RESOLUÇÃO N.º 813 DE 08 DE FEVEREIRO DE 2013

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO, no uso de suas atribuições regulamentares resolve:

Aprovar "*ad referendum*" a Política de Segurança da Informação do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo.

ARNALDO AUGUSTO CIQUIELO BORGES

Aprovada pela Resolução nº. 813
de 08 de fevereiro de 2013

Instituto Federal de Educação Ciência e Tecnologia de São Paulo

Política de Segurança da Informação

São Paulo, Fevereiro de 2013.

Arnaldo Augusto Ciquielo Borges
Reitor

Luciana de Oliveira Sakamoto Silva
Procuradora Federal

Comitê de Política de Segurança da Informação
Anne Camila Knoll Domenici (*Campus* Sertãozinho)
Diego Cesar Valente E. Silva (Reitoria)
Dirlei Paulino Pinto (*Campus* Boituva)
Edgar Noda (*Campus* Hortolândia)
Flávio Kyoshi Saito (Reitoria)
Fernando de Jesus Flores Parreira (*Campus* Votuporanga)
João Paulo Dal Poz Pereira (*Campus* Cubatão)
João Paulo Lemos Escola (*Campus* Barretos)
Kleber Manrique Trevisani (*Campus* Presidente Epitácio)
Paulo Orlando Ricarte Kawachi (Reitoria)
Paulo Roberto de Abreu (*Campus* São Paulo)
Roan Simões da Silva (*Campus* São João da Boa Vista)
Rodolfo Francisco de Oliveira (*Campus* Hortolândia)
Silvan Amaro Oliveira (*Campus* São Roque)

Sumário

1. Apresentação 4
2. Introdução 4
3. Objetivo 4
4. Abrangência 5
5. Segurança da Informação 5
6. Infrações 5
7. Penalidades 5
8. Órgãos, Comissões, Grupos e Pessoas Responsáveis pela Política de Segurança da Informação e suas Atribuições 6
    8.1. Conselho Superior 6
    8.2. Colégio de Dirigentes 6
    8.3. Comitê de Política de Segurança da Informação 6
    8.4. Diretoria de Infraestrutura e Rede 6
    8.5. Diretoria de Sistemas de Informação 6
    8.6. Procuradoria Federal 6
    8.7. Administrador de Computadores Servidores, Sistemas Computacionais e Infraestrutura de Rede 6
    8.8. Alunos, Servidores e demais pessoas que usam, têm ou terão contato com qualquer Ativo Protegido por esta Política 6
9. Normas de Segurança da Informação 7
    NormaSeg01 8
    NormaSeg02 12
    NormaSeg03 15
    NormaSeg04 19
    NormaSeg05 23
    NormaSeg06 26

1. Apresentação

Este documento foi elaborado pelo Comitê de Política de Segurança da Informação do IFSP, formado por indicação do Comitê de Tecnologia da Informação no dia 6 de junho de 2012, com as seguintes atribuições:

- Elaborar a Política de Segurança da Informação que dê sustentação às atividades de proteção das informações do Instituto;
- Propor o plano de melhoria de Segurança da Informação de acordo com a norma ISO/IEC 27005:2005.

O documento aborda a Segurança da Informação no Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - IFSP - em seus diversos aspectos, apresentando recomendações e ações que devem ser seguidas de forma a preservar o patrimônio, a informação e a reputação do IFSP.

Essa política deve ser revisada e atualizada anualmente.

2. Introdução

No IFSP são tratados diversos tipos de informações críticas, sendo essas diretamente relacionadas à atividade fim, como informações acadêmicas dos alunos ou administrativas que influenciam na continuidade.

Essas informações circulam e são armazenadas em grandes volumes, tanto no ambiente interno como no externo do Instituto, em mídia física ou lógica.

Para isso, utiliza-se um grande número de ativos, essenciais para a atividade fim do Instituto e, assim sendo, os recursos computacionais, de rede e de comunicação do IFSP, os documentos físicos gerados ou não por recursos computacionais e a informação através desses recursos precisam ser protegidos, como qualquer outro ativo importante para o Instituto. Com relação à segurança da informação, esta Política será caracterizada pela tentativa de manter a confidencialidade, a integridade e a disponibilidade das informações, independentemente de onde elas estejam, residentes em memória de máquinas e dispositivos, armazenadas em disco, em trânsito ou impressas em documentos; salvaguardando a exatidão e completeza das mesmas e dos métodos de processamento e garantindo que a comunidade obtenha acesso à informação e aos ativos correspondentes sempre que necessário e de acordo com a permissão atribuída a cada um.

3. Objetivo

Este documento tem como objetivo específico definir uma Política de Segurança para o Instituto, estabelecendo procedimentos e recomendações visando a prevenir e responder a incidentes de segurança.

4. Abrangência

No escopo definido até a presente data para esta Política, são tratados os sistemas de informação e serviços de comunicação e colaboração considerados mais críticos, sendo estes o Sistema Integrado de Gestão Acadêmica, o sistema acadêmico NAMBEI, o serviço de e-mail institucional e os serviços de armazenamento e compartilhamento de arquivos SAMBA e Nuvem IFSP.

Os quesitos da Política de Segurança da Informação devem ser aplicados de maneira mandatória na Reitoria e em todos os *campi* do IFSP quando se tratar de sistema ou serviço centralizado e disponibilizado para todo o Instituto.

Dentro do escopo são tratadas a confidencialidade, a integridade e a disponibilidade das informações.

5. Segurança da Informação

Considera-se como segurança da informação a preservação da autenticidade, confidencialidade, integridade, disponibilidade, irretratabilidade e legalidade da informação do Instituto.

6. Infrações

As regras das normas de Segurança da Informação obedecem tanto a leis relacionadas com segurança da informação quanto à normatização nacional e internacional de Segurança da Informação.

Qualquer desobediência às normas de segurança é considerada infração contra esta Política de Segurança da Informação.

As recomendações contidas nas normas de Segurança da Informação são de caráter informativo e não serão consideradas infrações se estas não forem seguidas.

7. Penalidades

Se a infração cometida contra esta Política de Segurança da Informação estiver relacionada a uma lei penal, será considerada crime penal e o infrator será denunciado à autoridade competente.

Se a infração não se enquadrar na situação citada acima, o infrator poderá ser julgado e sofrer penalidade como uma infração de natureza ética.

8. Órgãos, Comissões, Grupos e Pessoas Responsáveis pela Política de Segurança da Informação e suas Atribuições.

8.1. Conselho Superior

Ao Conselho Superior compete aprovar esta política e normas anexadas.

8.2. Colégio de Dirigentes

Ao Colégio de Dirigentes compete apreciar e recomendar normas de aperfeiçoamento da gestão.

8.3. Comitê de Política de Segurança da Informação

Ao Comitê de Política de Segurança da Informação compete o disposto no item 1 deste documento.

8.4. Diretoria de Infraestrutura e Rede

É responsável pela infraestrutura de redes físicas e lógicas do IFSP, com o objetivo de viabilizar a disponibilidade da informação e comunicação.

Mantém a independência externa em relação à operação de equipamentos, dispositivos e serviços que promovam a segurança ou gerência da informação.

Propõe melhorias para esta política.

8.5. Diretoria de Sistemas de Informação

Mantém as atividades de desenvolvimento, manutenção e atualização dos sistemas institucionais, estabelecendo normas, políticas, ações, padrões, rotinas e procedimentos para os sistemas informatizados, a fim de garantir a disponibilidade, integridade e confidencialidade da informação em consonância com as necessidades do Instituto.

8.6. Procuradoria Federal

A Procuradoria Federal junto ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – PF/IFSP – é o órgão de execução da Procuradoria-Geral Federal incumbido de exercer atividades de consultoria e assessoramento jurídico do IFSP.

8.7. Administrador de Computadores Servidores, Sistemas Computacionais e Infraestrutura de Rede.

Pessoa indicada pela Diretoria de Infraestrutura e Rede ou pela Diretoria de Sistemas de Informação com a responsabilidade de zelar pelo cumprimento das normas de segurança da informação dentro do âmbito de suas atividades.

8.8. Alunos, Servidores e demais pessoas que utilizam, têm ou terão contato com qualquer ativo protegido por esta política

Cabe aos alunos, servidores e a todos que utilizam ou terão acesso aos ativos protegidos cumprir com as determinações da Política de Segurança da Informação do IFSP e sugerir propostas de melhoria para esta.

