação (fragilidades ou ameaças, ocorridas ou suspeitas) devem ser notificadas ao Setor de Tecnologia da Informação.

IX) **Garantia da manutenção de instalações adequadas:** Os recursos tecnológicos e as instalações de processamento de informações críticas e vitais ao funcionamento da Universidade devem ser mantidos em áreas ambientalmente apropriadas, protegidas contra o acesso não autorizado, dano ou interferência. Deverão ser implementados controles de acesso às áreas de acesso restrito.

2.2 Dos Professores e Funcionários Técnico-Administrativos

Todos os professores e funcionários técnico-administrativos da Universidade obrigam-se ao cumprimento das seguintes diretrizes:

I) Utilizar os recursos de tecnologia da informação somente para a execução das atividades da Universidade;

II) Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento, conforme Anexo I, da Norma de Segurança Interna para a Utilização dos Recursos de TI;

III) Racionalizar o envio e recepção de informações digitais, evitando excessos que sobrecarreguem a rede e provoquem lentidão na transmissão e recepção de informações e prejuízo para a Universidade;

IV) Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela Universidade. Não divulgar informações privilegiadas da Universidade, sob pena sofrer as punições estabelecidas pela Instituição (Normas de Aplicação de Medidas Disciplinares) e previstas em Lei;

V) Não instalar ou utilizar equipamentos pessoais ou de terceiros no ambiente da Universidade;

VI) Não instalar ou armazenar qualquer tipo de *software* ou arquivos nos recursos de TI disponibilizados pela Universidade. Os arquivos deverão ser armazenados de acordo com a Normas de Utilização da Rede. Utilizar somente *softwares* homologados e instalados pelo setor de TI;

VII) Não copiar ou distribuir os conteúdos e mídias disponibilizados nos repositórios da Instituição;
VIII) Realizar somente *download* de arquivos da Internet que sejam necessários ao desempenho de suas atividades;
IX) Adotar cuidados no acesso as informações pessoais, aos sites de instituições financeiras (Internet *banking)* e de compras on-line por meio dos recursos de TI disponibilizados pela Universidade em salas de aula ou laboratórios. A Instituição não se responsabiliza pelas informações fornecidas pelo aluno nesses acessos;
X) Acessar o correio eletrônico pessoal no ambiente da Universidade é permitido desde que essa ferramenta não seja utilizada de modo indevido, ilegal ou antiético. O usuário deverá seguir as regras contidas nas Normas de Utilização de E-mail;
XI) Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
XII) Adotar senhas de acesso para garantir a segurança das informações e a proteção dos equipamentos de acordo com as Normas de Senhas;
XIII) Encerrar a sessão de trabalho ao término da utilização;
XIV) Não alterar de local os equipamentos de TI. Em caso de necessidade, realizar a solicitação de mudança de equipamento, conforme o Anexo IV;
XV) Comunicar imediatamente ao Setor de Tecnologia da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

2.3 Dos Alunos

Todos os alunos da Universidade obrigam-se ao cumprimento das seguintes diretrizes:

I) Assinar Contrato de Prestação de Serviços Educacionais, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, no ato da matrícula/rematrícula, bem como assumindo responsabilidade por seu cumprimento;
II) Cumprir as Normas para Utilização dos Laboratórios de Informática;
III) Não instalar equipamentos pessoais ou de terceiros no ambiente da Universidade;
IV) Não instalar ou armazenar qualquer tipo de *software* ou arquivos nos recursos de TI disponibilizados pela Universidade. Os arquivos deverão ser armazenados de acordo com a Norma de Utilização da Rede;
V) Utilizar dispositivos móveis ou portáteis particulares nas dependências da Universidade é de inteira responsabilidade do seu proprietário, tanto por conteúdos nele instalados ou armazenados, sejam *softwares,* músicas, fotos, entre outros;

VI) Conectar dispositivos móveis ou portáteis na rede da Universidade tornará passível de monitoramento. Esses dispositivos somente poderão ser conectados à rede da Instituição através de Rede Sem Fio *(Wireless)* e terão acesso a sites e serviço de transferência de arquivos, de acordo com a Norma de Acesso Wireless;

VII) Não divulgar informações privilegiadas da Universidade, sob pena sofrer as punições estabelecidas pela Instituição (Normas de Aplicação de Medidas Disciplinares) e previstas em Lei;

VIII) Não copiar ou distribuir os conteúdos e mídias disponibilizados nos repositórios da Instituição. Esses repositórios têm a finalidade educacional e devem ser utilizados como tal;

IX) Realizar somente *download* de arquivos da Internet que sejam necessários ao desempenho de suas atividades nas salas de aula, laboratórios e bibliotecas, desde que previstos nos documentos educacionais e/ou autorizados pelo docente do curso;

X) Adotar cuidados no acesso as informações pessoais, aos sites de instituições financeiras (Internet *banking)* e de compras on-line por meio dos recursos de TI disponibilizados pela Universidade em salas de aula ou laboratórios. A Instituição não se responsabiliza pelas informações fornecidas pelo aluno nesses acessos;

XI) Acessar o correio eletrônico pessoal no ambiente da Universidade é permitido desde que essa ferramenta não seja utilizada de modo indevido, ilegal ou antiético. O aluno deverá seguir as regras contidas nas Normas de Utilização de E-mail;

XII) Não alterar de local os equipamentos de TI disponibilizados pela Universidade.

2.4 Dos Serviços Terceirizados

As empresas e prestadores de serviços terceirizados obrigam-se ao cumprimento das seguintes diretrizes:

I) Adicionar no contrato de prestação de serviços que a contratada está ciente da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;

II) Tornar-se responsável pelos equipamentos que utilizar ou instalar no ambiente da Universidade;

III) Formalizar a necessidade de utilizar áreas de acesso restrito ou equipamentos da Universidade, não especificadas em contrato, através de documento que conste a finalidade, os profissionais e o tempo de acesso.

3. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

As seguintes condutas serão classificadas como falta grave e o infrator estará sujeito a sanções disciplinares e administrativas, de acordo com a Norma de Aplicação de Medidas Disciplinares:

I) Utilizar os Recursos de Tecnologia da Informação para fins que não sejam relacionados às atividades da Universidade;
II) Utilizar os recursos de TI da Universidade para conseguir acesso não autorizado a qualquer outro computador, rede, banco de dados ou informação armazenada eletronicamente (interna ou externamente);
III) Divulgar informações confidenciais ou de propriedade da Universidade, sem a devida autorização;
IV) Enviar em nome da Universidade, mensagens que externem opiniões pessoais;
V) Enviar textos, figuras, desenhos ou mensagens com conteúdo sexual, político, ideológico, racista, discriminatório, ofensivo ou difamatório ou que comprometam a reputação ou imagem da Universidade;
VI) Enviar mensagens do tipo corrente, que se multiplicam sucessivamente, através de recomendações, para que o destinatário as repasse a seus conhecidos (pedidos de ajuda, alertas sobre vírus, piadas, apresentações, etc.);
VII) Acessar ou armazenar material pornográfico, jogos, *chais* ou *softwares* mensageiros;
VIII) Copiar, distribuir ou imprimir material protegido por direitos autorais, sem permissão;
IX) Desativar ou violar os dispositivos de segurança instalados nos equipamentos;
X) Compartilhar com terceiros as senhas de acesso aos recursos de TI. As senhas são pessoais e intransferíveis;
XI) Retransmitir o sinal de rede para outros equipamentos;
XII) Retirar do local os equipamentos de TI sem a autorização do Setor de TI;
XIII) Estragar propositalmente os equipamentos de TI.

4. MONITORAMENTO

O monitoramento da utilização dos recursos de TI é direito da Universidade, amparado legalmente, e como tal, é suscetível aos processos de auditoria. As informações privadas, protegidas legalmente, tais como as contidas em sites de instituições financeiras e centros de medicina diagnóstica não serão monitorados. As demais, somente serão divulgadas quando solicitadas por comissão de sindicância, devidamente nomeada, conforme estabelecido pela Norma de Segurança Interna Para a Utilização dos Recursos de TI.

Compete ao Setor de TI da Universidade monitorar, a qualquer tempo e sem prévio aviso, todos os acessos a qualquer computador da Internet, bem como o envio e recepção de mensagens, com o intuito de assegurar que os recursos computacionais e de comunicação oferecidos pela Universidade sejam utilizados somente para as atividades da qual a instituição se propõe.

5. MEDIDAS DISCIPLINARES

Compete ao Setor de Recursos Humanos da Universidade:

I) Aplicar sanções disciplinares ao Professor ou Funcionário Técnico-Administrativo que violar ou permitir a violação desta Norma, de acordo com a Norma de Aplicação de Medidas Disciplinares.

Compete ao Coordenador de Curso:

I) Apor sanções disciplinares ao aluno que violar ou permitir a violação desta Norma, de acordo com a Norma de Aplicação de Medidas Disciplinares.

Compete ao Professor durante as suas aulas:

I) Aplicar sanções disciplinares ao aluno que violar ou permitir a violação desta Norma, de acordo com a Norma de Aplicação de Medidas Disciplinares.

Compete ao setor responsável pela contratação de prestadores de serviços:

I) Solicitar a inclusão de cláusula de obrigatoriedade do conhecimento e cumprimento desta Política e das Normas de Segurança Interna para a Utilização dos Recursos de TI, nos contratos de prestação de serviços que envolvam tecnologia da informação. Os contratos devem estabelecer quais recursos e áreas de TI serão disponibilizadas pela Universidade;
II) Encaminhar a aplicação das sanções para as infrações estabelecidas no contrato do serviço.

6. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Juntamente com a Política de Segurança da Informação fica instituído o Comitê de Segurança da Informação, sendo o responsável pela implementação e cumprimento da presente Política.

O Comitê de Segurança da Informação é composto por:

- Diretor Geral da URI - Campus de Frederico Westphalen
- Diretor Administrativo da URI - Campus de Frederico Westphalen
- Gerente do RH da URI - Campus de Frederico Westphalen
- Gerente de TI da URI - Campus de Frederico Westphalen
- Gerente de Redes da URI - Campus de Frederico Westphalen

7. DISPOSIÇÕES FINAIS

O Setor de TI e o Comitê de Segurança da Informação implementarão as regras definidas nesta Política, sendo responsável, também, pela adoção de medidas técnicas adicionais necessárias à manutenção da infra-estrutura e à otimização do uso dos recursos de tecnologia da informação.

O Setor de TI poderá, a qualquer momento, verificar os computadores, com o objetivo de averiguar e identificar possíveis não-conformidades descritas nesta Política de Segurança da Informação.

Ademais, todos os usuários da Universidade devem seguir as Normas de Segurança Interna para a Utilização dos Recursos de TI, visando o adequado emprego de seus recursos.

Fica sobre responsabilidade do Setor de TI a divulgação de boas práticas quanto ao uso seguro da tecnologia da informação no âmbito da Universidade. As dúvidas de interpretação desta Política, bem como os casos omissos, serão dirimidas pelo Comitê de Segurança da Informação.

A presente política passa a vigorar a partir da data de sua aprovação sendo válida por tempo indeterminado.

Frederico Westphalen, 24 de agosto de 2011.

Direção URI - Câmpus de Frederico Westphalen **Comitê de Segurança da Informação**

NORMAS PARA A UTILIZAÇÃO DOS LABORATÓRIOS DE INFORMÁTICA

URI - Campus de Frederico Westphalen

Os Laboratórios de Informática da Universidade Regional Integrada - Campus de Frederico Westphalen, mantida pela FuRI - Fundação Regional Integrada, aqui denominada instituição, tem como objetivo maior proporcionar suporte no processo ensino-aprendizagem desenvolvido nos cursos. Os Laboratórios de Informática ficarão disponíveis aos usuários de acordo com os horários fixados na entrada do local ou através de reserva prévia.

O acesso aos Laboratórios de Informática fica restrito as pessoas habilitadas e qualificadas para fazer o uso adequado e sem ônus para a Instituição, sendo vedada a utilização em atividades que se afastem do objetivo maior.

