MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO

RESOLUÇÃO N.º 38, DE 6 DE MAIO DE 2014

Aprova a Política de Segurança da Informação - 2014

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO, no uso de suas atribuições regulamentares e, considerando a decisão do Conselho Superior na reunião do dia 6 de maio de 2014,

RESOLVE:

Aprovar a Política de Segurança da Informação 2014, do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, na forma do anexo.

EDUARDO ANTONIO MODENA

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
SÃO PAULO

Diretoria de Infraestrutura e Redes

Gestão de Segurança da Informação

Política de Segurança da Informação

São Paulo, janeiro de 2014

Eduardo Antonio Modena
Reitor

Comitê de Política de Segurança da Informação
Anne Camila Knoll Domenici
Diego Cesar Valente E Silva
Dirlei Paulino Pinto
Edgar Noda
Flavio Kyoshi Saito
Fernando De Jesus Flores Parreira
João Paulo Dal Poz Pereira
Kleber Manrique Trevisani
Paulo Orlando Ricarte Kawachi
Paulo Roberto De Abreu
Roan Simões Da Silva
Rodolfo Francisco De Oliveira
Silvan Amaro Oliveira

Diretoria de Infraestrutura e Redes
Bruno Jamalaro
Dárcio Arantes Teófilo
Fábio Borges de Souza
Gabriel Gracioso Remondini
Júlio Villar Ornellas
Márcio Feliciano do Prado

Sumário

1. Histórico

A primeira versão deste documento foi elaborada pela Comissão de Política de Segurança da Informação do IFSP, criada com as seguintes atribuições:

- Elaborar a Política de Segurança da Informação que dê sustentação às atividades de proteção das informações do Instituto; e

- Propor o plano de melhoria de segurança da informação de acordo com a norma ISO/IEC 27005:2005.

Esta segunda versão do documento foi elaborada pela Diretoria de Infraestrutura e Redes, atendendo ao comunicado de auditoria 008/2013, que sanou deficiências apontadas pela auditoria e realizou correções de informações desatualizadas.

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.

Esta política deve ser revisada e atualizada anualmente.

2. Introdução

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

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

Para isto, utiliza um grande número de ativos, essenciais para os negócios do Instituto. Assim, 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 se caracterizará pela tentativa de manter a confidencialidade, a integridade e a disponibilidade das informações, independentemente de onde ela esteja, residente em memória de máquinas e dispositivos, armazenada em disco, em trânsito ou impressas em documentos, salvaguardando a exatidão e completeza da mesma, dos métodos de processamento e garantindo que a comunidade obtenham 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 prevenir e responder aos incidentes de segurança.

4. Comprometimento da direção

O Conselho Superior e a Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo declaram que estão comprometidos em proteger os ativos de informação abrangidos neste documento, apoiando as metas e os princípios da segurança da informação, alinhada com os objetivos e estratégias desta instituição.

5. Metas globais

Esta versão da política de segurança da informação tem por meta as seguintes ações:

- A institucionalização e formalização clara dos princípios da segurança da informação através da divulgação da política em portal próprio e de ações de conscientização registradas;
- Formalização das ações de prevenção contra incidentes de segurança através das Normas de Segurança com algumas ações registradas em documentos;
- Formalização das ações corretivas e de contingência em casos de ocorrência de incidentes de segurança que deverão ser documentadas conforme o Programa de Gestão de Continuidade de Negócio;

Tais metas deverão cumpridas até a atualização deste documento.

6. 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 esses 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 IFSP.

Dentro do escopo são tratadas a confidencialidade, a integridade e a disponibilidade das informações tanto para servidores e alunos quanto para terceiros..

7. Segurança da informação

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

8. 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 essas não forem seguidas.

9. Penalidades

Se a infração cometida contra esta Política de segurança da informação estiver relacionada a uma lei penal, a infração 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.

10. Órgãos, comissões, grupos e pessoas responsáveis pela Política de Segurança da Informação e suas atribuições

10.1. Conselho Superior

Ao Conselho Superior compete aprovar esta política e normas anexadas bem como se comprometer com a declaração do tópico 4 deste documento.

10.2. Colégio de Dirigentes

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

10.3. Diretoria de Infraestrutura e Rede

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.

Também é responsável por executar ou acompanhar ações preventivas e corretivas contra incidentes de segurança da informação assim como o registro dessas ocorrências.

10.4. 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.

10.5. Procuradoria Jurídica

À Procuradoria Jurídica compete representar judicial e extrajudicialmente o IFSP e exercer atividades de consultoria e prestar assessoramento jurídico aos órgãos do IFSP, aplicando-se, no que couber, o disposto no artigo 11, da Lei Complementar n.º 73, de 10 de fevereiro de 1993.

10.6. 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.

10.7. Alunos, servidores e demais pessoas que usam, têm ou terão contato com qualquer ativo protegido por esta política

Cumprir com as determinações da política de segurança da informação do IFSP.

11. ANEXOS

11.1. 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 ocorrer mudanças com relação à segurança da informação ou quando for alterado o escopo desta política. As revisões e atualizações nas normas devem ser feitas independentes das revisões e atualizações desta política.

Os documentos das normas de segurança anexadas à 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; e

NormaSeg06 - Norma de segurança da informação do Sistema Integrado de Gestão Acadêmica.

NormaSeg01

Norma de segurança da informação do serviço de e-mail institucional

Introdução

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 pela Comissão 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 termo de disponibilidade, integridade e confidencialidade, além de seu conteúdo ser considerado sigiloso pelo inciso XII, Art5º, da Constituição Federal.

A segurança de TI nesse serviço é implementada no nível de aplicação e no nível de infraestrutura cobrindo toda a área de TI.

Responsáveis

Diretoria de Infraestrutura e Redes - 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 do serviço.

Usuário do serviço - Responsáveis pela segurança da informação 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 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 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 um relatório de avaliação de capacidade.

1.5.2 - O intervalo de avaliação deve ser definido pela Diretoria de Infraestrutura e Rede e executada pela Coordenadoria de Infraestrutura, não podendo o intervalo ser maior do que 2 anos e menor do que 6 meses.

1.5.3 - Se a Coordenadoria de Infraestrutura e Serviços avaliar que há necessidade maior de espaço, sendo ocasionada pelo mau uso desse ou não, deve ser apresentado um plano de ação com o fim de otimizar o espaço 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.

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 for substituído sem apresentar falhas, deve ser realizada uma formatação em nível baixo antes de utilizar em outro computador servidor ou ceder 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 apresentar falhas e precisar ser substituído e descartado, 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 Redes, 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 comunicar a Coordenadoria de Infraestrutura para criação da conta de e-mail seguindo instruções do regulamento de uso do e-mail institucional.

2.3.2 - Pode 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 a 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 a permissão para envio de e-mail através do endereço de grupo, e é responsável por comunicar a 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 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 Redes, sendo esses autorizados 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, atender 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.

2.6.1 - O login de acesso é mantido pelo sistema LDAP, sendo esse documentado no NormaSeg02.

(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 permitisse.

2.7.2 - O acesso dado às eventuais perícias será feita 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 funcionando.

(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 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 desligado no prazo máximo de até 10 dias corridos após publicação no Diário Oficial da União.

2.10.1 - Recomenda-se que a Diretoria de Recursos Humanos comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que foi 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 enviar qualquer texto, 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; e

3.1.4 - conteúdos que violam a intimidade, a vida privada, a honra e a imagem das pessoas descrito no inciso X, Artº5, 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 dono 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, excluído(s) por uma ação realizada por qualquer usuário.