9. Normas de Segurança da Informação

As Normas de Segurança da Informação têm por objetivo estabelecer deveres e recomendar ações para os administradores e usuários dos ativos protegidos por esta política.

Essas normas devem ser revisadas e atualizadas quando ocorrerem mudanças com relação à segurança da informação ou quando for alterado o escopo desta política. As revisões e atualizações nas normas devem ser feitas independentemente das revisões e atualizações desta política.

Os documentos das normas de segurança anexados a esta política são:

NormaSeg01 - Norma de Segurança da Informação do serviço de e-mail institucional;

NormaSeg02 - Norma de Segurança da Informação do serviço LDAP;

NormaSeg03 - Norma de Segurança da Informação do Sistema Acadêmico NAMBEI;

NormaSeg04 - Norma de Segurança da Informação do serviço Nuvem IFSP;

NormaSeg05 - Norma de Segurança da Informação do serviço SAMBA;

NormaSeg06 - Norma de Segurança da Informação do Sistema Integrado de Gestão Acadêmica.

Órgãos, comissões, grupos e pessoas responsáveis pela Política de Segurança da Informação, relacionados nesta política, terão o prazo de 180 (cento e oitenta) dias, a partir de sua publicação, para se adequarem às normas de Segurança da Informação. Após este prazo, esta política entra em vigor.

NormaSeg01

Norma de Segurança da Informação do serviço de e-mail institucional

Apresentação

O serviço de e-mail do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo oferece aos usuários uma conta de correio eletrônico @ifsp.edu.br para comunicação autenticada interna e externa.

Objetivo e Abrangência

Este documento foi elaborado pelo Comitê de Política de Segurança da Informação e tem por objetivo estabelecer deveres para os administradores e usuários deste serviço, sendo mandatório para todo o IFSP.

Considerações de Segurança da Informação

O serviço de e-mail institucional poderá ser utilizado para envio de textos e documentos críticos e sensíveis e, portanto, requer a segurança dessas informações em termos de disponibilidade, integridade e confidencialidade, além de seu conteúdo ser considerado sigiloso pelo inciso XII, do artigo 5º da Constituição Federal.

A segurança de TI nesse serviço é implementada nos níveis de aplicação e de infraestrutura, cobrindo toda a área de TI.

Responsáveis

Diretoria de Infraestrutura e Rede - Responsável pela segurança física e de infraestrutura desse serviço.

Coordenadoria de Infraestrutura - Responsável pela segurança da plataforma, aplicação, controles de acesso e de serviços de rede.

Usuário - Responsável pela segurança da informação e pelo uso do serviço.

Regras de Segurança

1 - Da Operação

1.1 - O computador servidor desse serviço deve operar em conformidade com o acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.2 - O computador servidor desse serviço deve operar em um local com autonomia energética de 8 (oito) horas.
(Fulcro no item 9.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.3 - O computador servidor desse serviço deve operar em um local com certificado de infraestrutura segura contra ameaças naturais.
(Fulcro no item 9.1.4 da norma ABNT NBR ISO/IEC 27002:2005).

1.4 - A disponibilidade da aplicação desse serviço deve estar em conformidade com o acordo de nível de serviço.
1.4.1 - Os administradores do serviço e do computador servidor obedecerão aos procedimentos e ao acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.5 - O espaço em disco disponível para esse serviço deve ser suficiente para a necessidade do IFSP.

1.5.1 - Periodicamente a necessidade de espaço deve ser avaliada com todas as áreas de negócio e ser apresentado um relatório de avaliação de capacidade.

1.5.2 - O intervalo de avaliação deve ser definido pela Diretoria de Infraestrutura e Rede e executado pela Coordenadoria de Infraestrutura, não podendo ser superior a 2 (dois) anos e inferior a 6 (seis) meses.

1.5.3 - Se a Coordenadoria de Infraestrutura avaliar que há necessidade maior de espaço, em decorrência ou não do mau uso, deve ser apresentado um plano de ação com a finalidade de otimizar ou disponibilizar maior espaço para atender a essa necessidade.

(Fulcro no item 10.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.6 - O computador servidor desse serviço deve dispor de mecanismo de redundância, em caso falha em um dos discos, controlado via hardware.

1.6.1 - A conformidade com o item 1.6 garante que, em casos específicos de falha de disco, a quebra da disponibilidade do dispositivo de armazenamento não viole o acordo de nível de serviço.

(Fulcro no item 10.5.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.7 - O computador servidor desse serviço deve dispor de sistema de paridade controlado via hardware.

(Fulcro no item 12.2.3 da norma ABNT NBR ISO/IEC 27002:2005, com interpretação ampliada para nível de hardware e não somente no nível de aplicação).

1.8 - A disponibilidade do link de comunicação entre o usuário e o computador servidor deve estar em conformidade com o acordo de nível de serviço definido.

(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.9 - A comunicação entre o usuário e o computador servidor deve ser criptografada pelo protocolo SSL.

(Fulcro no item 12.3 da norma ABNT NBR ISO/IEC 27002:2005).

1.10 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço forem substituídos sem apresentar falhas, deve ser realizada uma formatação em nível baixo antes de serem utilizados em outro computador servidor ou cedidos a terceiros.

(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.11 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço apresentarem falhas e precisarem ser substituídos e descartados, o disco do HD deve ser destruído fisicamente antes do descarte.

(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

2 - Dos Privilégios e Controles de Acesso

2.1 - O acesso ao ambiente físico desse computador servidor só poderá ser feito mediante autorização de entrada.

2.1.1 - A autorização para acesso no ambiente físico desse computador servidor será dada somente pela Diretoria de Infraestrutura e Rede, a qual é atribuída a segurança física dos computadores servidores.

(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.2 - O computador servidor desse serviço deve operar em um local com controle de acesso físico implementado.

(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.3 - Esse serviço deve ser disponibilizado a todos os servidores e a quem mais a administração interessar.

2.3.1 - Para todos os usuários deve ser disponibilizada conta de uso individual para envio e recebimento.

2.3.1.1 - A chefia imediata do servidor ingressante deve solicitar à Coordenadoria de Infraestrutura a criação da conta de correio eletrônico seguindo as instruções do regulamento de uso do e-mail institucional.

2.3.2 – É permitido e recomenda-se que seja disponibilizado endereço de grupo de e-mail para órgãos, comissões, grupos e setores deste Instituto.

2.3.2.1 - A lista de usuários para recebimento de e-mail através do endereço de grupo deve ser mantida pela Coordenadoria de Infraestrutura.

2.3.2.2 - É de responsabilidade de cada órgão, comissão, grupo ou setor comunicar à Coordenadoria de Infraestrutura a atualização ou extinção da lista.

2.3.2.3 - Somente o presidente, dirigente ou chefia de cada órgão, comissão, grupo ou setor poderá autorizar o envio de e-mail através do endereço de grupo e é responsável por comunicar à Coordenadoria de Infraestrutura para que o procedimento de permissão seja realizado.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.4 - O acesso à administração deste serviço deve ser autorizado somente a pessoas designadas pela Diretoria de Infraestrutura e Rede.

2.4.1 - Os administradores do serviço terão acesso somente às configurações do serviço, não podendo acessar o conteúdo dos diretórios de outros usuários.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.5 - O acesso à administração do computador servidor deve ser feito somente por pessoal autorizado pelo Diretor de Infraestrutura e Rede.

2.5.1 - Os administradores desse computador servidor que não são administradores do serviço terão acesso somente às configurações do sistema, não podendo alterar as configurações do serviço.

2.5.2 - Os administradores desse computador servidor terão acesso a todos os diretórios para realizar manutenção no sistema, atualização, monitoramento e atendimento a auditorias e perícias criminais.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.6 - A senha de acesso é de uso pessoal e intransferível, não sendo permitido revelar a própria a ninguém.

(Fulcro no item 11.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

2.7 - Os administradores desse computador servidor ou desse serviço devem aceitar o termo de confidencialidade.

2.7.1 - A senha do usuário nunca poderá ser revelada, mesmo que o sistema o permita.

2.7.2 - O acesso dado às eventuais perícias será feito por outro meio, sem a revelação da senha.

(Fulcro no item 6.1.5 da norma ABNT NBR ISO/IEC 27002:2005).