A utilização dos Laboratórios de Informática será de inteira responsabilidade do professor orientador e dos alunos, no período no qual estiverem fazendo uso da sala e não houver um profissional responsável no local.

Para o funcionamento dos Laboratórios de Informática da Universidade, os usuários ficam proibidos de realizar quaisquer dos itens abaixo relacionados:

a) Instalar *softwares* e jogos de qualquer natureza;
b) Executar *softwares* que não sejam os instalados nos equipamentos;
c) Mudar as configurações das estações de trabalho;
d) Trocar os periféricos *(mouse*, teclado, monitor de vídeo, cabos, etc.) ou equipamentos de lugar;
e) Acessar a sites de conteúdo pornográfico;
f) Acessar a recursos de bate-papo;
g) Consumir alimentos, bebidas ou cigarros;
h) Retirar material ou equipamento do Laboratório;

Qualquer indisciplina, insubordinação ou desrespeito às normas vigentes, poderão implicar nas penalidades previstas nas Normas de Aplicação de Medidas Disciplinares.

Cada usuário é responsável pelo equipamento no período em que estiver fazendo uso deste. Visando preservar a integridade do patrimônio, qualquer dano causado por uso indevido devera ser ressarcido pelo causador do mesmo.

Frederico Westphalen, 24 de agosto de 2011.

Direção URI - Câmpus de Frederico Westphalen Comitê de Segurança da Informação

NORMAS DE SEGURANÇA INTERNA PARA A UTILIZAÇÃO DOS RECURSOS DE TI

URI - Campus de Frederico Westphalen

O objetivo das Normas de Segurança Interna para a Utilização dos Recursos de TI é garantir que os recursos de informática e a informação da Universidade Regional Integrada - URI - Campus de Frederico Westphalen estão sendo utilizados de forma adequada e segura. Para isso, é necessário que o usuário conheça todas as regras, evitando a exposição de qualquer informação que possa prejudicar a Instituição, seus Professores, Funcionários Técnico-Administrativos e Alunos.

A seguir serão detalhadas as normas que deverão ser seguidas pelos usuários da Universidade.

1. NORMAS DE UTILIZAÇÃO DE SOFTWARE(PROGRAMAS)

A Universidade Regional Integrada do Alto Uruguai e das Missões - URI - Campus de Frederico Westphalen disponibiliza para seus usuários um conjunto de *softwares* exclusivamente para o desempenho de suas atividades acadêmicas e administrativas.

É vedada ao usuário a instalação e execução de qualquer *software*, sem autorização prévia do Setor de TI. Todos os *softwares* instalados e executados nos computadores da Universidade devem ser devidamente licenciados, e o uso de qualquer *software* que não seja autorizado e/ou que viole os direitos do autor do programa de computador, são terminantemente proibidos.

Não são permitidas cópias ou distribuição de *softwares* licenciados à Universidade.

2. NORMAS DE UTILIZAÇÃO DE *HARDWARE* (EQUIPAMENTOS)

A Universidade disponibiliza à seus usuários um conjunto de equipamentos e recursos de TI exclusivamente para o desempenho de suas atividades. Dessa forma, o uso inadequado desses equipamentos e para fins que não sejam os delineados pela Instituição, é proibido.

É vedado o uso de quaisquer equipamentos que não sejam de propriedade da URI para conexão na rede interna física.

É proibida a abertura de computadores para qualquer tipo de reparo, independente do local ou circunstância. A realização de qualquer modificação ou manutenção deverá sempre ser realizada pelos profissionais do Setor de TI, com o conhecimento do usuário ou do superior imediato.

O usuário deverá observar os seguintes cuidados na utilização dos equipamentos de TI da Instituição:

a) Desligar o equipamento no final do uso, ou em ausências prolongadas;
b) Efetuar *logoff* ou bloqueio de tela toda vez que não for mais utilizar o computador, ou for se ausentar da sala, evitando que terceiros usem o nome de usuário ilicitamente;

3. NORMAS DE UTILIZAÇÃO DA REDE

Esse tópico visa definir as normas de utilização da rede que abrange o *login* e manutenção de arquivos no servidor. Esses itens serão abordados para orientação a todos os usuários dos sistemas e da rede de computadores da Universidade Regional Integrada - URI - Campus de Frederico Westphalen.

3.1 Regras Gerais de Segurança

Não são permitidas tentativas de obter acesso não autorizado, tais como, tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.

Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor, rede ou estação de trabalho. Isso inclui ataques, tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor.

Não são permitidas alterações das configurações de rede e inicialização dos computadores, bem como, modificações que possam trazer algum problema futuro. Não é permitido nenhum tipo de acesso remoto a estrutura interna, exceto os serviços disponibilizados pela instituição.

A Universidade disponibiliza acesso a rede *wireless.* Esse acesso é estabelecido pela autenticação da estrutura de rede. A rede *wireless* terá apenas a disponibilidade de acesso a páginas web e serviço FTP.

Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas. As áreas de armazenamento de arquivos são designadas conforme mostra a tabela a seguir:

Compartilhamento	Utilização
Diretório pessoal (H:)	Arquivos pessoais de responsabilidade do usuário.
Diretório público (X:)	Arquivos de compartilhamento geral, para todos os usuários.

O diretório *público* ou similar não deverá ser utilizado para o armazenamento de arquivos que contenham assuntos sigilosos. Devem ser armazenadas apenas informações comuns a todos. Não é permitido gravar arquivos de vídeo e áudio no servidor de arquivos. Isso tanto no servidor administrativo, quanto nos Laboratórios de Informática.

Os arquivos gravados em diretórios públicos podem ser acessados por todos os usuários que utilizarem a rede, portanto não se pode garantir sua integridade e disponibilidade. Estes arquivos poderão ser alterados ou excluídos sem prévio aviso e por qualquer usuário.

Os usuários deverão realizar manutenção no diretório pessoal, evitando acúmulo de arquivos desnecessários. Haverá limpeza semanal dos arquivos armazenados no diretório *público*, para que não haja acúmulo desnecessário de arquivos.

