Normas para o Administrador do serviço de e-mail

Os serviços de e-mails oferecidos pela USP - **Universidade de São Paulo -** impõem responsabilidades e obrigações a seus Administradores, com o objetivo de colaborar para que o sistema seja eficaz, eficiente e seguro, preservando dados, mantendo a integridade da segurança dos sistemas.

Será indicado pela Unidade dois Administradores de e-mail. Deverá ser repassada essa informação ao CCE e ao Centro de Informática, informando, nome completo, ramal e e-mail do mesmo.

O Administrador DEVE:

- Zelar pelo cumprimento das Normas de segurança;
- Preservar a integridade e a segurança dos sistemas;
- Acessar a interface gráfica de administração de e-mail de sua Unidade;
- Administrar contas de e-mail;
- Resetar senhas e alterar senhas a pedido dos usuários e ter a plena certeza que a solicitação partiu do usuário legítimo;
- Saber as regras tratadas a respeito dos espaços destinados as contas dos usuários. Essas regras devem ser seguidas. Cada Campus possui regras para definirmos os espaços (quotas) de seus usuários. Caso os usuários solicitem aumentos de quotas será necessário consultar o CI ou CCE antes de executar qualquer alteração;
- Solicitar ao CCE a restauração de backup da área de usuário;
- Gerenciar o bloqueio e desbloqueio de usuários. Portanto, antes de efetuar o desbloqueio do usuário o administrador deve verificar o motivo pelo qual foi bloqueado e se pode ser desbloqueado;
- Acessar os arquivos dos usuários somente quando for indispensável para manutenção do sistema, ou em casos de perícia, auditoria e incidentes de Segurança;
- Informar aos usuários sobre os mecanismos de correção de vulnerabilidades recomendáveis;
- Participar da lista de discussão dos Administradores de rede da USP;

- Acessar as páginas de segurança mantidas pela administração centralizada de informática da Universidade ou pelos Centros de Informática;
- Utilizar ferramentas apropriadas para acesso aos servidores de serviços;
- Gerenciar, adequadamente, os privilégios de usuários, as senhas de usuários, certificados digitais, os procedimentos de logon (shell scripts), de desconexão de usuários por inatividade e de política de troca de senha;
- Conhecer a Resolução Nº 4871, que estabelece o "Código de Ética da Universidade de São Paulo";
- Interagir com os Centros de Informática para troca de conhecimentos sobre ferramentas apropriadas a serem utilizadas para segurança e gerenciamento dos serviços;
- Administração de Listas;
- Checar, periodicamente, o servidor de correio eletrônico para determinar se existem endereços de e-mail inválidos nas listas disponibilizadas pelo servidor. Se a lista for administrada por outra pessoa, o Administrador deve contatá-la para que seja feita a remoção desses endereços inválidos;
- Configurar o servidor de listas para que o Usuário não possa executar determinados comandos (por exemplo, "who" para listar todos os usuários que façam parte da lista);
- Configurar um tamanho máximo para todas as mensagens que circulem através do servidor de listas;
- Remover endereços inscritos em listas de discussão, caso eles estejam retornando;
- Configurar o servidor de listas e, principalmente, seus inscritos devem ser rigorosamente controlados e limitados apenas ao Administrador (ou dono) da lista;
- Configurar o servidor de listas para que em todos os e-mails que circulem por ela seja incluída informação ao Usuário de como ele deve proceder para se descadastrar da lista, contatar um Administrador e receber outras informações;

O Administrador NÃO DEVE:

- Compartilhar senha ou o login de outra(s) pessoa(s);
- Escolher um código de usuário (login) para usuários;
- Divulgar a identificação e/ou senha de acesso de usuários;

- Utilizar a identificação e senha de acesso, arquivos e dados de usuários;
- Tentar enganar ou subverter as medidas de segurança dos sistemas;
- Passar por outra pessoa ou dissimular sua identidade quando estiver administrando os serviços e recursos de e-mail;
- Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos ao sistema e às informações armazenadas, tais como criação e propagação de vírus, criação e utilização de sistemas de criptografia que causem a indisponibilidade dos serviços e/ou destruição de dados;
- Tentar quebrar o sigilo de códigos alheios, ou tentar ter acesso a contas de usuários para encaminhamento de e-mails, modificações de arquivos ou qualquer outro ato que seja considerado indevido;
- Utilizar os serviços e recursos de e-mail para atividades direta ou indiretamente relacionadas a projetos, desenvolvimento, fabricação ou testes de aparato nuclear, armas químicas e biológicas, e criptografia;
- Utilizar os serviços e recursos de e-mail para fins comerciais, políticos, religiosos ou ideológicos tais como mala direta ou propagandas;
- Utilizar de documentação ou informação que tenha propriedade registrada, para ser copiada, modificada, disseminada ou usada, no todo ou em parte, e repassada por e-mail sem a permissão expressa do detentor do copyright;
- Utilizar os serviços e recursos de e-mail para negócios ou ganho pessoal;.
- Utilizar os serviços e recursos de e-mail para intimidar, assediar, difamar ou aborrecer qualquer pessoa;
- Utilizar os serviços e recursos de e-mail para armazenar, divulgar ou transmitir material (som e vídeo) ofensivo e abusivo;
- Desenvolver qualquer outra atividade que desobedeça as normas apresentadas acima;
- Sobrecarregar o sistema. Portanto, não deve utilizar ferramentas que remetam diversos e-mails a vários usuários sobre um determinado assunto, enfim que sejam considerados SPAMs;
- Violar ou tentar violar os sistemas de e-mail , quebrando ou tentando adivinhar a identidade eletrônica de usuários, senhas;