2.8 - A arquitetura, bem como a configuração de armazenamento desse computador servidor, deve ser de conhecimento apenas do administrador do servidor, incluindo o mapa de diretórios em que o sistema foi instalado e se encontra em funcionamento.

(Fulcro no item 10.7.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.9 - Com exceção do administrador do computador servidor, não é permitido o acesso a qualquer diretório do sistema.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.10 - Nos casos de relotação, exoneração, aposentadoria, remoção, falecimento ou qualquer outro fator que implique o desligamento do servidor do quadro de pessoal do IFSP, a Diretoria de Recursos Humanos deve comunicar à Coordenadoria de Infraestrutura o nome completo e o número do prontuário do servidor no prazo máximo de até 10 (dez) dias corridos após publicação no Diário Oficial da União.

2.10.1 - Recomenda-se à Diretoria de Recursos Humanos que comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que for entregue um documento oficial do desligamento à DRH.

(Fulcro no item 8.3.3 da norma ABNT NBR ISO/IEC 27002:2005).

3 - Do Uso do Serviço

3.1 - Não é permitido aos usuários elaborar ou enviar quaisquer textos, documentos ou arquivos com conteúdo ilegal, tais como:

3.1.1 - conteúdos que violam propriedade intelectual;

3.1.2 - pornografia infantil;

3.1.3 - conteúdos que incitam a discriminação ou preconceito descrito na lei 7.716/1989;

3.1.4 - conteúdos que violam a intimidade, a vida privada, a honra e a imagem das pessoas, descritos no inciso X, do art. 5º da Constituição Federal.

(Fulcro nos itens 15.1.1, 15.1.2 e 15.1.5 da norma ABNT NBR ISO/IEC 27002:2005).

3.2 - Não é permitido aos usuários enviar informações, através deste serviço, à comunidade externa ou interna sem o consentimento do proprietário da informação.

(Fulcro nos itens 7.1.2 e 10.9.3 da norma ABNT NBR ISO/IEC 27002:2005).

3.3 - É de inteira responsabilidade do usuário se determinada(s) correspondência(s) se tornar(em) indisponível(is), ou seja, for(em) excluída(s) por uma ação realizada por qualquer utente.

3.3.2 - A restauração de backup do sistema ou arquivos será realizada somente quando todo o sistema for comprometido.

(Fulcro nos itens 10.5.1 e 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

3.4 - Não é permitido aos usuários enviar informações do IFSP com conteúdos sensíveis ou considerados sigilosos por lei à comunidade externa ou interna através deste serviço.

3.4.1 - Qualquer conteúdo que, ao ser publicado, prejudique o bom funcionamento do negócio, poderá ser considerado conteúdo sensível.

(Fulcro no item 10.9.3 da norma ABNT NBR ISO/IEC 27002:2005).

3.5 - Esta norma protege somente o domínio de e-mail @ifsp.edu.br e autoriza o uso deste para requisições e comunicações oficiais.

(Fulcro no item 11.1.1 da norma ABNT NBR ISO/IEC 27002:2005).

NormaSeg02

Norma de Segurança da Informação do serviço LDAP

Apresentação

O LDAP é um serviço utilizado internamente pelas equipes de TI da reitoria do Instituto Federal de Educação Ciência e Tecnologia de São Paulo para armazenar informações de servidores (funcionários) e para utilizá-las na autenticação em sistemas de outros serviços de TI, como e-mail, nuvem, redmine e fórum.

Objetivo e Abrangência

Este documento foi elaborado pelo Comitê de Política de Segurança da Informação e tem por objetivo estabelecer deveres para os administradores e usuários deste serviço, sendo mandatório para todo o IFSP.

Considerações de Segurança da Informação

O serviço LDAP armazena, recebe e envia senhas de usuários para os computadores servidores dentro do data center. Tais informações, sigilosas e importantes para o bom funcionamento dos serviços de TI, requerem segurança em termos de disponibilidade, integridade e, principalmente, confidencialidade.

A segurança de TI nesse serviço é implementada nos níveis de aplicação e de infraestrutura, cobrindo toda a área de TI.

Responsáveis

Diretoria de Infraestrutura e Rede - Responsável pela segurança física e de infraestrutura desse serviço.

Coordenadoria de Infraestrutura - Responsável pela segurança da plataforma de serviços de rede e pela aplicação e controle de acesso do serviço.

Usuário do serviço - Responsável pela segurança de sua própria senha fora do âmbito da TI.

Regras de Segurança

1 - Da Operação

1.1 - O computador servidor desse serviço deve operar em conformidade com o acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.2 - O computador servidor desse serviço deve operar em um local com autonomia energética de no mínimo 8 (oito) horas.
(Fulcro no item 9.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.3 - O computador servidor desse serviço deve operar em um local com certificado de infraestrutura segura contra ameaças naturais.
(Fulcro no item 9.1.4 da norma ABNT NBR ISO/IEC 27002:2005).

1.4 - A disponibilidade da aplicação desse serviço deve estar em conformidade com o acordo de nível de serviço.
1.4.1 - Os administradores do serviço e do computador servidor devem obedecer aos procedimentos e ao acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.5 - O espaço em disco disponível para esse serviço deve ser suficiente para a necessidade do IFSP.

1.5.1 - Periodicamente a necessidade de espaço deve ser avaliada com todas as áreas de negócio e deve ser apresentado à Diretoria de Infraestrutura e Rede um relatório de avaliação de capacidade.

1.5.2 - O intervalo de avaliação é definido pela Diretoria de Infraestrutura e Rede e executado pela Coordenadoria de Infraestrutura, não podendo ser superior a 2 (dois) anos e inferior a 6 (seis) meses.

1.5.3 - Se a Coordenadoria de Infraestrutura avaliar que há necessidade maior de espaço, em decorrência ou não do mau uso, deve ser apresentado um plano de ação com a finalidade de otimizar ou disponibilizar maior espaço para atender a essa necessidade.

(Fulcro no item 10.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.6 - O computador servidor desse serviço deve dispor de mecanismo de redundância, em caso falha em um dos discos, controlado via hardware.

(Fulcro no item 10.5.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.7 - O computador servidor desse serviço deve dispor de sistema de paridade controlado via hardware.

(Fulcro no item 12.2.3 da norma ABNT NBR ISO/IEC 27002:2005, com interpretação ampliada para nível de hardware e não somente no nível de aplicação).

1.8 - A disponibilidade do link de comunicação entre o usuário e o computador servidor deve estar em conformidade com o acordo de nível de serviço.

(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.9 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço forem substituídos sem apresentarem falhas, deve ser realizada uma formatação em nível baixo antes de serem utilizados em outro computador servidor ou cedidos a terceiros.

(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.10 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço apresentarem falhas e precisarem ser substituídos e descartados, o disco do HD deve ser destruído fisicamente antes do descarte.

(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

2 - Dos Privilégios e Controles de Acesso

2.1 - O acesso ao ambiente físico desse computador servidor só poderá ser feito mediante autorização de entrada.

2.1.1 - A autorização para acesso no ambiente físico desse computador servidor será dada somente pela Diretoria de Infraestrutura e Rede, a qual é atribuída a segurança física dos computadores servidores.

(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.2 - O computador servidor desse serviço deve operar em um local com controle de acesso físico implementado.

(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.3 - Esse serviço é disponibilizado somente na zona desmilitarizada de rede (DMZ) para todos os computadores servidores que se encontrarem nessa rede.

(Fulcro nos itens 11.4.5, 11.4.7 e 12.5.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.4 - O acesso à administração desse serviço deve ser autorizado somente a pessoas designadas pela Diretoria de Infraestrutura e Rede.

2.4.1 - Os administradores do serviço terão acesso somente às configurações do serviço, não podendo acessar o conteúdo dos diretórios do computador servidor.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.5 - O acesso à administração do computador servidor deve ser feito somente por pessoal da Diretoria de Infraestrutura de Rede, mediante autorização do Diretor de Infraestrutura e Rede.

2.5.1 - Os administradores desse computador servidor que não são administradores do serviço terão acesso somente às configurações do sistema, não podendo alterar as configurações do serviço.

2.5.2 - Os administradores desse computador servidor terão acesso a todos os diretórios para realizar manutenção no sistema, atualização, monitoramento e atendimento a auditorias e perícias criminais.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.6 - O acesso a esse serviço é autorizado somente para uso em sistemas e serviços da TI da reitoria.