3.2 Regras para Professores e Funcionários Técnico-Administrativos

É obrigatório armazenar os arquivos inerentes à empresa no servidor de arquivos, para garantir a cópia de segurança dos mesmos.

Quando um Professor ou Funcionário Técnico-Administrativo é transferido entre departamentos, o coordenador deverá informar o Setor de TI sobre a mudança e qual modificação necessária que deverá ser realizada para sua nova função.

Quando ocorrer a demissão do Professor ou Funcionário Técnico-Administrativo, o Setor de Recursos Humanos deverá informar o Setor de TI para a imediata desativação dos acessos do usuário a qualquer recurso da rede. Deve-se verificar a necessidade de troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações.

3.3 Regras para Alunos

Todos os alunos regularmente matriculados na Universidade terão acesso à rede através de usuário e senha fornecida no ato da matrícula.

4. NORMAS DE ADMINISTRAÇÃO DE CONTAS DE USUÁRIOS

Essa norma é dividida por perfil de usuários, abrangendo a criação e manutenção de das contas, cotas de impressão e permissões que os usuários da Universidade possuem.

4.1 Perfil - A: Usuário Administrador

Compreendem-se como usuário Administrador, os membros do Setor de Gerência de Redes.

4.1.1 Permissões do perfil

- Acesso a Internet e Intranet;
- Acesso e gerenciamento total dos recursos e serviços de rede;
- Acesso total a dados e informações dentro da Intranet;
- Acesso e administração de bancos de dados;
- Instalação e configuração de sistemas operacionais, aplicativos e *softwares;*
- Administração de computadores servidores e clientes;
- Gerenciamento da Intranet e o acesso a Internet;
- Criação e alteração de contas e senhas de usuários de Administradores, Desenvolvedores, Professores, Funcionários, Alunos e de Projeto;

4.1.2 Criação e Alteração de Usuário Administrador

A criação e exclusão do usuário Administrador serão realizadas apenas pelo Setor de Gerência de Redes. Assim como a alteração e delegação de permissões e alteração de senha.

4.1.3 Impressão

As cotas de impressão para o usuário Administrador é de caráter destinado a funções internas e profissionais, sendo assim contabilizada de forma quantitativa e não monetária.

4.2 Perfil - B: Usuário Desenvolvedor

Consideram-se como usuário Desenvolvedor, os membros do Setor de Desenvolvimento de Sistemas.

4.2.1 Permissões do perfil

- Acesso a Internet e Intranet;
- Acesso e administração de bancos de dados;
- Criação de contas e alteração de senhas de usuários de Professores, Funcionários e Alunos;
- Acesso a documentos do seu respectivo usuário em unidade local ou remota;
- Acesso aos documentos do setor e outros setores específicos para a realização do trabalho;
- Instalação e configuração de sistemas operacionais, aplicativos e softwares;

4.2.2 Criação e Alteração de Usuário Desenvolvedor

A criação e exclusão do usuário Desenvolvedor serão realizadas apenas pelo Setor de Gerência de Redes. Assim como a alteração e delegação de permissões e alteração de senha.

4.2.3 Impressão

As cotas de impressão para o usuário Desenvolvedor é de caráter destinado a funções internas e profissionais, sendo assim contabilizada de forma quantitativa e não monetária.

4.2.4 Domínio

O grupo de usuários pertencentes ao perfil Desenvolvedor, assim como os respectivos computadores se enquadrarão ao domínio de rede a qual se destinará seu desenvolvimento.

4.3 Perfil - C: Usuário Suporte

Os funcionários técnico-administrativos e estagiários do Setor de Suporte a Computadores da Universidade são membros deste grupo;

4.3.1 Permissões

- Acesso a Internet e Intranet;
- Instalação e configuração de sistemas operacionais, aplicativos e softwares;
- Administração de computadores clientes;

4.3.2 Criação e Alteração de Usuário Suporte

A criação e exclusão do Usuário Suporte serão realizadas apenas pelo Setor de Gerência de Redes. Assim como a alteração e delegação de permissões e alteração de senha.

4.3.3 Cotas de impressão

As cotas de impressão para o usuário Suporte é de caráter destinado a funções internas e profissionais, sendo assim contabilizada de forma quantitativa e não monetária.

4.3.4 Domínio

O grupo de usuário pertencente ao perfil Suporte, assim como os respectivos computadores se enquadrarão ao domínio PROTEUS.

4.4 Perfil - D: Usuário Professor

Compreendem-se como usuário Professor, os empregados que exercem a função de professor da Universidade.

4.4.1 Permissões

- Acesso a Internet e Intranet;
- Acesso a documentos do seu respectivo usuário em unidade local ou remota;
- Acesso a documentos do setor;
- Acesso e utilização de aplicativos e softwares instalados e configurados pelo setor de Suporte;

4.4.2 Criação e Alteração de Usuário Professor

A criação do usuário Professor será realizada somente pelo Setor de Gerência de Redes. A alteração de senha será realizada através dos métodos destinados a esse fim no sistema URInet, ou pessoalmente portando um documento de identificação (RG ou CPF) no Setor de Gerencia de Redes da URI Campus de Frederico Westphalen.

A desativação da conta será realizada automaticamente pelo sistema, ou manualmente pelo Setor de Gerência de Redes, se o Setor de Recursos Humanos constatarem que o funcionário não possuir mais vínculo como a Universidade. O perfil do usuário constando dados e informações serão excluídas em um período estipulado de acordo com as leis cabíveis.

4.4.3 Impressão

As cotas de impressão para o Usuário Professor é de caráter destinado a funções internas e profissionais, sendo assim contabilizada de forma quantitativa e não monetária.

4.4.4 Domínio

O grupo de usuário pertencente ao perfil Professor, assim como os respectivos computadores se enquadrarão ao domínio PROTEUS.

4.4.5 Armazenamento

O usuário que pertencente ao perfil Professor tem direito a 300 MB (Mega Bytes) de armazenamento em seu diretório pessoal (H).

Outras formas de armazenamento como unidades móveis (pendrive, CD/DVD, disquete, entre outros) e unidade local (HD) serão limitadas de acordo com a capacidade desses dispositivos.