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, através deste serviço, à comunidade externa ou 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 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 desse domínio 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 serviço 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) do IFSP para utilizar na autenticação em sistemas de outros serviços de TI, como e-mail, nuvem, redmine e fórum.

Objetivo e abrangência

Este documento foi elaborado pela Comissão 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, envia e recebe senhas de usuários para os computadores servidores dentro do data center, sendo, essa informação, sigilosa e importante para o bom funcionamento dos serviços de TI e, portanto, requer a segurança dessas informações em termo de disponibilidade, integridade e, principalmente, confidencialidade.

A segurança de TI nesse serviço é implementada no nível de aplicação e no nível de infraestrutura cobrindo toda a área de TI.

Responsáveis

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

Coordenadoria de Infraestrutura - Responsável pela segurança da plataforma, de serviços de rede, 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 mínimo 8 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 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 executada pela Coordenadoria de Infraestrutura, não podendo o intervalo ser maior do que 2 anos e menor do que 6 meses.

1.5.3 - Se a Coordenadoria de Infraestrutura e Serviços avaliar que há necessidade de maior espaço, sendo ocasionada pelo mau uso desse ou não, deve ser apresentado à Diretoria de infraestrutura e rede um plano de ação com o fim de otimizar o espaço 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 for substituído sem apresentar falhas, deve ser realizada uma formatação em nível baixo antes de utilizar em outro computador servidor ou ceder 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 apresentar falhas e precisar ser substituído e descartado, 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 Redes, 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 Redes, sendo esses autorizados 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, atender a auditorias e perícias criminais.

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

2.6 - O acesso ao uso desse 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 senha para ninguem.

2.7.1 - O login de acesso é mantido pelo sistema LDAP.

(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 permitisse.

2.8.2 - O acesso dado às eventuais perícias será feita 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 funcionando.

(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 desligado no prazo máximo de até 10 dias corridos após publicação no Diário Oficial da União.

2.12.1 - Recomenda-se que a Diretoria de Recursos Humanos comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que foi 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 suporte@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 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

O sistema 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) a gestão de cursos e grades curriculares, (ii) a gestão de horários, professores e turmas, (iii) a matricula de alunos, (iv) a gestão de registros escolares e emissão de atestados e diplomas/certificados, (v) a gestão de recursos humanos, e (vi) a gestão de biblioteca. A aplicação é de uso restrito aos servidores do Instituto.

Objetivo e abrangência

Este documento foi elaborado pela Comissão 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, como dados acadêmicos dos alunos. Também armazena informações pessoais de alunos, docentes e servidores administrativos, bem como dados funcionais destes. É de uso obrigatório institucional para a emissão de documentos, diplomas, controle de ponto, etc. Dessa forma requer a segurança dessas informações em termo de disponibilidade, integridade e confidencialidade.

A segurança de TI nesse serviço é implementada no nível de aplicação e no nível de infraestrutura cobrindo toda a área de TI.

Responsáveis

Diretoria de Infraestrutura e Redes - 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 - Responsável pela segurança da plataforma e configuração dos computadores clientes nos campi.

Usuário do serviço - 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 mínimo 8 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 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 executada pela Coordenadoria de Infraestrutura, não podendo o intervalo ser maior do que 2 anos e menor do que 6 meses.

1.5.3 - Se a Coordenadoria de Infraestrutura e Serviços avaliar que há necessidade maior de espaço, sendo ocasionada pelo mau uso desse ou não, deve ser apresentado à Diretoria de infraestrutura e rede um plano de ação com o fim de otimizar o espaço 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 for substituído sem apresentar falhas, deve ser realizada uma formatação em nível baixo antes de utilizar em outro computador servidor ou ceder 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 apresentar falhas e precisar ser substituído e descartado, 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 Redes, 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 a somente 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 de cada campus ou servidores de setores previamente indicados pelo diretor de cada campus.

2.3.2.1 - Recomenda-se que o diretor geral indique as coordenadorias de mesmo nome dos módulos disponibilizados e, na inexistência da coordenadoria recomendada, fica a cargo do diretor geral 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 ser disponibilizado, também, 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 ser disponibilizado, também, 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 pela chefia de cada RH, 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 pela chefia de cada biblioteca, sendo disponibilizado o acesso somente ao banco de dados do órgão lotado.

2.3.6 - O acesso ao módulo ADMIN deve ser disponibilizado somente para as equipes de TI de cada campus e, somente na inexistência de equipe de TI no campus, 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, dos diretores gerais ou das 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 banco de dados desse serviço 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 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 Sistemas da Informação, sendo esses autorizados 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, atender 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 senha para 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 permitisse.

2.7.2 - O acesso dado às eventuais perícias será feita 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 funcionando.

(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 desligado no prazo máximo de até 10 dias corridos após publicação no Diário Oficial da União.

2.11.1 - Recomenda-se que a Diretoria de Recursos Humanos comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que foi 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, pessoas 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 cadastrada, alterada ou excluída erroneamente por uma ação realizada pelo usuário.

3.3.1 - Recomenda-se que os usuários que tenham nível de acesso para edição já tenham noção de uso desse 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.)

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 e ainda podendo compartilhar esses arquivos com qualquer usuário cadastrado no sistema ou publicar um link para compartilhar com a comunidade toda sem a necessidade do cadastro.

Objetivo e abrangência

Este documento foi elaborado pela Comissão 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 termo de disponibilidade, integridade e confidencialidade.

A segurança de TI nesse serviço é implementada no nível de aplicação e no nível de infraestrutura cobrindo toda a área de TI.

Responsáveis

Diretoria de Infraestrutura e Redes - 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 do serviço.

Usuário do serviço - Responsáveis pela segurança da informação 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 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 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 removerá 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 executada pela Coordenadoria de Infraestrutura, não podendo o intervalo ser maior do que 2 anos e menor do que 6 meses.

1.6.3 - Se a Coordenadoria de Infraestrutura e Serviços avaliar que há necessidade maior de espaço, sendo ocasionada pelo mau uso desse ou não, deve ser apresentado um plano de ação com o fim de otimizar o espaço 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 criptografado 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 for substituído sem apresentar falhas, deve ser realizada uma formatação em nível baixo antes de utilizar em outro computador servidor ou ceder 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 apresentar falhas e precisar ser substituído e descartado, 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 Redes, 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 donos das informações.

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 no diretório desses.

(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 Redes, sendo esses autorizados 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, atender 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 senha para ninguém.

2.6.1 - O login de acesso é mantido pelo sistema LDAP, sendo esse documentado no NormaSeg02.

(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 permitisse.

2.7.2 - O acesso dado às eventuais perícias será feita 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 funcionando.

(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 desligado no prazo máximo de até 10 dias corridos após publicação no Diário Oficial da União.

2.10.1 - Recomenda-se que a Diretoria de Recursos Humanos comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que foi 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 e 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; e

3.1.4 - conteúdos que violam a intimidade, a vida privada, a honra e a imagem das pessoas descrito no inciso X, Artº5, 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 dono 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, apagado(s) por uma ação realizada por qualquer usuário.

3.3.1 - Recomenda-se que se o arquivo ou diretório for compartilhado com outros usuários, os usuários que tenham nível de acesso para edição já tenham noção de uso desse 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.)

3.4 - Não é permitido aos usuários publicar informações do IFSP com conteúdos sensíveis ou considerados sigilosos por lei, através deste serviço, à 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 acessados pela rede interna e ainda podendo compartilhar esses arquivos com usuários cadastrados na mesma pasta no sistema.