(Fulcro no item 12.5.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.7 - A senha de acesso é de uso pessoal e intransferível, não sendo permitido revelar a própria a ninguém.

(Fulcro no item 11.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

2.8 - Os administradores desse computador servidor ou desse serviço deverão aceitar o termo de confidencialidade.

2.8.1 - A senha do usuário nunca poderá ser revelada, mesmo que o sistema desse serviço o permita.

2.8.2 - O acesso dado às eventuais perícias será feito por outro meio, sem a revelação da senha.

(Fulcro nos itens 6.1.5 e 15.1.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.9 - Com exceção do administrador do computador servidor, não é permitido o acesso a qualquer diretório do sistema.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.10 - O mapa da árvore de diretórios de serviço deve ser de conhecimento apenas de pessoas autorizadas pela Diretoria de Infraestrutura e Rede.

(Fulcro nos itens 10.7.4 e 12.5.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.11 - A arquitetura, bem como a configuração de armazenamento desse computador servidor, deve ser de conhecimento apenas do administrador do servidor, incluindo o mapa de diretórios em que o sistema foi instalado e se encontra em funcionamento.

(Fulcro no item 10.7.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.12 - Nos casos de relotação, exoneração, aposentadoria, remoção, falecimento ou qualquer outro que implique o desligamento do servidor do quadro de pessoal do IFSP, a Diretoria de Recursos Humanos deve comunicar à Coordenadoria de Infraestrutura o nome completo e o prontuário do servidor no prazo máximo de até 10 (dez) dias corridos após publicação no Diário Oficial da União.

2.12.1 - Recomenda-se à Diretoria de Recursos Humanos que comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que for entregue um documento oficial do desligamento à DRH.

(Fulcro no item 8.3.3 da norma ABNT NBR ISO/IEC 27002:2005).

3 - Do Uso do Serviço

3.1 - Qualquer manipulação das informações cadastradas nesse serviço deve partir de uma solicitação formalizada para o e-mail cif@ifsp.edu.br.

(Fulcro nos itens 10.1.1 e 10.10.1 da norma ABNT NBR ISO/IEC 27002:2005).

3.2 - A solicitação para manipulação das informações cadastradas nesse serviço é aceita somente quando feita a partir de endereços de e-mails do @ifsp.edu.br.

(Fulcro no item 11.5.2 da norma ABNT NBR ISO/IEC 27002:2005).

NormaSeg03

Norma de Segurança da Informação do sistema acadêmico NAMBEI

Apresentação

NAMBEI é o sistema integrado de gestão acadêmica do IFSP. É dividido nos módulos: ADMIN, CTP, CEN, MATRIC, CRE, ESCOLAC, GRH e BIBLIOT. O NAMBEI é responsável por: (i) gestão de cursos e grades curriculares, (ii) gestão de horários, professores e turmas, (iii) matrícula de alunos, (iv) gestão de registros escolares e emissão de atestados e diplomas/certificados, (v) gestão de recursos humanos e (vi) gestão de biblioteca. A aplicação é de uso restrito aos servidores do Instituto.

Objetivo e Abrangência

Este documento foi elaborado pelo Comitê de Política de Segurança da Informação e tem por objetivo estabelecer deveres para os administradores e usuários deste serviço, sendo mandatório para todo o IFSP.

Considerações de Segurança da Informação

O NAMBEI armazena e manipula informações sigilosas e/ou essenciais para o Instituto, tais como dados acadêmicos dos alunos, informações pessoais de discentes, docentes e servidores administrativos, bem como dados funcionais destes. É de uso obrigatório institucional para a emissão de documentos, diplomas, controle de ponto, etc. Sendo assim, requer a segurança dessas informações em termos de disponibilidade, integridade e confidencialidade.

A segurança de TI nesse serviço é implementada nos níveis de aplicação e de infraestrutura, cobrindo toda a área de TI.

Responsáveis

Diretoria de Infraestrutura e Rede - Responsável pela segurança física e de infraestrutura desse serviço.

Coordenadoria de Infraestrutura - Responsável pela segurança de serviços de rede.

Coordenadoria de Sistemas da Informação - Responsável pela segurança da plataforma do computador servidor, aplicação cliente-servidor e controle de acesso do serviço.

Coordenadoria Técnico-Operacional - Responsável pela segurança da plataforma e configuração dos computadores clientes na reitoria.

Assessorias e Coordenadorias de Tecnologia da Informação – Responsáveis pela segurança da plataforma e configuração dos computadores clientes nos *campi*.

Usuário - Responsável pela segurança da informação no uso do serviço.

Regras de Segurança

1 - Da Operação

1.1 - O computador servidor desse serviço deve operar em conformidade com o acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.2 - O computador servidor desse serviço deve operar em um local com autonomia energética de no mínimo 8 (oito) horas.
(Fulcro no item 9.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.3 - O computador servidor desse serviço deve operar em um local com certificado de infraestrutura segura contra ameaças naturais.
(Fulcro no item 9.1.4 da norma ABNT NBR ISO/IEC 27002:2005).

1.4 - A disponibilidade da aplicação desse serviço deve estar em conformidade com o acordo de nível de serviço.
1.4.1 - Os administradores do serviço e do computador servidor devem obedecer aos procedimentos e ao acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.5 - O espaço em disco disponível para esse serviço deve ser suficiente para a necessidade do IFSP.
1.5.1 - Periodicamente a necessidade de espaço deve ser avaliada com todas as áreas de negócio e deve ser apresentado à Diretoria de Infraestrutura e Rede um relatório de avaliação de capacidade.
1.5.2 - O intervalo de avaliação é definido pela Diretoria de Infraestrutura e Rede e executado pela Coordenadoria de Infraestrutura, não podendo ser superior a 2 (dois) anos e inferior a 6 (seis) meses.
1.5.3 - Se a Coordenadoria de Infraestrutura avaliar que há necessidade maior de espaço, em decorrência ou não do mau uso, deve ser apresentado um plano de ação com a finalidade de otimizar ou disponibilizar maior espaço para atender a essa necessidade.
(Fulcro no item 10.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.6 - O computador servidor desse serviço deve dispor de mecanismo de redundância, em caso falha em um dos discos, controlado via hardware.
(Fulcro no item 10.5.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.7 - O computador servidor desse serviço deve dispor de sistema de paridade controlado via hardware.
(Fulcro no item 12.2.3 da norma ABNT NBR ISO/IEC 27002:2005, com interpretação ampliada para nível de hardware e não somente no nível de aplicação).

1.8 - A disponibilidade do link de comunicação entre o usuário e o computador servidor deve estar em conformidade com o acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.9 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço forem substituídos sem apresentarem falhas, deve ser realizada uma formatação em nível baixo antes de serem utilizados em outro computador servidor ou cedidos a terceiros.
(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.10 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço apresentarem falhas e precisarem ser substituídos e descartados, o disco do HD deve ser destruído fisicamente antes do descarte.
(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

2 - Dos Privilégios e Controles de Acesso

2.1 - O acesso ao ambiente físico desse computador servidor só poderá ser feito mediante autorização de entrada.
2.1.1 - A autorização para acesso no ambiente físico desse computador servidor será dada somente pela Diretoria de Infraestrutura e Rede, a qual é atribuída a segurança física dos computadores servidores.
(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.2 - O computador servidor desse serviço deve operar em um local com controle de acesso físico implementado.
(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.3 - Esse serviço deve ser disponibilizado para todos os servidores com diferentes níveis de acesso.

2.3.1 - Deve ser disponibilizado o módulo ESCOLAC para todos os servidores, com acesso restrito somente ao banco de dados do órgão lotado.

2.3.2 - O acesso aos módulos CTP, CEN, CRE e MATRIC deve ser disponibilizado nos *campi* somente para servidores indicados e autorizados pelo diretor geral ou para servidores de setores previamente indicados pelo diretor de cada *campus*.

2.3.2.1 - Recomenda-se ao diretor geral que indique as coordenadorias de mesmo nome dos módulos disponibilizados e, na inexistência da coordenadoria recomendada, fica a cargo dele a indicação dos servidores que terão acesso aos módulos.

2.3.2.2 - O setor recomendado para o módulo MATRIC é a secretaria.