4.5 Perfil - E: Usuário Funcionário

Os empregados da Universidade que exercem atividades técnico-administrativas fazem parte deste perfil.

4.5.1 Permissões

- Acesso a Internet e Intranet;
- Acesso apenas a documentos do seu respectivo usuário em unidade local ou remota;
- Acesso a documentos do setor em unidade local ou remota se assim disponível;
- Acesso e utilização de aplicativos e softwares instalados e configurados pelo setor de Suporte;

4.5.2 Criação e Alteração de Usuário Funcionário

A criação do usuário Funcionário será realizada somente pelo Setor de Gerência de Redes.

A alteração de senha será realizada através dos métodos destinados a esse fim no sistema URInet, ou pessoalmente portando um documento de identificação (RG ou CPF) no Setor de Gerência de Redes da URI Campus de Frederico Westphalen.

A desativação da conta será realizada automaticamente pelo sistema, ou manualmente pelo Setor de Gerência de Redes, se o Setor de Recursos Humanos constatarem que o funcionário não possuir mais vínculo como a Universidade. O perfil do usuário constando dados e informações serão excluídas em um período estipulado de acordo com as leis cabíveis.

4.5.3 Impressão

As cotas de impressão para o Usuário Funcionário é de caráter destinado a funções internas e profissionais, sendo assim contabilizada de forma quantitativa e não monetária.

4.5.4 Domínio

O grupo de usuário pertencente ao perfil Funcionário, assim como os respectivos computadores se enquadrarão ao domínio PROTEUS ou TELLUS, dependendo das atividades que desempenham.

4.5.5 Armazenamento

O usuário que pertencente ao perfil Funcionário tem direito a 200 MB (Mega Bytes) de armazenamento em seu diretório pessoal (H).

Outras formas de armazenamento como unidades móveis (pendrive, CD/DVD, disquete, entre outros) e unidade local (HD) serão limitadas de acordo com a capacidade desses dispositivos.

4.6 Perfil - F: Usuário Aluno

Compreendem-se como usuário Aluno, todos os alunos regularmente matriculados na Universidade.

4.6.1 Permissões

- Acesso a Internet e Intranet;
- Acesso a documentos do seu respectivo usuário em unidade local ou remota;
- Acesso e utilização de aplicativos e softwares instalados e configurados pelo Setor de Suporte;

4.6.2 Criação, Exclusão e Alteração de Usuário Aluno

A criação do usuário Aluno será realizada automaticamente pelo sistema.

A alteração de senha será realizada através dos métodos destinados a esse fim no sistema URInet, ou pessoalmente portando um documento de identificação (RG ou CPF) no Setor de TI da URI Campus de Frederico Westphalen.

A desativação será realizada automaticamente pelo sistema, ou manualmente pelo administrador da rede, se o mesmo constatar que o aluno não possuir mais vínculo como a Universidade. O perfil do usuário constando dados e informações serão excluídas em um período estipulado de acordo com as leis cabíveis.

4.6.3 Impressão

As cotas de impressão para o Usuário Aluno são contabilizadas de forma quantitativa e monetária de acordo com o valor estipulado pelo Setor Financeiro da Universidade.

O aluno que desejar imprimir deverá adquirir as cotas de impressão na Tesouraria da Instituição. A impressão somente poderá ser realizada através dos computadores dos laboratórios de informática da URI.

4.6.4 Domínio

O grupo de usuário pertencente ao perfil Aluno, assim como os respectivos computadores se enquadrarão ao domínio OCEANUS.

4.6.5 Armazenamento

O usuário que pertencente ao perfil Aluno tem direito a 100 MB (Mega Bytes) de armazenamento em seu diretório pessoal (H).

Outras formas de armazenamento como unidades móveis (pendrive, CD/DVD, disquete, entre outros) e unidade local (HD) serão limitadas de acordo com a capacidade desses dispositivos.

4.7 Perfil - G: Usuário de Projeto

Compreende-se como usuário Projeto, todos os terceiros ou vigentes em programas e projetos da URI, que necessitem de acesso aos recursos de rede.

4.7.1 Permissões

- Acesso a Internet;

4.7.2 Criação, Exclusão e Alteração de Usuário de Projeto

A criação do Usuário de Projeto será realizada apenas pelo Setor de Gerência de Redes. Assim como a alteração e delegação de permissões e alteração de senha. A alteração

de senha será realizada apenas pessoalmente, tendo que o usuário portar um documento de identificação (RG ou CPF).

A desativação será realizada automaticamente pelo sistema, ou manualmente pelo Setor de Gerência de Redes, se o mesmo constatar que o usuário não possui mais vínculo como a Universidade. O perfil do usuário constando dados e informações serão excluídas em um período estipulado de acordo com as leis cabíveis.

4.7.3 Impressão

As cotas de impressão para o Usuário de Projeto é de caráter destinado a funções acadêmicas e educacionais, sendo assim contabilizada de forma quantitativa e monetária de acordo com o valor estipulado pelo Setor Financeiro da Universidade.

4.7.4 Domínio

O grupo de usuário pertencente ao perfil Projeto, assim como os respectivos computadores se enquadrarão ao domínio OCEANUS.

4.7.5 Armazenamento

O usuário que pertencente ao perfil Projeto tem direito a 100 MB (Mega Bytes) de armazenamento em seu diretório pessoal (H).

Outras formas de armazenamento como unidades móveis (pendrive, CD/DVD, disquete, entre outros) e unidade local (HD) serão limitadas de acordo com a capacidade desses dispositivos.

5. NORMAS DE SENHAS

As senhas são utilizadas para o acesso a rede, sistemas e serviços da Universidade Regional Integrada - URI - Campus de Frederico Westphalen, que necessitem de autenticação. As senhas para os serviços disponibilizadas pela Universidade devem ser sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese.

As responsabilidades do usuário incluem, principalmente, os cuidados para a manutenção da segurança dos recursos, tais como, sigilo da senha e o monitoramento de sua conta, evitando sua utilização indevida.

Tudo o que for executado com a senha de usuário da rede, ou de outro sistema será de inteira responsabilidade do usuário, por isso a necessidade de todo o cuidado de se manter a senha secreta.