Objetivo e abrangência

Este documento foi elaborado pela Comissão 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 termo de disponibilidade, integridade e confidencialidade.

A segurança de TI nesse serviço é implementada no nível de aplicação e no nível de infraestrutura cobrindo toda a área de TI.

Responsáveis

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

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

Usuário do serviço - Responsáveis pela segurança da informação 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 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 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 executada pela Coordenadoria de Infraestrutura, não podendo o intervalo ser maior do que 2 anos e menor do que 6 meses.

1.5.3 - Se a Coordenadoria de Infraestrutura e Serviços avaliar que há necessidade maior de espaço, sendo ocasionada pelo mau uso desse ou não, deve ser apresentado um plano de ação com o fim de otimizar o espaço 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 for substituído sem apresentar falhas, deve ser realizada uma formatação em nível baixo antes de utilizar em outro computador servidor ou ceder 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 apresentar falhas e precisar ser substituído e descartado, 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 feita 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 Redes, 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 servidores 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 servidores com o nível de acesso total na mesma pasta.

2.3.3 - Também é disponibilizado o nível de acesso total a servidores que solicitou 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 em que não foi autorizado 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 Redes, sendo esses autorizados 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, atender 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 senha para 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 permitisse.

2.7.2 - O acesso dado às eventuais perícias será feita 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 funcionando.

(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 desligado no prazo máximo de até 10 dias corridos após publicação no Diário Oficial da União.

2.10.1 - Recomenda-se que a Diretoria de Recursos Humanos comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que foi 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 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; e

3.1.4 - conteúdos que violam a intimidade, a vida privada, a honra e a imagem das pessoas descrito no inciso X, Artº5, 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, apagado(s) por uma ação realizada por qualquer usuário.

3.3.1 - Recomenda-se que se for autorizado o acesso total a um usuário, esse usuário 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.)

NormaSeg06

Norma de segurança da informação do serviço Sistema Integrado de Gestão Acadêmica

Apresentação

O sistema 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 pela Comissão 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 informações sigilosas como valores monetários, informações de processos e dados pessoais e funcionais dos servidores. Além de ser de uso obrigatório institucional para diversos fluxos em diversos setores. Dessa forma requer a segurança dessas informações em termo de disponibilidade, integridade e confidencialidade.

A segurança de TI nesse serviço é implementada no nível de aplicação e no nível de infraestrutura cobrindo toda a área de TI.

Responsáveis

Diretoria de Infraestrutura e Redes - 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, aplicação e controle de acesso do serviço bem como o desenvolvimento e manutenção.

Usuário do serviço - 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 mínimo 8 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 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 executada pela Coordenadoria de Infraestrutura, não podendo o intervalo ser maior do que 2 anos e menor do que 6 meses.

1.5.3 - Se a Coordenadoria de Infraestrutura e Serviços avaliar que há necessidade maior de espaço, sendo ocasionada pelo mau uso desse ou não, deve ser apresentado à Diretoria de infraestrutura e rede um plano de ação com o fim de otimizar o espaço 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 for substituído sem apresentar falhas, deve ser realizada uma formatação em nível baixo antes de utilizar em outro computador servidor ou ceder 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 apresentar falhas e precisar ser substituído e descartado, 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 Redes, 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 para todos os servidores o módulo ADM simples.

2.3.2 - Deve ser disponibilizado os módulos ADM referentes a cada transação somente para servidores autorizados pela chefia do setor de cada transação.

2.3.3 - Deve ser disponibilizado o módulo PROT restrito de cada setor para servidores que pertencem ao setor e autorizados pela chefia do setor.

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, nos campi, devem partir de e-mails institucionais, @ifsp.edu.br, dos diretores gerais ou das acessorias e coordenadorias de TI dos campi.

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 ao banco de dados desse serviço 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 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 Sistemas da Informação, sendo esses autorizados 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, atender 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 senha para ninguém.

2.6.1 - O login de acesso é mantido pelo sistema LDAP, sendo esse documentado no NormaSeg02.

(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 permitisse.

2.8.2 - O acesso dado às eventuais perícias será feita 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 funcionando.

(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 desligado no prazo máximo de até 10 dias corridos após publicação no Diário Oficial da União.

2.12.1 - Recomenda-se que a Diretoria de Recursos Humanos comunique o desligamento do servidor à Coordenadoria de Infraestrutura na mesma data em que foi 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, pessoas 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 cadastrada, alterada ou excluída erroneamente por uma ação realizada pelo usuário.

3.3.1 - Recomenda-se que os usuários que tenham nível de acesso para edição já tenham noção de uso desse 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.)

11.2. Programa de Gestão de Continuidade de Negócio

O processo de Gestão de Continuidade de Negócio objetiva minimizar impactos decorrentes de incidentes de segurança sobre as atividades deste instituto.

O conjunto de planos que serão apresentados a seguir deverá ser seguido para manter as atividades dos servidores e a interação com o público em um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

Os planos de gerenciamento de incidente (PlanoGeInc) contêm informações e instruções relevantes para a resolução ou resposta ao incidente de segurança.

Os planos de continuidade de negócio (PlanoCoNeg) contêm informações e instruções relevantes que deverão ser seguidas na prevenção, durante o incidente/contingência e após a contingência para recuperação e retorno à normalidade.

Esses planos devem ser revisados e atualizados quando ocorrer mudanças com relação à segurança da informação ou quando for alterado o escopo desta política. As revisões e atualizações nos planos devem ser feitas independentes das revisões e atualizações desta política.

Os documentos do Programa de Gestão de Continuidade de Negócio anexados à esta política são:

PlanoGeInc01 – Indisponibilidade de sistema ou serviço de rede

PlanoCoNeg01 – Indisponibilidade de sistema ou serviço de rede

PlanoGeInc02 – Indisponibilidade da rede ou link de internet

PlanoCoNeg02 – Indisponibilidade da rede ou link de internet

PlanoGeInc03 – Perda de dados

PlanoCoNeg03 – Perda de dados

PlanoGeInc04 – Roubo de dados

PlanoCoNeg04 – Roubo de dados

PlanoGeInc05 – Modificação não autorizada de servidor

PlanoCoNeg05 – Modificação não autorizada de servidor

PlanoGeInc06 – Utilização indevida de recursos de TI

PlanoCoNeg06 – Utilização indevida de recursos de TI

PlanoGeInc01

Plano de Gerenciamento de Incidentes - 01

Incidente: **Indisponibilidade de sistema ou serviço de rede**

Local: Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Autor: Paulo Orlando Ricarte Kawachi

Contato: paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento tem como objetivo apontar ações corretivas que serão tomadas caso algum sistema ou serviço de rede, crítico ou não, se torne indisponível totalmente ou parcialmente.

A análise da criticidade determinará ações de contingência descritas no Plano de Continuidade de Negócio.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DO GERENCIAMENTO DE INCIDENTES

Procedimento 01: Análise da comunicação do incidente

Grupo funcional:	Gerência de Suporte e Treinamento
Responsável:	André Luis Vieira
ID	Instrução
1	Caso qualquer usuário comunique a indisponibilidade de determinado sistema ou serviço de rede, verifique se isso ocorre em mais de um usuário ou grupos de usuários e, se confirmado, classifique a comunicação como incidente de segurança. Após a classificação, comunique imediatamente o grupo funcional responsável por aquele sistema ou serviço de rede. Senão, trate como caso isolado e atenda como chamado técnico comum.
2	Caso necessário comunique a Assessoria de Tecnologia da Informação.
3	Caso a resolução do incidente necessite ações em terminais de usuários, auxilie o grupo funcional responsável na execução.