2.3.3 - O acesso aos módulos ESCOLAC irrestrito, CTP, CEN, CRE e MATRIC deve ser disponibilizado, na reitoria, para servidores da Pró-reitoria de Ensino autorizados pelo pró-reitor e diretores dessa Pró-reitoria.

2.3.3.1 - O acesso ao módulo CTP pode também ser disponibilizado para servidores da Diretoria de Ensino à Distância autorizados pelo diretor de ensino à distância.

2.3.3.2 - O acesso ao módulo ESCOLAC irrestrito pode também ser disponibilizado para servidores da Pró-reitoria de Pesquisa autorizados pelo pró-reitor de pesquisa.

2.3.4 - O acesso ao módulo GRH deve ser disponibilizado somente para servidores do RH de cada órgão, autorizados pelas respectivas chefias, sendo disponibilizado o acesso somente ao banco de dados do órgão lotado.

2.3.5 - O acesso ao módulo BIBLIOT deve ser disponibilizado somente para servidores da biblioteca de cada órgão, autorizados pelas respectivas chefias, sendo disponibilizado o acesso somente ao banco de dados do órgão lotado.

2.3.6 - O acesso ao módulo ADMIN deve ser disponibilizado exclusivamente para as equipes de TI de cada *campus* e, somente na inexistência destas, o diretor geral deverá indicar um ou mais servidores com conhecimento técnico para obter o acesso.

2.3.7 - As autorizações e indicações nos *campi* devem partir de e-mails institucionais, @ifsp.edu.br, enviados pelos diretores gerais ou assessorias e coordenadorias de TI dos *campi*.

2.3.8 - As autorizações na reitoria devem partir de e-mails institucionais, @ifsp.edu.br, das pessoas indicadas no item 2.3 desta norma.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.4 - O acesso à administração desse serviço ou ao seu banco de dados deve ser autorizado somente a pessoas designadas pelo Diretor de Sistemas da Informação.

2.4.1 - Os administradores do serviço terão acesso somente às configurações ou banco de dados, não podendo acessar o conteúdo dos diretórios do computador servidor.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.5 - O acesso à administração do computador servidor deve ser feito somente por pessoal da Diretoria de Sistemas da Informação, sendo este autorizado pelo Diretor de Sistemas da Informação.

2.5.1 - Os administradores desse computador servidor que não são administradores do serviço terão acesso somente às configurações do sistema, não podendo alterar as configurações do serviço e nem acessar o banco de dados.

2.5.2 - Os administradores desse computador servidor terão acesso a todos os diretórios para realizar manutenção no sistema, atualização, monitoramento e atendimento a auditorias e perícias criminais.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.6 - A senha de acesso é de uso pessoal e intransferível, não sendo permitido revelar a própria a ninguém.

(Fulcro no item 11.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

2.7 - Os administradores desse computador servidor ou desse serviço deverão aceitar o termo de confidencialidade.

2.7.1 - A senha do usuário nunca poderá ser revelada, mesmo que o sistema desse serviço o permita.
2.7.2 - O acesso dado às eventuais perícias será feito por outro meio, sem a revelação da senha.
(Fulcro nos itens 6.1.5 e 15.1.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.8 - Com exceção do administrador do computador servidor, não é permitido o acesso a qualquer diretório do sistema.
(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.9 - O mapa da árvore de diretórios de serviço deve ser de conhecimento apenas de pessoas autorizadas pela Diretoria de Sistemas da Informação.
(Fulcro nos itens 10.7.4 e 12.5.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.10 - A arquitetura, bem como a configuração de armazenamento desse computador servidor, deve ser de conhecimento apenas do administrador do servidor, incluindo o mapa de diretórios em que o sistema foi instalado e se encontra em funcionamento.
(Fulcro no item 10.7.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.11 - Nos casos de relotação, exoneração, aposentadoria, remoção, falecimento ou qualquer outro que implique o desligamento do servidor do quadro de pessoal do IFSP, a Diretoria de Recursos Humanos deve comunicar à Coordenadoria de Infraestrutura o nome completo e o prontuário do servidor no prazo máximo de até 10 (dez) dias corridos após publicação no Diário Oficial da União.
2.11.1 - Recomenda-se à Diretoria de Recursos Humanos que comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que for entregue um documento oficial do desligamento à DRH.
(Fulcro no item 8.3.3 da norma ABNT NBR ISO/IEC 27002:2005).

3 - Do Uso do Serviço

3.1 - Não é permitido aos usuários e administradores intencionalmente cadastrar informações falsas, alterar informações corretas para que se tornem falsas ou excluir, sem autorização, informações do banco de dados desse serviço.
(Fulcro nos itens 12.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

3.2 - Não é permitido aos usuários e administradores revelar informações cadastradas no banco de dados desse serviço a pessoas sem autorização de acesso, que não são proprietárias das informações reveladas ou sem o interesse e autorização da administração.
(Fulcro nos itens 10.8.1 e 12.5.4 da norma ABNT NBR ISO/IEC 27002:2005).

3.3 - É de inteira responsabilidade do usuário se determinada(s) informação(ões) for(em) cadastrada(s), alterada(s) ou excluída(s) erroneamente por uma ação realizada pelo usuário.
3.3.1 - Recomenda-se que os usuários com nível de acesso para edição já tenham noção de uso desse serviço e compreendam o item 3.3 desta norma.
3.3.2 - A restauração de backup dos arquivos será realizada somente quando todo o sistema for comprometido.
(Fulcro nos itens 10.5.1 e 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

NormaSeg04

Norma de Segurança da Informação do serviço Nuvem IFSP

Apresentação

O serviço de Nuvem do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo oferece espaço de armazenamento para documentos, imagens e arquivos que poderão ser acessados pela internet, sendo possível, ainda, compartilhar esses arquivos com qualquer usuário cadastrado no sistema ou publicar um link para compartilhamento para toda a comunidade sem a necessidade do cadastro.

Objetivo e Abrangência

Este documento foi elaborado pelo Comitê de política de Segurança da Informação e tem por objetivo estabelecer deveres para os administradores e usuários deste serviço, sendo mandatório para todo o IFSP.

Considerações de Segurança da Informação

O serviço de Nuvem poderá ser utilizado para armazenamento de documentos críticos e sensíveis e, portanto, requer a segurança dessas informações em termos de disponibilidade, integridade e confidencialidade.

A segurança de TI nesse serviço é implementada nos níveis de aplicação e de infraestrutura, cobrindo toda a área de TI.

Responsáveis

Diretoria de Infraestrutura e Rede - Responsável pela segurança física e de infraestrutura desse serviço.

Coordenadoria de Infraestrutura - Responsável pela segurança da plataforma, aplicação, controles de acesso lógico e de serviços de rede.

Usuário - Responsável pela segurança da informação e pelo uso do serviço.

Regras de Segurança

1 - Da Operação

1.1 - O computador servidor desse serviço deve operar em conformidade com o acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.2 - O computador servidor desse serviço deve operar em um local com autonomia energética de 8 (oito) horas.
(Fulcro no item 9.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.3 - O computador servidor desse serviço deve operar em um local com certificado de infraestrutura segura contra ameaças naturais.
(Fulcro no item 9.1.4 da norma ABNT NBR ISO/IEC 27002:2005).

1.4 - A disponibilidade da aplicação desse serviço deve estar em conformidade com o acordo de nível de serviço.

1.4.1 - Os administradores do serviço e do computador servidor obedecerão aos procedimentos e ao acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.5 - Esse serviço deve dispor de mecanismos no nível de aplicação para versionamento de arquivos alterados.

1.5.1 - A remoção do arquivo também excluirá todas as versões, e acarretará no item 3.3 desta norma.

(Fulcro nos itens 10.5.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.6 - O espaço em disco disponível para esse serviço deve ser suficiente para a necessidade do IFSP.

1.6.1 - Periodicamente a necessidade de espaço deve ser avaliada com todas as áreas de negócio e deve ser apresentado à Diretoria de Infraestrutura e Rede um relatório de avaliação de capacidade.

1.6.2 - O intervalo de avaliação é definido pela Diretoria de Infraestrutura e Rede e executado pela Coordenadoria de Infraestrutura, não podendo este ser superior a 2 (dois) anos e inferior a 6 (seis) meses.

1.6.3 - Se a Coordenadoria de Infraestrutura avaliar que há necessidade maior de espaço, em decorrência ou não do mau uso, deve ser apresentado um plano de ação com a finalidade de otimizar ou disponibilizar maior espaço para atender à necessidade.