As senhas tornam-se efetivas quando usadas corretamente, e requerem alguns cuidados na sua escolha e uso, como:

I) Adotar senha da conta com quantidade mínima de 08 (oito) caracteres, combinando letras, números e caracteres especiais, em grafia maiúscula e minúscula, seguindo o conceito de senha forte, a seguir detalhado;
II) Trocar a senha a cada 3 (três) meses ou sob qualquer suspeita de uso de seu login por terceiros.
1. Os usuários devem seguir as seguintes normas para escolha de senhas, adotando o conceito de senha forte:
I) Não utilizar como senha o nome de sua conta de rede, ou qualquer variação do mesmo (invertido, com letras maiúsculas, duplicado, etc.);
II) Não utilizar como senha qualquer um de seus nomes ou sobrenomes, ou qualquer variação destes;
III) Não utilizar como senha qualquer informação a seu respeito que possa ser facilmente obtida (placa de automóvel, número de telefone, nome de pessoas de sua família, data de nascimento, endereço, etc.);
IV) Não utilizar como senha apenas números, ou repetições de uma mesma letra;

A senha pode ser alterada através do sistema URInet ou pessoalmente no Setor de TI, munido de documento de identificação. Não serão alteradas senhas por telefone.

6. NORMAS DE UTILIZAÇÃO DE E-MAIL

O e-mail disponibilizado pela URI deve ser utilizado apenas para as atividades relacionadas com os objetivos que a Universidade se apóia. Para a utilização do e-mail da instituição é necessário que o usuário aceite os termos de uso junto ao Gmail da Google.

O serviço de e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens.

É proibido o envio de mensagens de e-mail, caracterizadas como spam, que de acordo com a capacidade técnica da rede, seja prejudicial ou gere reclamações de outros usuários, salvo em caso de solicitações e aprovação do Setor de TI.

É aconselhável a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis.

Não execute ou abra arquivos anexados enviados por emitentes desconhecidos ou suspeitos. Não abra arquivos anexados com as extensões .bat, .exe, .src, .lnk, .bin e .com, se não tiver certeza absoluta de quem enviou este e-mail.

São considerados assuntos proibidos para o envio de e-mais:

I) Propaganda político partidária;
II) Propaganda com finalidades comerciais;

III) Pornografia e de caráter sexual;
IV) Pornografia infantil (pedofilia);
V) Terrorismo;
VI) Drogas;
VII) Crackers ou programas de códigos maliciosos;
VIII) Sites de relacionamento;
IX) Jogos;
X) Violência e Agressividade (racismo, preconceito, etc.);
XI) Violação de direito autoral (pirataria, etc.);
XII) Áudio e Vídeo, salvo com conteúdo relacionado, diretamente, a URI;
XIII) Conteúdo impróprio, ofensivo, ilegal, discriminatório, e similares.
XIV) Correntes (ajuda a pessoas, aviso de vírus, forma de ganhar dinheiro, etc.)

A Instituição não se responsabiliza pela indisponibilidade do serviço de e-mail, haja visto que a estrutura está vinculada ao Gmail da Google.

7. NORMAS DE ACESSO A INTERNET

A Internet é uma ferramenta de trabalho e pesquisas que deve ser utilizada para esse fim pelos professores, funcionários técnico-administrativos e alunos da Universidade Regional Integrada do Alto Uruguai e das Missões - URI - Campus de Frederico Westphalen. Não é permitido o seu uso para fins pessoais ou recreativos em horários de trabalho ou de aula.

É proibida a divulgação de informações confidenciais da Universidade Regional Integrada -URI - Campus de Frederico Westphalen em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo passível sofrer as penalidades previstas na Norma de Aplicação de Medidas Disciplinares e/ou na forma da Lei.

O envio e recepção de informações digitais devem ser racionalizados, evitando excessos que sobrecarreguem a rede e provoquem lentidão na transmissão e recepção de informações e prejuízo para a Universidade.

Os downloads de arquivos da Internet devem ser realizados através de sites confiáveis e somente os que sejam necessários ao desempenho das atividades.

Não será permitida a utilização de serviços de streaming, tais como, rádios on-line.

Poderão ser bloqueados arquivos e/ou domínios que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos.

Todo acesso dos usuários a sites será armazenado na forma de log, possibilitando auditorias futuras.

Não é permitido burlar a estrutura de TI da Instituição.

8. NORMAS DE UTILIZAÇÃO DA REDE WIRELESS

A utilização da rede wireless engloba os seguintes itens:

I) O acesso a rede wireless é permitido apenas para alunos regularmente matriculados, professores e funcionários da Instituição, exigindo login e senha, já utilizados no portal URInet;
II) Não é permitida tentativa de acesso não autorizado em qualquer servidor, rede ou conta de usuário da Instituição ou terceiros;
III) Não é permitida tentativa de interferir no serviço de qualquer outro usuário, servidor ou rede. Isso inclui ataque do tipo "negação de serviço", provocar congestionamento em rede wireless, tentativa deliberada de sobrecarregar o serviço e tentativa de invasão de um servidor;
IV) Não são permitidas alterações das configurações básicas de rede (IP, Gateway, DNS, etc.);
V) É proibida a instalação de qualquer Router, Access Point ou equipamento de propagação de sinal nas instalações da Instituição;

Responsabilidades:

I) A URI Campus de Frederico Westphalen não se responsabiliza por danos de software ou hardware causados em qualquer equipamento que utiliza este serviço, tais como perda de dados, roubo de informações, violação de acesso, queima de dispositivos, ou quaisquer outros eventos que podem acontecer utilizando a estrutura;
II) O usuário será responsabilizado por qualquer dano causado à rede onde suas credenciais estiverem contidas em logs de acesso;
III) O setor de Gerência de Redes da URI é responsável e único habilitado a realizar a configuração e instalação de Routers e Access Point que possam prover acesso à rede;
IV) O Setor de Gerência de Redes poderá intervir e interromper acessos para manutenções na rede a qualquer momento sem comunicação prévia;
V) Por questões de segurança, só é permitido o acesso à sites para busca de informações de âmbito acadêmico, ficando proibido qualquer tipo de acesso à conteúdos indevidos, tais como:
    - Sites pornográficos e de caráter sexual;
    - Compartilhamento de arquivos (ex.: peer to peer);
    - Pornografia infantil (pedofilia);
    - Terrorismo;
    - Drogas;
    - Sites de códigos maliciosos (vírus e malwares);