Procedimento 02: Análise da criticidade do incidente

Grupo funcional:	Diretoria de Infraestrutura e Redes, Diretoria de Sistemas da Informação
Responsável:	Paulo Orlando Ricarte Kawachi, Brunno dos Passos Alves
ID	Instrução
1	Após a confirmação do incidente pelo grupo Gerência de Suporte e Treinamento, faça uma reunião rápida e informal entre os responsáveis pelas duas diretorias, a fim de verificar a responsabilidade pela resolução do incidente. Tempo máximo da reunião: 15 minutos.
2	Faça uma análise da interoperabilidade entre o sistema ou serviço de rede indisponível com outros serviços e comunique os serviços que serão afetados para a Assessoria de Tecnologia da Informação.
3	Faça uma análise do tempo de resolução. Caso o tempo de resolução exceda um período do dia, de manhã até às 12 horas ou de tarde até às 18 horas, acione os procedimentos de contingência se o serviço indisponível for considerado crítico.
4	Se o serviço indisponível não for crítico, acione os procedimentos de contingência caso o tempo de resolução exceda 2 dias úteis.
5	Para serviços úteis, porém dispensáveis, desconsidere o acionamento da contingência.
6	Formalize a análise em ata.

Procedimento 03: Comunicações

Grupo funcional:	Assessoria de Tecnologia da Informação
Responsável:	Eduardo Leal
ID	Instrução
1	Após análise da criticidade do incidente, avalie a necessidade da comunicação para o público externo ou interno.
2	Obtenha do grupo funcional técnico as informações do incidente para construção textual, caso a comunicação seja necessária. Tome essa ação antes, durante e depois da resolução do incidente.
3	Mantenha as principais partes interessadas informadas.

Procedimento 04: Resolução do incidente

Grupo funcional:	Diretoria de Infraestrutura e Redes ou Diretoria de Sistemas da Informação
Responsável:	Paulo Orlando Ricarte Kawachi ou Brunno dos Passos Alves
ID	Instrução
1	Faça uma reunião com o grupo enumerando fatos constatados, elaborando soluções e dividindo tarefas. Repita as reuniões para cada período do dia, manhã, tarde e noite, até a resolução do incidente.
2	Caso necessário, contate os fornecedores e os faça participar da resolução do incidente.
3	Caso necessário solicite apoio dos campi através da Assessoria de Tecnologia da Informação.
4	Documente toda tarefa realizada.

Procedimento 05: Relatório do incidente

Grupo funcional:	Diretoria de Infraestrutura e Redes ou Diretoria de Sistemas da Informação
Responsável:	Paulo Orlando Ricarte Kawachi ou Brunno dos Passos Alves
ID	Instrução
1	Elabore relatório descrevendo o incidente ocorrido, danos causados e as ações realizadas para o retorno à normalização e as ações para entrada e saída da contingência.
2	Encaminhe relatório para a Assessoria de Tecnologia da Informação.

PlanoCoNeg01

Plano de Continuidade de Negócio - 01

Incidente: **Indisponibilidade de sistema ou serviço de rede**

Local: Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Autor: Paulo Orlando Ricarte Kawachi

Contato: paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento descreve as ações que devem ser tomadas em casos de acionamento da contingência. O estado de contingência só deve ser acionado após análise descrita no Plano de Gerenciamento de Incidente.

Este Plano descreve instruções que serão seguidas antes, durante e depois da contingência.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DE CONTINUIDADE DE NEGÓCIO

Procedimento 01: Antes da contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Implemente redundâncias dos sistemas e serviços mais críticos.
2	Avalie e implemente redundâncias remotas, caso necessário e se possível.
3	Caso o sistema não possibilite redundância, mantenha backup da base de dados e arquivos para a reconstrução ou snapshot da máquina virtual para ser utilizado se necessário.
4	Monitore sempre que possível o desempenho da máquina principal e teste ao menos uma vez por trimestre a máquina de redundância e os backups. Os relatórios de testes devem ser guardados pelos grupos funcionais responsáveis. O último relatório de teste deve ser apresentado junto ao relatório de incidente quando houver.
5	Instrua todos os gestores da reitoria e dos campi a manterem cópia de segurança dos sistemas de colaboração.

Procedimento 02: Durante a contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Se estiver implementado, os sistemas redundantes deverão ser ativados.
2	Durante a contingência será permitida a inserção, extração e manipulação de dados e arquivos contidos nos sistemas pela equipe de TI, caso isso seja possível. Esta ação somente deverá ser tomada com autorização da Assessoria de Tecnologia da Informação.
3	Para serviços de comunicação, como VoIP e Videoconferência, remarque para conferências presenciais durante a contingência ou utilize a telefonia convencional.
4	Para sistemas acadêmicos e de gestão, comunique a necessidade de alteração de prazos caso precise e se não houver sistemas redundantes.
5	Para sistemas de colaboração, como E-mail, SAMBA e Nuvem, recomende a não utilização de contas pessoais em servidores privados. Em casos urgentes adote a instrução 2 deste procedimento ou opte pelos serviços de comunicação durante a contingência.
6	Monitore e registre o impacto causado pela contingência. Acrescente essa informação no relatório de incidente.

Procedimento 03: Após a contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Após resolução do incidente, encontrado a causa e o sistema ou serviço afetado reestabelecido, caso o recurso humano do grupo funcional responsável seja insuficiente para a normalização em tempo hábil, se a intervenção nos terminais de usuários seja necessária, a Assessoria de Tecnologia da Informação deverá mobilizar outros grupos da TI para auxiliar.
2	Realize testes com as partes interessadas e solicite o fechamento dos chamados, caso tenham abertos.
3	A Assessoria de Tecnologia da Informação deverá, se necessário, elaborar e publicar um comunicado para o público externo ou interno ou apenas explanar o ocorrido para as principais partes interessadas.
4	Oriente todos os colaboradores para que não divulguem ou comentem nada sobre o ocorrido, pois somente a Assessoria de Tecnologia da Informação é a responsável pela comunicação oficial da TI institucionalizada pelo órgão.
5	Se necessário, oriente e auxilie a atualização de dados e arquivos que foram tratados de modo off-line.

PlanoGeInc02

Plano de Gerenciamento de Incidentes - 02

Incidente:	**Indisponibilidade ou instabilidade da rede ou link de internet**
Local:	Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo
Autor:	Paulo Orlando Ricarte Kawachi
Contato:	paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento tem como objetivo apontar ações corretivas que serão tomadas caso a rede interna ou link de internet estiver interrompida totalmente ou parcialmente.

A análise da criticidade determinará ações de contingência descritas no Plano de Continuidade de Negócio.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DO GERENCIAMENTO DE INCIDENTES

Procedimento 01: Análise da comunicação do incidente

Grupo funcional:	Gerência de Suporte e Treinamento
Responsável:	André Luis Vieira
ID	Instrução
1	Caso qualquer usuário comunique a indisponibilidade ou instabilidade da rede, verifique se isso ocorre em mais de um usuário ou grupos de usuários e, se confirmado, classifique a comunicação como incidente de segurança. Após a classificação, comunique imediatamente a Diretoria de Infraestrutura e Redes. Senão, trate como caso isolado e atenda como chamado técnico comum.
2	Caso necessário comunique a Assessoria de Tecnologia da Informação.
3	Caso a resolução do incidente necessite ações em terminais de usuários, auxilie a Diretoria de Infraestrutura e Redes na execução, se necessário.