(Fulcro no item 10.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.7 - O computador servidor desse serviço deve dispor de mecanismo de redundância, em caso falha em um dos discos, controlado via hardware.

(Fulcro no item 10.5.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.8 - O computador servidor desse serviço deve dispor de sistema de paridade controlado via hardware.

(Fulcro no item 12.2.3 da norma ABNT NBR ISO/IEC 27002:2005, com interpretação ampliada para nível de hardware, e não somente no nível de aplicação).

1.9 - A disponibilidade do link de comunicação entre o usuário e o computador servidor deve estar em conformidade com o acordo de nível de serviço definido.

(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.10 - A comunicação entre o usuário e o computador servidor deve ser criptografada pelo protocolo SSL.

(Fulcro no item 12.3 da norma ABNT NBR ISO/IEC 27002:2005).

1.11 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço forem substituídos sem apresentar falhas, deve ser realizada uma formatação em nível baixo antes de serem utilizados em outro computador servidor ou cedidos a terceiros.

(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.12 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço apresentarem falhas e precisarem ser substituídos e descartados, o disco do HD deve ser destruído fisicamente antes do descarte.

(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

2 - Dos Privilégios e Controles de Acesso

2.1 - O acesso ao ambiente físico desse computador servidor só poderá ser feito mediante autorização de entrada.

2.1.1 - A autorização para acesso no ambiente físico desse computador servidor será dada somente pela Diretoria de Infraestrutura e Rede, a qual é atribuída a segurança física dos computadores servidores.

(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.2 - O computador servidor desse serviço deve operar em um local com controle de acesso físico implementado.

(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.3 - Esse serviço deve ser disponibilizado para toda a comunidade com diferentes níveis de acesso.

2.3.1 - Para a comunidade externa é disponibilizado o nível de acesso somente-leitura a informações autorizadas pelos respectivos donos.

2.3.2 - Para os docentes e técnicos administrativos do IFSP é disponibilizado o nível de acesso total aos próprios diretórios e nível de acesso definido por outros usuários, para acesso ao diretório destes.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.4 - O acesso à administração desse serviço deve ser autorizado somente a pessoas designadas pela Diretoria de Infraestrutura e Rede.

2.4.1 - Os administradores do serviço terão acesso somente às configurações do serviço, não podendo acessar o conteúdo dos diretórios de outros usuários.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.5 - O acesso à administração do computador servidor deve ser feito somente por pessoal da Diretoria de Infraestrutura de Rede, devendo este ser autorizado pelo Diretor de Infraestrutura e Rede.

2.5.1 - Os administradores desse computador servidor que não são administradores do serviço terão acesso somente às configurações do sistema, não podendo alterar as configurações do serviço.

2.5.2 - Os administradores desse computador servidor terão acesso a todos os diretórios para realizar manutenção no sistema, atualização, monitoramento e atendimento a auditorias e perícias criminais.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.6 - A senha de acesso é de uso pessoal e intransferível, não sendo permitido revelar a própria a ninguém.

(Fulcro no item 11.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

2.7 - Os administradores desse computador servidor ou desse serviço deverão aceitar o termo de confidencialidade.

2.7.1 - A senha do usuário nunca poderá ser revelada, mesmo que o sistema o permita.

2.7.2 - O acesso dado às eventuais perícias será feito por outro meio, sem a revelação da senha.

(Fulcro no item 6.1.5 da norma ABNT NBR ISO/IEC 27002:2005).

2.8 - Com exceção do administrador do computador servidor, não é permitido o acesso a diretórios que não tenham sido autorizados, seguindo o item 2.3 desta norma.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.9 - A arquitetura, bem como a configuração de armazenamento desse computador servidor, deve ser de conhecimento apenas do administrador do servidor, incluindo o mapa de diretórios em que o sistema foi instalado e se encontra em funcionamento.

(Fulcro no item 10.7.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.10 - Nos casos de relotação, exoneração, aposentadoria, remoção, falecimento ou qualquer outro que implique o desligamento do servidor do quadro de pessoal do IFSP, a Diretoria de Recursos Humanos deve comunicar à Coordenadoria de Infraestrutura o nome completo e o prontuário do servidor no prazo máximo de até 10 (dez) dias corridos após publicação no Diário Oficial da União.

2.10.1 - Recomenda-se à Diretoria de Recursos Humanos que comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que for entregue um documento oficial do desligamento à DRH.

(Fulcro no item 8.3.3 da norma ABNT NBR ISO/IEC 27002:2005).

3 - Do Uso do Serviço

3.1 - Não é permitido aos usuários fazer upload ou criar qualquer documento ou arquivo com conteúdo ilegal nesse serviço, tais como:

3.1.1 - conteúdos que violam propriedade intelectual;

3.1.2 - pornografia infantil;

3.1.3 - conteúdos que incitam a discriminação ou preconceito descrito na lei 7.716/1989;

3.1.4 - conteúdos que violam a intimidade, a vida privada, a honra e a imagem das pessoas, descritos no inciso X, do art. 5º da Constituição Federal.

(Fulcro nos itens 15.1.1, 15.1.2 e 15.1.5 da norma ABNT NBR ISO/IEC 27002:2005).

3.2 - Não é permitido aos usuários publicar informações, através deste serviço, à comunidade externa e interna sem o consentimento do proprietário da informação.

(Fulcro nos itens 7.1.2 e 10.9.3 da norma ABNT NBR ISO/IEC 27002:2005).

3.3 - É de inteira responsabilidade do usuário se determinado(s) arquivo(s) se tornar(em) indisponível(is), ou seja, for(em) apagado(s) por uma ação realizada por qualquer utente.

3.3.1 - Recomenda-se que, se o arquivo ou diretório for compartilhado com outros usuários, aqueles com nível de acesso para edição já tenham noção de uso desse serviço e compreendam o item 3.3 desta norma.

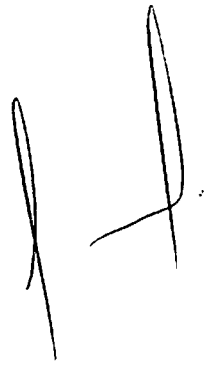
3.3.2 - A restauração de backup dos arquivos será realizada somente quando todo o sistema for comprometido.

(Fulcro nos itens 10.5.1 e 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

3.4 - Não é permitido aos usuários publicarem informações do IFSP com conteúdos sensíveis ou considerados sigilosos por lei, através deste serviço, para a comunidade externa e interna.

3.4.1 - Qualquer conteúdo que, ao ser publicado, prejudique o bom funcionamento do negócio, poderá ser considerado conteúdo sensível.

(Fulcro no item 10.9.3 e 15.1.5 da norma ABNT NBR ISO/IEC 27002:2005).



NormaSeg05

Norma de Segurança da Informação do serviço SAMBA da reitoria

Apresentação

O serviço SAMBA do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo oferece pastas de armazenamento para documentos, imagens e arquivos que poderão ser acessadas pela rede interna. Tais arquivos podem ser compartilhados por todos os usuários cadastrados na mesma pasta no sistema.

Objetivo e Abrangência

Este documento foi elaborado pelo Comitê de Política de Segurança da informação e tem por objetivo estabelecer deveres para os administradores e usuários deste serviço, sendo mandatório somente na reitoria.

Considerações de Segurança da Informação

O serviço SAMBA poderá ser utilizado para armazenamento de documentos críticos e sensíveis e, portanto, requer a segurança dessas informações em termos de disponibilidade, integridade e confidencialidade.

A segurança de TI nesse serviço é implementada nos níveis de aplicação e de infraestrutura, cobrindo toda a área de TI.

Responsáveis

Diretoria de Infraestrutura e Rede - Responsável pela segurança física e de infraestrutura desse serviço.

Coordenadoria de Infraestrutura - Responsável pela segurança da plataforma de serviços de rede e pela aplicação e controle de acesso do serviço.

Usuário - Responsável pela segurança da informação e pelo uso do serviço.

Regras de Segurança

1 - Da Operação

1.1 - O computador servidor desse serviço deve operar em conformidade com o acordo de nível de serviço definido.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.2 - O computador servidor desse serviço deve operar em um local com autonomia energética de 8 (oito) horas.
(Fulcro no item 9.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.3 - O computador servidor desse serviço deve operar em um local com certificado de infraestrutura segura contra ameaças naturais.
(Fulcro no item 9.1.4 da norma ABNT NBR ISO/IEC 27002:2005).