- Sites de relacionamento;
- Jogos;
- Violência e agressividade (racismo, preconceito, etc.);
- Violação de direito autoral (pirataria, etc.);
- Áudio e Vídeo, salvo com conteúdo relacionado, diretamente a URI e liberado pelo COMITÊ DE SEGURANÇA DA INFORMAÇÃO;
- InstantMessenger (MSN, meebo, webmessenger, etc.).
- Propaganda político partidária;
- Conteúdo impróprio, ofensivo, ilegal, discriminatório, e similares.

VI) O acesso à internet durante os horários das aulas, somente pode ocorrer mediante autorização do professor e seu conteúdo compatível com a aula;

VII) É terminantemente proibido desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas em qualquer servidor localizado fora ou dentro da estrutura da URI, tais como:

- Criação e propagação de vírus e worms;
- Criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados;
- Engajar-se em ações que possam ser caracterizadas como violação da segurança computacional;
- Envios de mala direta ou disparo de e-mails;
- Quaisquer outros tipos de ataques à serviços, servidores e/ou qualquer outro dispositivo não importando o proposito do feito.

9. NORMAS DO USO DE IMPRESSORAS

Esse tópico visa definir as normas de utilização de impressoras disponíveis nos departamentos da Universidade Regional Integrada - URI - Campus de Frederico Westphalen.

9.1 Regras Gerais

O uso das impressoras deve ser feito exclusivamente para impressão de documentos ou outras informações que sejam de interesse da Universidade ou que estejam relacionados com o desempenho de suas atividades acadêmicas.

O usuário deve ter o cuidado de retirar com a maior brevidade da impressora os documentos que tenha solicitado a impressão que contenham informações sensíveis da Instituição. Impressões que contenham informações sensíveis que não tenham mais utilidade devem ser destruídas, visando preservar o sigilo.

Não é permitido deixar impressões de qualquer informação junto às impressoras. A Universidade, em cumprimento ao seu compromisso com a responsabilidade social, recomenda que sejam impressos apenas documentos indispensáveis, devendo os demais ser lidos na própria tela do computador.

10. NORMAS DE SEGURANÇA FÍSICA

O objetivo desta norma é prevenir o acesso não autorizado, dano e interferência às informações e instalações físicas da Universidade. A segurança física dos equipamentos de TI e das informações da Instituição deve ser protegida de possíveis danos.

As instalações do Setor de TI devem minimizar acesso público direto, riscos ao fornecimento de energia e serviços de telecomunicações. Apenas pessoas autorizadas podem acessar as instalações do Setor de TI, devendo esses utilizar crachás de identificação.

Nos departamentos que tratam com informações confidenciais, como, por exemplo, documentação, informações financeiras, acadêmicas, o acesso deve ser permitido somente para pessoas autorizadas.

Empresas terceirizadas, que necessitarem acesso a áreas restritas ou equipamentos de TI, devem assinar Termo de Visita e Utilização de Equipamentos, informando a finalidade, o tempo de acesso às áreas restritas, os profissionais e recursos envolvidos, de acordo com o Anexo II.

11. TERMO DE COMPROMISSO

O termo de compromisso é utilizado para que os professores, funcionários técnico-administrativos e alunos da Universidade Regional Integrada do Alto Uruguai e das Missões - URI -Campus de Frederico Westphalen se comprometam formalmente a seguir a Política de Segurança da Informação, tomando ciência das punições impostas ao seu não cumprimento.

O documento deve ser assinado por todos os professores, funcionários técnico-administrativos, e será renovado sempre que necessário, conforme Anexo I.

Os alunos da Instituição, através da assinatura do Contrato de Prestação de Serviços Educacionais firmará compromisso em seguir a Política de Segurança da Informação e suas normas.

12. VERIFICAÇÃO DA UTILIZAÇÃO DA POLÍTICA

Para garantir o cumprimento das normas mencionadas acima, a Universidade Regional Integrada do Alto Uruguai e das Missões - URI - Campus de Frederico Westphalen se reserva no direito de:

I) Implantar sistemas que possibilitem monitorar e gravar todos os acessos à Internet e computadores da Instituição.
II) Auditar qualquer arquivo armazenado na rede, tanto no disco local do computador ou nas áreas privadas da rede, visando assegurar o cumprimento desta política.

13. REVISÕES E COMENTÁRIOS FINAIS

A Universidade Regional Integrada do Alto Uruguai e das Missões - URI - Campus de Frederico Westphalen se reserva ao direito de revisar, adicionar ou modificar essa Norma de Segurança para aprimorar e garantir o perfeito funcionamento das normas e regras por ele definidas.

Essa revisão, adição ou modificação será notificada aos usuários com antecedência, exceto em situações emergenciais.

14. ENCERRAMENTO

Os casos omissos e esclarecimentos da Política de Segurança da Informação, bem como normas regulamentares, deverão ser encaminhados ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO para avaliação em conjunto com a Direção e posterior recomendação de como proceder.

Ademais, todas as normas e procedimentos acima não se esgotam neste instrumento, sobretudo em razão da constante evolução tecnológica, não consistindo em rol enumerativo, motivo pelo qual é obrigação do COMITÊ DE SEGURANÇA DA INFORMAÇÃO, bem como dos usuários adotar todo e qualquer procedimento de segurança que esteja ao seu alcance, visando sempre proteger as informações da Instituição.

Para publicidade e conhecimento geral dos usuários da Universidade, este documento será publicado na rede interna.

A presente política passa a vigorar a partir da data de sua aprovação sendo válida por tempo indeterminado.

Frederico Westphalen - RS, 24 de agosto de 2011.