Procedimento 02: Análise da criticidade do incidente

Grupo funcional:	Diretoria de Infraestrutura e Redes
Responsável:	Paulo Orlando Ricarte Kawachi
ID	Instrução
1	Analise a criticidade do incidente levando em consideração se há interrupção parcial, intermitente ou total e a abrangência da interrupção.
2	Se a interrupção for total ou parcial, acione os procedimentos de contingência conforme a abrangência da interrupção e conforme instrução 3 deste procedimento. Se a interrupção for intermitente, acione os procedimentos de contingência somente se a interrupção superar 10% do tempo, medido durante 1 hora.
3	Faça uma análise do tempo de resolução. Caso o tempo de resolução exceda um período do dia, de manhã até às 12 horas ou de tarde até às 18 horas, acione os procedimentos de contingência conforme instrução 2 deste procedimento.
4	Se a interrupção intermitente com interrupção de 10% persistir por 2 dias úteis, acione a contingência.
5	Formalize a análise em ata.

Procedimento 03: Comunicações

Grupo funcional:	Assessoria de Tecnologia da Informação
Responsável:	Eduardo Leal
ID	Instrução
1	Após análise da criticidade do incidente, avalie a necessidade da comunicação para o público externo ou interno.
2	Obtenha do grupo funcional técnico as informações do incidente para construção textual, caso a comunicação seja necessária. Tome essa ação antes, durante e depois da resolução do incidente.
3	Mantenha as principais partes interessadas informadas.
4	Se considerar necessário, poderá forçar o acionamento da contingência ou retardar o acionamento.

Procedimento 04: Resolução do incidente

Grupo funcional:	Diretoria de Infraestrutura e Redes
Responsável:	Paulo Orlando Ricarte Kawachi
ID	Instrução
1	Faça uma reunião com o grupo enumerando fatos constatados, elaborando soluções e dividindo tarefas. Repita as reuniões para cada período do dia, manhã, tarde e noite, até a resolução do incidente.
2	Caso necessário, solicite intervenção da Diretoria de Sistemas da Informação nas aplicações dos servidores.
3	Caso necessário, contate os fornecedores e os faça participar da resolução do incidente.
4	Caso necessário solicite apoio dos campi através da Assessoria de Tecnologia da Informação.
5	Documente toda tarefa realizada.

Procedimento 05: Relatório do incidente

Grupo funcional:	Diretoria de Infraestrutura e Redes
Responsável:	Paulo Orlando Ricarte Kawachi
ID	Instrução
1	Elabore relatório descrevendo o incidente ocorrido, danos causados e as ações realizadas para o retorno à normalização e as ações para entrada e saída da contingência.
2	Encaminhe relatório para a Assessoria de Tecnologia da Informação.

PlanoCoNeg02

Plano de Continuidade de Negócio - 02

Incidente:	**Indisponibilidade ou instabilidade da rede ou link de internet**
Local:	Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo
Autor:	Paulo Orlando Ricarte Kawachi
Contato:	paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento descreve as ações que devem ser tomadas em casos de acionamento da contingência. O estado de contingência só deve ser acionado após análise descrita no Plano de Gerenciamento de Incidente.

Este Plano descreve instruções que serão seguidas antes, durante e depois da contingência.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DE CONTINUIDADE DE NEGÓCIO

Procedimento 01: Antes da contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Contrate e implemente pelo menos um link de redundância e link de dados móvel (3G/4G)
2	Avalie e implemente redundâncias remotas de sistemas, caso necessário e se possível.
3	Monitore sempre que possível o desempenho da máquina principal e teste ao menos uma vez por trimestre a máquina de redundância. Os relatórios de testes devem ser guardados pelos grupos funcionais responsáveis. O último relatório de teste deve ser apresentado junto ao relatório de incidente quando houver.
4	Instrua todos os gestores da reitoria e dos campi a manterem cópia de segurança dos sistemas de colaboração.

Procedimento 02: Durante a contingência

Grupo funcional:	IFSP
Responsável:	Todos os gestores do IFSP
ID	Instrução
1	Se estiver implementado, os sistemas redundantes deverão ser ativados.
2	Se há link redundante ou link de dados móvel, estes deverão ser utilizados.
3	Durante a contingência será permitida a inserção, extração e manipulação de dados e arquivos contidos nos sistemas pela equipe de TI, caso isso seja possível. Esta ação somente deverá ser tomada com autorização da Assessoria de Tecnologia da Informação.
4	Se possível, dispense os servidores cujo todo trabalho é indispensável o uso da rede ou internet, durante a contingência. Se há tarefa para esses servidores que dispense o uso da rede ou internet, esta ação não deverá ser tomada. Se a ação da instrução 2 tiver sucesso para a abrangência necessária, esta ação não deverá ser tomada.
5	Para comunicação, utilize a telefonia convencional.
6	Monitore e registre o impacto causado pela contingência. Acrescente essa informação no relatório de incidente.

Procedimento 03: Após a contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Após resolução do incidente, encontrado a causa e o sistema ou serviço afetado reestabelecido, caso o recurso humano do grupo funcional responsável seja insuficiente para a normalização em tempo hábil, se a intervenção nos terminais de usuários seja necessária, a Assessoria de Tecnologia da Informação deverá mobilizar outros grupos da TI para auxiliar.
2	Realize testes com as partes interessadas e solicite o fechamento dos chamados, caso tenham abertos.
3	A Assessoria de Tecnologia da Informação deverá, se necessário, elaborar e publicar um comunicado para o público externo ou interno ou apenas explanar o ocorrido para as principais partes interessadas.
4	Oriente todos os colaboradores para que não divulguem ou comentem nada sobre o ocorrido, pois somente a Assessoria de Tecnologia da Informação é a responsável pela comunicação oficial da TI institucionalizada pelo órgão.
5	Se necessário, oriente e auxilie a atualização de dados e arquivos que foram tratados de modo off-line.

PlanoGeInc03

Plano de Gerenciamento de Incidentes - 03

Incidente: **Perda de dados**

Local: Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Autor: Paulo Orlando Ricarte Kawachi

Contato: paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento tem como objetivo apontar ações corretivas que serão tomadas caso algum dado, informação ou arquivo seja perdido tanto em um servidor como em um terminal de usuário.

A análise da criticidade determinará ações de contingência descritas no Plano de Continuidade de Negócio.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DO GERENCIAMENTO DE INCIDENTES

Procedimento 01: Análise da comunicação do incidente

Grupo funcional:	Gerência de Suporte e Treinamento
Responsável:	André Luis Vieira
ID	Instrução
1	Caso qualquer usuário comunique a perda dos dados, verifique onde os dados estavam armazenados e, se for em um servidor, verifique se ocorreu com outros usuários.
2	Caso necessário comunique a Assessoria de Tecnologia da Informação.
3	Caso a resolução do incidente necessite ações em terminais de usuários, auxilie o grupo funcional responsável na execução, se necessário.
4	Se os dados estavam armazenados no terminal do usuário, registre também o nome de todos os usuários daquele terminal.

Procedimento 02: Análise da criticidade do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Analise a criticidade do incidente levando em consideração a relevância dos dados perdidos, a quantidade de dados e se já se sabe quem ou o que ocasionou a perda.
2	Acione a contingência para o usuário que teve a perda de dados no seu terminal. O tempo de contingência será de 2 dias úteis, assim que o usuário autorizar.
3	Se a perda de dados for em um servidor, faça uma análise do tempo de restauração do backup. Caso o tempo de restauração exceda um período do dia, de manhã até às 12 horas ou de tarde até às 18 horas, acione os procedimentos de contingência.
4	Formalize a análise em ata.