1.4 - A disponibilidade da aplicação desse serviço deve estar em conformidade com o acordo de nível de serviço definido.
1.4.1 - Os administradores do serviço e do computador servidor obedecerão aos procedimentos e ao acordo de nível de serviço definido.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.5 - O espaço em disco disponível para esse serviço deve ser suficiente para a necessidade do IFSP.

1.5.1 - Periodicamente a necessidade de espaço deve ser avaliada com todas as áreas de negócio e deve ser apresentado à Diretoria de Infraestrutura e Rede um relatório de avaliação de capacidade.
1.5.2 - O intervalo de avaliação é definido pela Diretoria de Infraestrutura e Rede e executado pela Coordenadoria de Infraestrutura, não podendo este ser superior a 2 (dois) anos e inferior a 6 (seis) meses.
1.5.3 - Se a Coordenadoria de Infraestrutura avaliar que há necessidade maior de espaço, em decorrência ou não do mau uso, deve ser apresentado um plano de ação com a finalidade de otimizar ou disponibilizar maior espaço para atender à necessidade.
(Fulcro no item 10.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.6 - O computador servidor desse serviço deve dispor de mecanismo de redundância, em caso falha em um dos discos, controlado via hardware.
(Fulcro no item 10.5.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.7 - A disponibilidade do link de comunicação entre o usuário e o computador servidor deve estar em conformidade com o acordo de nível de serviço definido.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.8 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço forem substituídos sem apresentarem falhas, deve ser realizada uma formatação em nível baixo antes de serem utilizados em outro computador servidor ou cedidos a terceiros.
(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.9 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço apresentarem falhas e precisarem ser substituídos e descartados, o disco do HD deve ser destruído fisicamente antes do descarte.
(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

2 - Dos Privilégios e Controles de Acesso

2.1 - O acesso ao ambiente físico desse computador servidor só poderá ser feito mediante autorização de entrada.
2.1.1 - A autorização para acesso no ambiente físico desse computador servidor será dada somente pela Diretoria de Infraestrutura e Rede, a qual é atribuída a segurança física dos computadores servidores.
(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.2 - O computador servidor desse serviço deve operar em um local com controle de acesso físico implementado.
(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.3 - Esse serviço deve ser disponibilizado somente aos servidores lotados na reitoria, com diferentes níveis de acesso.
2.3.1 - É disponibilizado o nível de acesso somente-leitura a uma pasta para servidores autorizados por outros com nível de acesso somente-leitura ou acesso total na mesma pasta.
2.3.2 - É disponibilizado o nível de acesso total a uma pasta para servidores autorizados por outros com o nível de acesso total na mesma pasta.
2.3.3 - Também é disponibilizado o nível de acesso total a servidores que solicitaram a criação da pasta, sendo essa criação previamente autorizada pela administração.
(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.4 - O acesso à administração desse serviço deve ser autorizado somente a pessoas designadas pela Diretoria de Infraestrutura e Rede.
2.4.1 - Os administradores do serviço terão acesso somente às configurações do serviço, não podendo acessar o conteúdo dos diretórios a que não foram autorizados, seguindo o item 2.3 desta norma.
(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.5 - O acesso à administração do computador servidor deve ser feito somente por pessoal da Diretoria de Infraestrutura de Rede, sendo esse autorizado pelo Diretor de Infraestrutura e Rede.

2.5.1 - Os administradores desse computador servidor que não são administradores do serviço terão acesso somente às configurações do sistema, não podendo alterar as configurações do serviço.

2.5.2 - Os administradores desse computador servidor terão acesso a todos os diretórios para realizar manutenção no sistema, atualização, monitoramento e atendimento a auditorias e perícias criminais.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.6 - A senha de acesso é de uso pessoal e intransferível, não sendo permitido revelar a própria a ninguém.

(Fulcro no item 11.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

2.7 - Os administradores desse computador servidor ou desse serviço deverão aceitar o termo de confidencialidade.

2.7.1 - A senha do usuário nunca poderá ser revelada, mesmo que o sistema o permita.

2.7.2 - O acesso dado às eventuais perícias será feito por outro meio, sem a revelação da senha.

(Fulcro no item 6.1.5 da norma ABNT NBR ISO/IEC 27002:2005).

2.8 - Com exceção do administrador do computador servidor, não é permitido o acesso a diretórios que não tenha sido autorizado seguindo o item 2.3 desta norma.

(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.9 - A arquitetura, bem como a configuração de armazenamento desse computador servidor, deve ser de conhecimento apenas do administrador do servidor, incluindo o mapa de diretórios em que o sistema foi instalado e se encontra em funcionamento.

(Fulcro no item 10.7.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.10 - Nos casos de relotação, exoneração, aposentadoria, remoção, falecimento ou qualquer outro que implique o desligamento do servidor do quadro de pessoal do IFSP, a Diretoria de Recursos Humanos deve comunicar à Coordenadoria de Infraestrutura o nome completo e o prontuário do servidor no prazo máximo de até 10 (dez) dias corridos após publicação no Diário Oficial da União.

2.10.1 - Recomenda-se à Diretoria de Recursos Humanos que comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que for entregue um documento oficial do desligamento à DRH.

(Fulcro no item 8.3.3 da norma ABNT NBR ISO/IEC 27002:2005).

3 - Do Uso do Serviço

3.1 - Não é permitido aos usuários fazer upload de qualquer documento e arquivo com conteúdo ilegal, tais como:

3.1.1 - conteúdos que violam propriedade intelectual;

3.1.2 - pornografia infantil;

3.1.3 - conteúdos que incitam a discriminação ou preconceito descrito na lei 7.716/1989;

3.1.4 - conteúdos que violam a intimidade, a vida privada, a honra e a imagem das pessoas, conforme descrito no inciso X, art.5º da Constituição Federal.

(Fulcro nos itens 15.1.2 e 15.1.5 da norma ABNT NBR ISO/IEC 27002:2005).

3.3 - É de inteira responsabilidade do usuário se determinado(s) arquivo(s) se tornar(em) indisponível(is), ou seja, for(em) apagado(s) por uma ação realizada por qualquer utente.

3.3.1 - Recomenda-se que quando for autorizado o acesso total a um usuário, este tenha noção de uso do serviço e compreenda o item 3.3 desta norma.

3.3.2 - A restauração de backup dos arquivos será realizada somente quando todo o sistema for comprometido.

(Fulcro nos itens 10.5.1 e 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

Norma de Segurança da Informação do serviço Sistema Integrado de Gestão Acadêmica

Apresentação

O SIGA-ADM é um sistema integrado de gestão administrativa. No IFSP é utilizado para: (i) a gestão de protocolos e processos, (ii) a gestão do almoxarifado, (iii) a gestão financeira e (iv) a gestão dos patrimônios da instituição. A aplicação é de uso restrito aos servidores do Instituto e é acessível pela Internet.

Objetivo e Abrangência

Este documento foi elaborado pelo Comitê de Política de Segurança da Informação e tem por objetivo estabelecer deveres para os administradores e usuários deste serviço, sendo mandatório para todo o IFSP.

Considerações de Segurança da Informação

O SIGA-ADM armazena e manipula dados sigilosos como valores monetários e informações concernentes a processos e dados pessoais e funcionais dos servidores. É de uso obrigatório institucional para diversos fluxos em vários setores e, dessa forma, requer a segurança dessas informações em termos de disponibilidade, integridade e confidencialidade.

A segurança de TI nesse serviço é implementada nos níveis de aplicação e de infraestrutura, cobrindo toda a área de TI.

Responsáveis

Diretoria de Infraestrutura e Rede - Responsável pela segurança física e de infraestrutura desse serviço.

Coordenadoria de Infraestrutura - Responsável pela segurança de serviços de rede e controle de acesso do serviço.

Coordenadoria de Sistemas da Informação - Responsável pela segurança da plataforma do computador servidor, pela aplicação e controle de acesso do serviço, bem como pelo desenvolvimento e manutenção.

Usuário - Responsável pela segurança da informação no uso do serviço.