Direção URI - Câmpus de Frederico Westphalen **Comitê de Segurança da Informação**

NORMAS DE APLICAÇÃO DE MEDIDAS DISCIPLINARES

URI - Campus de Frederico Westphalen

A FuRI - Fundação Regional Integrada, mantenedora da Universidade Regional Integrada do Alto Uruguai e das Missões - URI - Campus de Frederico Westphalen, através das Normas de Aplicação de Medidas Disciplinares, visa aplicar as medidas cabíveis em caso de não cumprimento da Política de Segurança da Informação, bem como de suas normas.

A Universidade ao detectar uma violação irá determinar a sua razão, ou seja, verificar se a infração pode ter ocorrido por negligência, acidente ou erro, por desconhecimento da política ou por ação previamente determinada, ignorando a política estabelecida.

Um processo de esclarecimento deve determinar as circunstâncias da violação, como e porque ela ocorreu. Verificando-se alguma inconformidade com a Política de Segurança da Informação e suas normas, o infrator será comunicado da punição, como descrito a seguir.

Regras para Professores e Funcionários Técnico-Administrativos

Caso seja necessário advertir o professor ou funcionário técnico-administrativo, o departamento de Recursos Humanos será informado a fim de interagir e manter-se informado da situação.

O não cumprimento, pelo professor ou funcionário técnico-administrativo, das normas estabelecidas neste documento, seja isolada ou acumulativamente, poderá causar, de acordo com a infração cometida, as seguintes punições:

- Comunicação de descumprimento
  O professor ou funcionário técnico-administrativo será convocado a comparecer ao departamento de Recursos Humanos e será comunicado sobre o descumprimento da Política e das Normas de Segurança da Informação, com a indicação precisa da violação praticada.
- Advertência ou suspensão
  A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade. Uma cópia dessa advertência deve ser acondicionada na pasta do professor ou funcionário técnico-administrativo, junto ao departamento de Recursos Humanos.
- Desligamento
  Nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, fica desde já estabelecido que a Direção da Universidade Regional Integrada do Alto Uruguai e das Missões - URI - Campus de Frederico Westphalen, no uso do poder diretivo e disciplinar que lhe é atribuído, poderá aplicar a pena que entender devida.

Regras para Alunos

Caso seja necessário advertir o aluno, a coordenação de curso será informada para interagir e manter-se informada da situação. O não cumprimento pelo aluno, das normas estabelecidas nesta Política de Segurança da Informação, seja isolada ou acumulativamente, poderá causar, de acordo com a infração cometida, as punições estabelecidas no Regimento Geral da URI, na Seção IV - Do Regime Disciplinar.

Frederico Westphalen - RS, 24 de agosto de 2011.

Direção URI - Câmpus de Frederico Westphalen	**Departamento de Recursos Hunanos**	**Comitê de Segurança da Informação**

Anexo I

Termo de Compromisso para Professores e Funcionários Técnico-Administrativos

TERMO DE COMPROMISSO

Eu,_____ empregado da FuRI - Fundação Regional Integrada, mantenedora da Universidade Regional Integrada do Alto Uruguai e das Missões - URI - Câmpus de Frederico Westphalen, inscrito com n° de CPF _____ e RG n°_____ AFIRMO QUE ESTOU CIENTE E COMPROMETO-ME a cumprir a Política de Segurança da Informação e a utilizar os recursos de TI apenas para desenvolver as atividades da Universidade.

Frederico Westphalen - RS, ____ de _____ de 20___.

_____

Assinatura

Anexo II

Termo de Visitas e Utilização de Equipamentos de TI

TERMO DE VISITAS E UTILIZAÇÃO DE EQUIPAMENTOS DE TI

Solicitamos a FuRI - Fundação Regional Integrada, mantenedora da Universidade Regional Integrada do Alto Uruguai e das Missões - URI - Campus de Frederico Westphalen a cedência dos equipamentos e áreas de TI para a prestação dos serviços a seguir descritos.

A serviço:	Telefone:
Requerente:	Responsável:
Acesso a áreas restritas: □ Sim □ Não	Quais:
Descrição do Serviço:	

Profissionais Envolvidos	
Nome	RG
Período de Utilização	
Início: ___/___/_____ ___:___	Término: ___/___/_____ ___:___
Equipamentos Utilizados:	

Afirmamos que estamos cientes da Política e das Normas de Segurança da Informação desta Instituição, bem como assumimos responsabilidade pelo seu cumprimento.

Frederico Westphalen - RS, _____ de _____ de 20_____.

_____ _____

Assinatura do Requerente Assinatura do Funcionário da FuRI

Anexo III

Termo de Doações de Equipamentos de TI

Termo de Doações de Equipamentos de TI

Eu,_____, inscrito com n° de CPF _____ e RG n° _____ CONFIRMO A DOAÇÃO DOS EQUIPAMENTOS de minha propriedade, a seguir descritos, para o uso incondicional e definitivo à FuRI - Fundação Regional Integrada, mantenedora da Universidade Regional Integrada do Alto Uruguai e das Missões - URI - Câmpus de Frederico Westphalen. Estou ciente que os equipamentos doados deverão obedecer a Política e as Normas de Segurança da Informação da Universidade.

Quantidade	Descrição do Equipamento

Frederico Westphalen - RS, _____ de _____ de 20_____.

_____

Assinatura do Doador

Anexo IV

Solicitação para Alteração de Localização de Equipamentos de TI

Solicitação para Alteração de Localização de Equipamentos de TI

Requerente:	
Setor:	Telefone:
Equipamentos a serem alterados:	
Local atual:	Local pretendido:
Motivo da alteração:	

Frederico Westphalen - RS, _____ de _____ de 20_____.

_____ _____

Assinatura do Solicitante Assinatura do Responsável do Setor

Anexo V

Solicitação para Reservas de Equipamentos de TI

Solicitação para Reservas de Equipamentos de TI

Requerente:	
Setor:	Telefone:
Finalidade da Reserva:	
Início: ___/___/_____ ___:___	Término: ___/___/_____ ___:___
Local:	
Equipamentos necessários:	

Frederico Westphalen - RS, _____ de _____ de 20_____.

_____

Assinatura do Requerente