Procedimento 03: Comunicações

Grupo funcional:	Assessoria de Tecnologia da Informação
Responsável:	Eduardo Leal
ID	Instrução
1	Após análise da criticidade do incidente, avalie a necessidade da comunicação para o público externo ou interno.
2	Obtenha do grupo funcional técnico as informações do incidente para construção textual, caso a comunicação seja necessária. Tome essa ação antes, durante e depois da resolução do incidente.
3	Mantenha as principais partes interessadas informadas e avise sobre possíveis perdas permanentes.
4	Se considerar necessário, poderá forçar o acionamento da contingência ou retardar o acionamento.

Procedimento 04: Resolução do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Faça uma reunião com o grupo enumerando fatos constatados, elaborando soluções e dividindo tarefas. Repita as reuniões para cada período do dia, manhã, tarde e noite, até a resolução do incidente.
2	Restaure o backup, se o incidente ocorrer em um servidor. Se o backup for antigo comunique a Assessoria de Tecnologia da Informação juntamente com o log de atividades recentes.
	Utilize ferramentas de recuperação de dados, se o incidente ocorrer no terminal do usuário.
2	Caso necessário, solicite auxílio de outros grupos da TI.
3	Caso necessário, contate os fornecedores e os faça participar da resolução do incidente.
5	Documente toda tarefa realizada.

Procedimento 05: Relatório do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Elabore relatório descrevendo o incidente ocorrido, danos causados e as ações realizadas para o retorno à normalização e as ações para entrada e saída da contingência.
2	Encaminhe relatório para a Assessoria de Tecnologia da Informação.

PlanoCoNeg03

Plano de Continuidade de Negócio - 03

Incidente: **Perda de dados**

Local: Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Autor: Paulo Orlando Ricarte Kawachi

Contato: paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento descreve as ações que devem ser tomadas em casos de acionamento da contingência. O estado de contingência só deve ser acionado após análise descrita no Plano de Gerenciamento de Incidente.

Este Plano descreve instruções que serão seguidas antes, durante e depois da contingência.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DE CONTINUIDADE DE NEGÓCIO

Procedimento 01: Antes da contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Implemente sistemas de backups automáticos.
2	Implemente procedimentos para backup periódico manual.
3	Monitore sempre que possível o desempenho dos servidores e teste ao menos uma vez por trimestre os backups. Os relatórios de testes devem ser guardados pelos grupos funcionais responsáveis. O último relatório de teste deve ser apresentado junto ao relatório de incidente quando houver.
4	Instrua todos os gestores da reitoria e dos campi a manterem cópia de segurança dos sistemas de colaboração e dos terminais.

Procedimento 02: Durante a contingência

Grupo funcional:	IFSP
Responsável:	Todos os gestores do IFSP
ID	Instrução
1	Durante a restauração de backup adote procedimentos de contingência do Plano de Continuidade de Negócio 01, pois o sistema afetado ficará indisponível durante o processo, caso a perda seja em um servidor.
2	Se a perda de dados for no terminal do usuário, disponibilize outro terminal de reserva durante a recuperação de dados.
3	Durante a contingência será permitida a inserção, extração e manipulação de dados e arquivos contidos nos sistemas pela equipe de TI, caso isso seja possível. Esta ação somente deverá ser tomada com autorização da Assessoria de Tecnologia da Informação.
4	Monitore e registre o impacto causado pela contingência. Acrescente essa informação no relatório de incidente.

Procedimento 03: Após a contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Após resolução do incidente, encontrado a causa e o sistema ou serviço afetado reestabelecido, caso o recurso humano do grupo funcional responsável seja insuficiente para a normalização em tempo hábil, se a intervenção nos terminais de usuários seja necessária, a Assessoria de Tecnologia da Informação deverá mobilizar outros grupos da TI para auxiliar.
2	Realize testes com as partes interessadas e solicite o fechamento dos chamados, caso tenham abertos.
3	A Assessoria de Tecnologia da Informação deverá, se necessário, elaborar e publicar um comunicado para o público externo ou interno ou apenas explanar o ocorrido para as principais partes interessadas.
4	Oriente todos os colaboradores para que não divulguem ou comentem nada sobre o ocorrido, pois somente a Assessoria de Tecnologia da Informação é a responsável pela comunicação oficial da TI institucionalizada pelo órgão.
5	Se necessário, oriente e auxilie a atualização de dados e arquivos que foram tratados de modo off-line.

PlanoGeInc04

Plano de Gerenciamento de Incidentes - 04

Incidente: **Roubo de dados**

Local: Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Autor: Paulo Orlando Ricarte Kawachi

Contato: paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento tem como objetivo apontar ações corretivas e investigativas que serão tomadas caso algum dado, informação ou arquivo interceptado, recebido ou entregue de forma não autorizada.

A análise da criticidade determinará ações de contingência descritas no Plano de Continuidade de Negócio.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DO GERENCIAMENTO DE INCIDENTES

Procedimento 01: Análise da comunicação do incidente

Grupo funcional:	Gerência de Suporte e Treinamento
Responsável:	André Luis Vieira
ID	Instrução
1	Caso qualquer usuário comunique o roubo de dados, sigilosos ou não, verifique junto ao usuário o detalhamento do caso e, após análise, comunique o grupo funcional responsável.
2	Caso necessário comunique a Assessoria de Tecnologia da Informação.
3	Caso a resolução do incidente necessite ações em terminais de usuários, auxilie o grupo funcional responsável na execução, se necessário.
4	Se os dados estavam armazenados no terminal do usuário, registre também o nome de todos os usuários daquele terminal.

Procedimento 02: Análise da criticidade do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Analise a criticidade do incidente levando em consideração a relevância dos dados roubados, se o dado é classificado como sigiloso ou não, se foi roubado de um servidor, no tráfego ou do terminal do usuário e se já se sabe quem roubou.
2	Acione a contingência para o usuário que teve roubo de dados do seu terminal. O tempo de contingência será de 2 dias úteis, assim que o usuário autorizar.
3	Se o roubo de dados for de um servidor ou no tráfego, faça uma análise do tempo de investigação. Caso necessário estabeleça um tempo de isolamento não superior a 2 dias úteis. Se o tempo de isolamento exceder um período do dia, de manhã até às 12 horas ou de tarde até às 18 horas, acione os procedimentos de contingência.
4	Formalize a análise em ata.

Procedimento 03: Comunicações

Grupo funcional:	Assessoria de Tecnologia da Informação
Responsável:	Eduardo Leal
ID	Instrução
1	Após análise da criticidade do incidente, avalie a necessidade da comunicação para o público externo ou interno.
2	Obtenha do grupo funcional técnico as informações do incidente para construção textual, caso a comunicação seja necessária. Tome essa ação antes, durante e depois da resolução do incidente.
3	Mantenha as principais partes interessadas informadas.
4	Se considerar necessário, poderá forçar o acionamento da contingência ou retardar o acionamento.

Procedimento 04: Resolução do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Faça uma reunião com o grupo enumerando fatos constatados, elaborando soluções e dividindo tarefas. Repita as reuniões para cada período do dia, manhã, tarde e noite, até a resolução do incidente.
2	Se necessário, isole o ativo afetado durante a investigação, tornando impossível qualquer ação adicional do indivíduo que roubou os dados.
3	Caso necessário, solicite auxílio de outros grupos da TI.
4	Caso necessário, contate os fornecedores e os faça participar da resolução do incidente.
5	Documente toda tarefa realizada.