Regras de Segurança

1 - Da Operação

1.1 - O computador servidor desse serviço deve operar em conformidade com o acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.2 - O computador servidor desse serviço deve operar em um local com autonomia energética de no mínimo 8 (oito) horas.
(Fulcro no item 9.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.3 - O computador servidor desse serviço deve operar em um local com certificado de infraestrutura segura contra ameaças naturais.
(Fulcro no item 9.1.4 da norma ABNT NBR ISO/IEC 27002:2005).

1.4 - A disponibilidade da aplicação desse serviço deve estar em conformidade com o acordo de nível de serviço.

1.4.1 - Os administradores do serviço e do computador servidor devem obedecer aos procedimentos e ao acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.5 - O espaço em disco disponível para esse serviço deve ser suficiente para a necessidade do IFSP.

1.5.1 - Periodicamente a necessidade de espaço deve ser avaliada com todas as áreas de negócio e deve ser apresentado à Diretoria de Infraestrutura e Rede um relatório de avaliação de capacidade.

1.5.2 - O intervalo de avaliação é definido pela Diretoria de Infraestrutura e Rede e executado pela Coordenadoria de Infraestrutura, não podendo este ser superior a 2 (dois) anos e inferior a 6 (seis) meses.

1.5.3 - Se a Coordenadoria de Infraestrutura avaliar que há necessidade maior de espaço, em decorrência ou não do mau uso, deve ser apresentado à Diretoria de Infraestrutura e Rede um plano de ação com a finalidade de otimizar ou disponibilizar maior espaço para atender à necessidade.
(Fulcro no item 10.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.6 - O computador servidor desse serviço deve dispor de mecanismo de redundância, em caso falha em um dos discos, controlado via hardware.
(Fulcro no item 10.5.1 da norma ABNT NBR ISO/IEC 27002:2005).

1.7 - O computador servidor desse serviço deve dispor de sistema de paridade controlado via hardware.
(Fulcro no item 12.2.3 da norma ABNT NBR ISO/IEC 27002:2005, com interpretação ampliada para nível de hardware e não somente no nível de aplicação).

1.8 - A disponibilidade do link de comunicação entre o usuário e o computador servidor deve estar em conformidade com o acordo de nível de serviço.
(Fulcro no item 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005.)

1.9 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço forem substituídos sem apresentarem falhas, deve ser realizada uma formatação em nível baixo antes de serem utilizados em outro computador servidor ou cedidos a terceiros.
(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

1.10 - Caso o HD desse computador servidor ou HD do storage que comporta arquivos desse serviço apresentarem falhas e precisarem ser substituídos e descartados, o disco do HD deve ser destruído fisicamente antes do descarte.
(Fulcro no item 10.7.2 da norma ABNT NBR ISO/IEC 27002:2005).

2 - Dos Privilégios e Controles de Acesso

2.1 - O acesso ao ambiente físico desse computador servidor só poderá ser feito mediante autorização de entrada.

2.1.1 - A autorização para acesso ao ambiente físico desse computador servidor será dada somente pela Diretoria de Infraestrutura e Rede, a qual é atribuída a segurança física dos computadores servidores.
(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.2 - O computador servidor desse serviço deve operar em um local com controle de acesso físico implementado.
(Fulcro no item 9.1.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.3 - Esse serviço deve ser disponibilizado para todos os servidores com diferentes níveis de acesso.

2.3.1 - Pode ser disponibilizado a todos os servidores o módulo ADM simples.

2.3.2 - Devem ser disponibilizados os módulos ADM referentes a cada transação somente a servidores autorizados pela chefia do setor correspondente a cada uma delas.

2.3.3 - Deve ser disponibilizado o módulo PROT restrito de cada setor para servidores pertencentes ao setor e autorizados pela respectiva chefia.
2.3.4 - Deve ser disponibilizado o módulo PROT irrestrito para servidores da Coordenadoria de Documentação e Arquivo autorizados pelo Coordenador de Documentação e Arquivo.
2.3.5 - As autorizações para os *campi* serão concedidas mediante solicitação dos diretores gerais ou assessorias e coordenadorias de TI dos *campi*. Esta deverá ser feita através do e-mail institucional @ifsp.edu.br.
2.3.6 - As autorizações na reitoria devem partir de e-mails institucionais, @ifsp.edu.br, das pessoas indicadas no item 2.3 desta norma.
(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.4 - O acesso à administração desse serviço ou a seu banco de dados deve ser autorizado somente a pessoas designadas pelo Diretor de Sistemas da Informação.
2.4.1 - Os administradores do serviço terão acesso somente às configurações ou banco de dados, não podendo acessar o conteúdo dos diretórios do computador servidor.
(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.5 - O acesso à administração do computador servidor deve ser feito somente por pessoal da Diretoria de Sistemas da Informação, tendo sido este autorizado pelo Diretor de Sistemas da Informação.
2.5.1 - Os administradores desse computador servidor que não são administradores do serviço terão acesso somente às configurações do sistema, não podendo alterar as configurações do serviço e nem acessar o banco de dados.
2.5.2 - Os administradores desse computador servidor terão acesso a todos os diretórios para realizar manutenção no sistema, atualização, monitoramento e atendimento a auditorias e perícias criminais.
(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.6 - A senha de acesso é de uso pessoal e intransferível, não sendo permitido revelar a própria a ninguém.
(Fulcro no item 11.3.1 da norma ABNT NBR ISO/IEC 27002:2005).

2.8 - Os administradores desse computador servidor ou desse serviço deverão aceitar o termo de confidencialidade.
2.8.1 - A senha do usuário nunca poderá ser revelada, mesmo que o sistema desse serviço o permita.
2.8.2 - O acesso dado às eventuais perícias será feito por outro meio, sem a revelação da senha.
(Fulcro nos itens 6.1.5 e 15.1.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.9 - Com exceção do administrador do computador servidor, não é permitido o acesso a qualquer diretório do sistema.
(Fulcro no item 11.2.2 da norma ABNT NBR ISO/IEC 27002:2005).

2.10 - O mapa da árvore de diretórios de serviço deve ser de conhecimento apenas de pessoas autorizadas pela Diretoria de Sistemas da Informação.
(Fulcro nos itens 10.7.4 e 12.5.4 da norma ABNT NBR ISO/IEC 27002:2005).

2.11 - A arquitetura, bem como a configuração de armazenamento desse computador servidor, deve ser de conhecimento apenas do administrador do servidor, incluindo o mapa de diretórios em que o sistema foi instalado e está em funcionamento.
(Fulcro no item 10.7.4 da norma ABNT NBR ISO/IEC 27002:2005).
2.12 - Nos casos de relotação, exoneração, aposentadoria, remoção, falecimento ou qualquer outro que implique o desligamento do servidor do quadro de pessoal do IFSP, a Diretoria de Recursos Humanos deve comunicar à Coordenadoria de Infraestrutura o nome completo e o prontuário do servidor no prazo máximo de até 10 (dez) dias corridos após publicação no Diário Oficial da União.

2.12.1 - Recomenda-se à Diretoria de Recursos Humanos que comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que for entregue um documento oficial do desligamento à DRH.
(Fulcro no item 8.3.3 da norma ABNT NBR ISO/IEC 27002:2005).

3 - Do Uso do Serviço

3.1 - Não é permitido aos usuários e administradores intencionalmente cadastrar informações falsas, alterar informações corretas para que se tornem falsas ou excluir, sem autorização, informações do banco de dados desse serviço.
(Fulcro nos itens 12.2.1 da norma ABNT NBR ISO/IEC 27002:2005).

3.2 - Não é permitido aos usuários e administradores revelar informações cadastradas no banco de dados a pessoas sem autorização de acesso, que não são proprietárias das informações reveladas ou sem o interesse e autorização da administração.
(Fulcro nos itens 10.8.1 e 12.5.4 da norma ABNT NBR ISO/IEC 27002:2005).

3.3 - É de inteira responsabilidade do usuário se determinada(s) informação(ões) for(em) cadastrada(s), alterada(s) ou excluída(s) erroneamente por uma ação realizada pelo usuário.
3.3.1 - Recomenda-se que os usuários com nível de acesso para edição já tenham noção de uso desse serviço e compreendam o item 3.3 desta norma.
3.3.2 - A restauração de backup dos arquivos será realizada somente quando todo o sistema for comprometido.
(Fulcro nos itens 10.5.1 e 13.2.1 da norma ABNT NBR ISO/IEC 27002:2005).