- Interceptar ou tentar interceptar a transmissão de dados através de monitoração, exceto quando autorizado, explicitamente, pelo superior hierárquico, com prévio conhecimento do Centro de Informática do campus;
- Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais da Universidade;
- Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus e worms, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, engajar-se em ações que possam ser caracterizadas como violação da segurança computacional;
- Ler mensagens de seus usuários, a não ser em casos em que se suspeite que a mensagem possa ser um spam ou desviar-se dos propósitos estabelecidos nesse documento, por exemplo, após o Administrador verificar a fila de mensagens do sistema e detectar alguma irregularidade.

Responsabilidades

O administrador é responsável por:

- Todas as atividades originadas a partir de sua identificação;
- Pelas consequências caso execute algumas das atitudes relacionadas nos itens acima;

Penalidades

O não cumprimento das regras definidas nos itens I e II, acarretará ao Administrador:

- As penalidades cabíveis, podendo resultar até em ação legal por parte da USP;

O Centro de Informática, Instituto ou Unidade de Ensino e Pesquisa deve avaliar as infrações ocorridas no âmbito de sua responsabilidade através de uma Comissão instituída. Cabe ainda a esses Órgãos aplicar ou recomendar as penalidades para cada caso.

Validade

- Fica a cargo do Administrador informar ao seu superior imediato sua não concordância em ser o Administrador.
- O superior imediato também poderá indicar outro funcionário para ser o Administrador do sistema.

Administrador CCE

Os serviços de e-mails oferecidos pela USP - **Universidade de São Paulo**, impõem responsabilidades e obrigações a seus Administradores, com o objetivo de colaborar para que o sistema seja eficaz, eficiente e seguro, preservando dados, mantendo a integridade da segurança dos sistemas.

O administrador do CCE deve verificar e cumprir os deveres e não deveres do administrador da Unidade e, também, verificar e cumprir os deveres e não deveres descritos abaixo, portanto, o Administrador do CCE DEVE:

- Cumprir as regras e diretrizes definidas nos itens acima;
- Preservar a integridade e a segurança dos sistemas;
- Manter os registros e logs de utilização dos serviços;
- Armazenar registros e logs em dispositivos de backup;
- Manter o backup dos dados dos usuários;
- Após a solicitação do administrador da Unidade, restaurar o backup de dados do usuário em um prazo de 48 horas, caso seja possível;
- Configurar o servidor de correio eletrônico de maneira a evitar problemas do tipo "*open-relay*", "*open-proxy*", "*formmail*" e outros;
- Fazer mecanismos do tipo POP3, IMAP, HTTP (Webmail), de preferência utilizando as versões mais seguras desses protocolos APOP, SMTP-AUTH, POP com SSH, HTTPS;
- Providenciar o cadastramento do endereço do servidor de e-mail no DNS com o nome e o reverso;
- Fornecer registros e logs somente à administração central de informática da Universidade, ou a quem ela indicar;

- Acessar os arquivos dos usuários somente quando for indispensável para manutenção do sistema, ou em casos de perícia, auditoria e incidentes de Segurança;

- Manter o sincronismo NTP em todos servidores responsáveis pelo fornecimento de algum serviço de rede;

- Atualizar os sistemas aplicando mecanismos de correção (atualizações);

- Informar aos usuários sobre os mecanismos de correção de vulnerabilidades recomendáveis.

O administrador do CCE deve verificar o cumprimento dos deveres e não deveres do administrador da Unidade e, também, verificar e cumprir os deveres e não deveres descritos abaixo, portanto, o Administrador do CCE não DEVE:

- Interceptar ou tentar interceptar a transmissão de dados através de monitoração, exceto quando autorizado, explicitamente, pelo superior hierárquico, com prévio conhecimento do Centro de Informática do campus,

- Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais da Universidade;

- Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus e worms, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, engajar-se em ações que possam ser caracterizadas como violação da segurança computacional;

Recomenda-se:

- Que o servidor de correio eletrônico seja configurado para enviar email só após a autenticação do Usuário, utilizando configurações do tipo "smtp auth", "smtp after pop";

- Que o Administrador implemente medidas para filtragem de vírus no sistema de correio eletrônico;

- Que o Administrador implemente medidas para filtragem de spam e emails indesejados (correntes, mensagens pornográficas, propagandas, etc.) no sistema de correio eletrônico;

- Que o Administrador implemente medidas para limitar o tamanho das caixas postais de seus usuários, por exemplo, utilizando um mecanismo de quota;

- Que o servidor de correio eletrônico seja configurado de forma que o Usuário não tenha acesso de "login" ao servidor;

- Que o Administrador monitore o funcionamento do servidor de correio eletrônico, em termos de número de conexões, número de mensagens enviadas e recebidas, número de mensagens bloqueadas, banda consumida na rede.