Procedimento 05: Relatório do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Elabore relatório descrevendo o incidente ocorrido, danos causados e as ações realizadas para o retorno à normalização e as ações para entrada e saída da contingência.
2	Encaminhe relatório para a Assessoria de Tecnologia da Informação.

PlanoCoNeg04

Plano de Continuidade de Negócio - 04

Incidente: **Roubo de dados**

Local: Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Autor: Paulo Orlando Ricarte Kawachi

Contato: paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento descreve as ações que devem ser tomadas em casos de acionamento da contingência. O estado de contingência só deve ser acionado após análise descrita no Plano de Gerenciamento de Incidente.

Este Plano descreve instruções que serão seguidas antes, durante e depois da contingência.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DE CONTINUIDADE DE NEGÓCIO

Procedimento 01: Antes da contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Implemente repositório central de log de atividade.
2	Implemente ferramentas de monitoramento de rede.
3	Verifique a segurança dos terminais de usuários.
4	Instrua todos os gestores da reitoria e dos campi a seguirem recomendações típicas de segurança da informação, como mesa limpa, tela limpa e senha segura.

Procedimento 02: Durante a contingência

Grupo funcional:	IFSP
Responsável:	Todos os gestores do IFSP
ID	Instrução
1	Durante a investigação em isolamento adote procedimentos de contingência do Plano de Continuidade de Negócio 01, pois o sistema afetado ficará indisponível durante o processo, caso o roubo seja de um servidor.
2	Se o roubo de dados for do terminal do usuário, disponibilize outro terminal de reserva durante a investigação, se necessário.
3	Monitore e registre o impacto causado pela contingência. Acrescente essa informação no relatório de incidente.

Procedimento 03: Após a contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Após resolução do incidente, encontrado a causa e o sistema ou serviço afetado reestabelecido, caso o recurso humano do grupo funcional responsável seja insuficiente para a normalização em tempo hábil, se a intervenção nos terminais de usuários seja necessária, a Assessoria de Tecnologia da Informação deverá mobilizar outros grupos da TI para auxiliar.
2	Realize testes com as partes interessadas e solicite o fechamento dos chamados, caso tenham abertos.
3	A Assessoria de Tecnologia da Informação deverá, se necessário, elaborar e publicar um comunicado para o público externo ou interno ou apenas explanar o ocorrido para as principais partes interessadas.
4	Oriente todos os colaboradores para que não divulguem ou comentem nada sobre o ocorrido, pois somente a Assessoria de Tecnologia da Informação é a responsável pela comunicação oficial da TI institucionalizada pelo órgão.
5	Se necessário, oriente e auxilie a atualização de dados e arquivos que foram tratados de modo off-line.

PlanoGeInc05

Plano de Gerenciamento de Incidentes - 05

Incidente:	**Modificação não autorizada de servidor**
Local:	Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo
Autor:	Paulo Orlando Ricarte Kawachi
Contato:	paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento tem como objetivo apontar ações corretivas e investigativas que serão tomadas caso algum sistema sofra modificações sem o conhecimento da equipe de TI.

A análise da criticidade determinará ações de contingência descritas no Plano de Continuidade de Negócio.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DO GERENCIAMENTO DE INCIDENTES

Procedimento 01: Análise da comunicação do incidente

Grupo funcional:	Gerência de Suporte e Treinamento
Responsável:	André Luis Vieira
ID	Instrução
1	Caso qualquer usuário comunique a modificação em um servidor, constate a modificação e confirme se realmente não foi autorizado e então comunique o grupo funcional responsável.
2	Caso necessário comunique a Assessoria de Tecnologia da Informação.
3	Caso a resolução do incidente necessite ações em terminais de usuários, auxilie o grupo funcional responsável na execução, se necessário.

Procedimento 02: Análise da criticidade do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Analise a criticidade do incidente levando em consideração o grau de modificação, ofensividade da modificação, se a modificação está causando outro incidente de segurança ou não e se a modificação é facilmente reversível ou não.
3	Faça uma análise do tempo de investigação. Caso necessário estabeleça um tempo de isolamento não superior a 2 dias úteis. Se o tempo de isolamento exceder um período do dia, de manhã até às 12 horas ou de tarde até às 18 horas, acione os procedimentos de contingência.
4	Formalize a análise em ata.

Procedimento 03: Comunicações

Grupo funcional:	Assessoria de Tecnologia da Informação
Responsável:	Eduardo Leal
ID	Instrução
1	Após análise da criticidade do incidente, avalie a necessidade da comunicação para o público externo ou interno.
2	Obtenha do grupo funcional técnico as informações do incidente para construção textual, caso a comunicação seja necessária. Tome essa ação antes, durante e depois da resolução do incidente.
3	Mantenha as principais partes interessadas informadas.
4	Se considerar necessário, poderá forçar o acionamento da contingência ou retardar o acionamento.

Procedimento 04: Resolução do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Faça uma reunião com o grupo enumerando fatos constatados, elaborando soluções e dividindo tarefas. Repita as reuniões para cada período do dia, manhã, tarde e noite, até a resolução do incidente.
2	Se necessário, isole o ativo afetado durante a investigação, tornando impossível qualquer ação adicional do indivíduo que realizou modificações.
3	Caso necessário, solicite auxílio de outros grupos da TI.
4	Caso necessário, contate os fornecedores e os faça participar da resolução do incidente.
5	Documente toda tarefa realizada.

Procedimento 05: Relatório do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Elabore relatório descrevendo o incidente ocorrido, danos causados e as ações realizadas para o retorno à normalização e as ações para entrada e saída da contingência.
2	Encaminhe relatório para a Assessoria de Tecnologia da Informação.

PlanoCoNeg05

Plano de Continuidade de Negócio - 05

Incidente: **Modificação não autorizada de servidor**

Local: Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Autor: Paulo Orlando Ricarte Kawachi

Contato: paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento descreve as ações que devem ser tomadas em casos de acionamento da contingência. O estado de contingência só deve ser acionado após análise descrita no Plano de Gerenciamento de Incidente.

Este Plano descreve instruções que serão seguidas antes, durante e depois da contingência.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DE CONTINUIDADE DE NEGÓCIO

Procedimento 01: Antes da contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Implemente repositório central de log de atividade.
2	Implemente ferramentas de monitoramento de rede.
3	Verifique a segurança dos terminais de usuários.
4	Instrua todos os gestores da reitoria e dos campi a seguirem recomendações típicas de segurança da informação, como mesa limpa, tela limpa e senha segura.

Procedimento 02: Durante a contingência

Grupo funcional:	IFSP
Responsável:	Todos os gestores do IFSP
ID	Instrução
1	Durante a investigação em isolamento adote procedimentos de contingência do Plano de Continuidade de Negócio 01, pois o sistema afetado ficará indisponível durante o processo, caso o roubo seja de um servidor.
2	Monitore e registre o impacto causado pela contingência. Acrescente essa informação no relatório de incidente.

Procedimento 03: Após a contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Após resolução do incidente, encontrado a causa e o sistema ou serviço afetado reestabelecido, caso o recurso humano do grupo funcional responsável seja insuficiente para a normalização em tempo hábil, se a intervenção nos terminais de usuários seja necessária, a Assessoria de Tecnologia da Informação deverá mobilizar outros grupos da TI para auxiliar.
2	Realize testes com as partes interessadas e solicite o fechamento dos chamados, caso tenham abertos.
3	A Assessoria de Tecnologia da Informação deverá, se necessário, elaborar e publicar um comunicado para o público externo ou interno ou apenas explanar o ocorrido para as principais partes interessadas.
4	Oriente todos os colaboradores para que não divulguem ou comentem nada sobre o ocorrido, pois somente a Assessoria de Tecnologia da Informação é a responsável pela comunicação oficial da TI institucionalizada pelo órgão.
5	Se necessário, oriente e auxilie a atualização de dados e arquivos que foram tratados de modo off-line.

PlanoGeInc06

Plano de Gerenciamento de Incidentes - 06

Incidente: **Utilização indevida de recurso de TI**

Local: Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Autor: Paulo Orlando Ricarte Kawachi

Contato: paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento tem como objetivo apontar ações corretivas e investigativas que serão tomadas caso algum sistema seja utilizado para fins que não foram projetados pela equipe de TI.

A análise da criticidade determinará ações de contingência descritas no Plano de Continuidade de Negócio.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DO GERENCIAMENTO DE INCIDENTES

Procedimento 01: Análise da comunicação do incidente

Grupo funcional:	Gerência de Suporte e Treinamento
Responsável:	André Luis Vieira
ID	Instrução
1	Caso qualquer usuário comunique a utilização indevida dos recursos de TI, constate o incidente e então comunique o grupo funcional responsável.
2	Caso necessário comunique a Assessoria de Tecnologia da Informação.
3	Caso a resolução do incidente necessite ações em terminais de usuários, auxilie o grupo funcional responsável na execução, se necessário.

Procedimento 02: Análise da criticidade do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Analise a criticidade do incidente levando em consideração se foi utilizado um servidor ou um terminal de usuário, se causou outros incidentes de segurança, se foi um ato criminal ou não, se foi culposo ou não ou se foi um indivíduo interno ou externo.
3	Faça uma análise do tempo de investigação. Caso necessário estabeleça um tempo de isolamento não superior a 2 dias úteis. Se o tempo de isolamento exceder um período do dia, de manhã até às 12 horas ou de tarde até às 18 horas, acione os procedimentos de contingência.
4	Formalize a análise em ata.

Procedimento 03: Comunicações

Grupo funcional:	Assessoria de Tecnologia da Informação
Responsável:	Eduardo Leal
ID	Instrução
1	Após análise da criticidade do incidente, avalie a necessidade da comunicação para o público externo ou interno.
2	Obtenha do grupo funcional técnico as informações do incidente para construção textual, caso a comunicação seja necessária. Tome essa ação antes, durante e depois da resolução do incidente.
3	Mantenha as principais partes interessadas informadas.
4	Se considerar necessário, poderá forçar o acionamento da contingência ou retardar o acionamento.

Procedimento 04: Resolução do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Faça uma reunião com o grupo enumerando fatos constatados, elaborando soluções e dividindo tarefas. Repita as reuniões para cada período do dia, manhã, tarde e noite, até a resolução do incidente.
2	Se necessário, isole o ativo afetado durante a investigação, tornando impossível qualquer ação adicional do indivíduo que realizou modificações.
3	Caso necessário, solicite auxílio de outros grupos da TI.
4	Caso necessário, contate os fornecedores e os faça participar da resolução do incidente.
5	Documente toda tarefa realizada.

Procedimento 05: Relatório do incidente

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Elabore relatório descrevendo o incidente ocorrido, danos causados e as ações realizadas para o retorno à normalização e as ações para entrada e saída da contingência.
2	Encaminhe relatório para a Assessoria de Tecnologia da Informação.

PlanoCoNeg06

Plano de Continuidade de Negócio - 06

Incidente: **Utilização indevida de recurso de TI**

Local: Reitoria do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Autor: Paulo Orlando Ricarte Kawachi

Contato: paulo.ok@ifsp.edu.br **Fone comercial:** +55 (11) 3775-4553

Objetivo

Este documento descreve as ações que devem ser tomadas em casos de acionamento da contingência. O estado de contingência só deve ser acionado após análise descrita no Plano de Gerenciamento de Incidente.

Este Plano descreve instruções que serão seguidas antes, durante e depois da contingência.

Contatos

RESPONSÁVEIS PELA EXECUÇÃO

Grupo funcional: Assessoria de Tecnologia da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Eduardo Leal	Assessor	+55 (11) 3775-4552	leal@ifsp.edu.br

Grupo funcional: Diretoria de Infraestrutura e Redes

Nome	Cargo/Função	Telefone(s)	E-mail
Paulo Orlando Ricarte Kawachi	Diretor	+55 (11) 3775-4553	paulo.ok@ifsp.edu.br
Bruno Jamalaro	Coordenador de Infraestrutura e Serviços	+55 (11) 3775-4553	bruno.jamalaro@ifsp.edu.br

Grupo funcional: Diretoria de Sistemas da Informação

Nome	Cargo/Função	Telefone(s)	E-mail
Brunno dos Passos Alves	Diretor	+55 (11) 3775-4558	brunno.alves@ifsp.edu.br
Thiago Vieira da Silva	Coordenador de Projetos de Sistema	+55 (11) 3775-4558	cops@ifsp.edu.br
Ronaldo Tadashi Yonamine	Coordenador de Banco de Dados	+55 (11) 3775-4558	cad@ifsp.edu.br
Danilo da Silva Rocha	Coordenador de Qualidade e Testes	+55 (11) 3775-4558	cgt@ifsp.edu.br

Grupo funcional: Gerência de Suporte e Treinamento

Nome	Cargo/Função	Telefone(s)	E-mail
André Luis Vieira	Gerente	+55 (11) 3775-4556	andrevieira@ifsp.edu.br
Carlos Roberto Feitoza de Melo	Coordenador de Monitoramento e Operação	+55 (11) 3775-4556	carlosfeitoza@ifsp.edu.br

PROCEDIMENTOS DE CONTINUIDADE DE NEGÓCIO

Procedimento 01: Antes da contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Implemente repositório central de log de atividade.
2	Implemente ferramentas de monitoramento de rede.
3	Verifique a segurança dos terminais de usuários.
4	Instrua todos os gestores da reitoria e dos campi a seguirem recomendações típicas de segurança da informação, como mesa limpa, tela limpa e senha segura.

Procedimento 02: Durante a contingência

Grupo funcional:	IFSP
Responsável:	Todos os gestores do IFSP
ID	Instrução
1	Durante a investigação em isolamento adote procedimentos de contingência do Plano de Continuidade de Negócio 01, pois o sistema afetado ficará indisponível durante o processo, caso o roubo seja de um servidor.
2	Monitore e registre o impacto causado pela contingência. Acrescente essa informação no relatório de incidente.

Procedimento 03: Após a contingência

Grupo funcional:	Equipe de Tecnologia da Informação
Responsável:	Todos os gestores de Tecnologia da Informação
ID	Instrução
1	Após resolução do incidente, encontrado a causa e o sistema ou serviço afetado reestabelecido, caso o recurso humano do grupo funcional responsável seja insuficiente para a normalização em tempo hábil, se a intervenção nos terminais de usuários seja necessária, a Assessoria de Tecnologia da Informação deverá mobilizar outros grupos da TI para auxiliar.
2	Realize testes com as partes interessadas e solicite o fechamento dos chamados, caso tenham abertos.
3	A Assessoria de Tecnologia da Informação deverá, se necessário, elaborar e publicar um comunicado para o público externo ou interno ou apenas explanar o ocorrido para as principais partes interessadas.
4	Oriente todos os colaboradores para que não divulguem ou comentem nada sobre o ocorrido, pois somente a Assessoria de Tecnologia da Informação é a responsável pela comunicação oficial da TI institucionalizada pelo órgão.
5	Se necessário, oriente e auxilie a atualização de dados e arquivos que foram tratados de modo off-line.