UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA STI/POSIN 06 – CONTROLE DE ACESSO LÓGICO

Devido à natureza da Universidade, deve haver um livre fluxo de informação e intercâmbio de ideias. Por outro lado, existem impedimentos legais e éticos a determinadas ações, que implicam em responsabilidades atribuídas tanto a Ufes quanto ao usuário. Por isso, a Ufes deverá usar instrumentos para o rastreamento de tais ações, para que seja possível a determinação do responsável por um ato ilícito.

Deve haver um sistema único de autenticação de caráter pessoal (cada pessoa com uma única identificação, vinculada a ela e não ao cargo que ocupa). As informações para autenticação devem ser consideradas pessoais e intransferíveis, não podendo a Ufes armazená-las de forma que permita a sua recuperação, nem o usuário divulgá-las sob qualquer pretexto.

O acesso aos sistemas corporativos da Ufes utilizará *login* como forma de estabelecer permissões e gerenciar o que cada perfil do usuário poderá acessar podendo ser exigidas etapas adicionais no processo de autenticação. Poderão ainda ser estabelecidas exigências quanto às características do equipamento utilizado no acesso, incluindo o seu registro em um sistema de inventário.

Os controles de acesso devem ser aplicados nos seguintes âmbitos:

- Controle de Acesso Lógico: Permite que os sistemas de TIC verifiquem a identidade dos usuários que tentam utilizar seus serviços. Deve ainda utilizar a legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto, no âmbito da rede corporativa, por meio de canal seguro.
- Controle de Acesso Físico: Por questão de segurança, os ativos sensíveis devem ser protegidos fisicamente e acessíveis apenas às pessoas autorizadas.

Todas as contas de acesso aos ativos de informação e as instalações físicas da Ufes deverão ser revogadas ou suspensas quando não mais necessárias, conforme normas e legislação específica em vigor.

Do mesmo modo, dispositivos usados para autenticação, tais como cartões, tokens e afins, devem ser guardados com zelo e o seu extravio imediatamente comunicado a Superintendência de Tecnologia da Informação (STI) ou ao órgão emissor.

1. ACESSO À INTERNET

Conforme estabelecido na Política de Uso da Rede Ipê (disponível em https://www.rnp.br/arquivos/doc0108d.pdf), a Ufes pode utilizar os Serviços de Redes disponíveis, suas facilidades de trânsito nacional e internacional, bem como usufruir dos acordos de interconexão existentes entre a RNP e outras redes estaduais, regionais e internacionais para promoção de suas atividades de ensino, pesquisa e extensão.

2. REDE SEM FIO (WI-FI)

A Ufes deverá oferecer uma solução de cobertura de rede sem fio baseado no padrão 802.11 para todos os seus campi. Quaisquer equipamentos que forneçam acesso Wi-Fi (*Access Points* – AP) funcionando sem a exigência de autenticação e/ou não permitam rastreamento das conexões deverão ser desligados e removidos.

Não serão permitidos equipamentos que forneçam acesso à rede Ufes, inclusive Wi-Fi (*Access Points – AP*), que não sejam os providos oficialmente pela Ufes ou que possuam autorização expressa da Superintendência de Tecnologia da Informação (STI). Essa autorização considerará os mecanismos de segurança existentes no equipamento e os riscos à segurança de dados na infraestrutura de TIC da Ufes.

3. POLÍTICA DE SENHA

Esta seção estabelece os princípios que devem ser observados, por todos os usuários no âmbito da Ufes, no uso de senhas de acesso de forma a preservar a segurança das informações. Adicionalmente estabelece os critérios de responsabilidades no uso e gerenciamento de senhas.

A Ufes utiliza de uma gestão centralizada de senhas chamada Login Único, cujo intuito é garantir um acesso facilitado aos portais corporativos da instituição, pois tira a obrigação do usuário de memorizar várias senhas para sistemas diferentes.

Toda a gerência do Login Único é feita através do sítio https://senha.ufes.br.

3.1 FORMATO DA SENHA

- A senha deverá ter o tamanho mínimo de 8 (oito) caracteres;
- A senha deverá obedecer aos seguintes critérios:

- Utilizar letras maiúsculas;
- Utilizar letras minúsculas;
- Utilizar caracteres especiais;
- Utilizar números;
- A STI se reserva no direito de proibir o uso de certas combinações como, por exemplo, data de nascimento, nome e outras informações pessoais que tornem a senha mais suscetível a ataques de engenharia social.

3.2 RESPONSABILIDADES DOS USUÁRIOS

- O usuário é o responsável pela sua senha, sendo essa de uso pessoal e intransferível;
- O usuário titular das credenciais de acesso terá total responsabilidade pelo seu uso;
- Nenhum usuário está autorizado a solicitar a senha de outros usuários;
- Cuidar para que ninguém observe o momento da digitação da senha;
- Nunca aceitar ou solicitar ajuda de estranhos na digitação de senha;
- Comunicar imediatamente ao superior imediato e/ou ao setor responsável pela Segurança da Informação (SI) os casos de violação das credenciais, acidental ou não, e providenciar a sua substituição;
- O usuário deverá trocar a senha periodicamente a cada 6 (seis) meses;
- Evitar o acesso aos sistemas corporativos da Ufes a partir de computadores que possam estar com a segurança comprometida, assim como a partir de redes públicas ou redes privadas não confiáveis.

3.3 RESPONSABILIDADES DA STI

- Prover e manter sistema de guarda, criação e alteração das credenciais dos usuários;
- Garantir que a senha do usuário sempre trafegue por canal seguro (criptografada);
- Bloquear ou desabilitar as credenciais em casos de suspeitas de fraudes ou mal-uso, determinação administrativa ou judicial;
- Armazenar as senhas em sistema seguro, de forma criptografada e irreversível;

- Implementar mecanismos adicionais de segurança, podendo solicitar a colaboração do usuário;

4. MONITORAMENTO

O monitoramento tem por objetivo detectar atividades não autorizadas de processamento da informação. Sendo assim, os sistemas devem ser monitorados e eventos de segurança da informação devem ser registrados.

Registros de operador e registros de falhas devem ser utilizados para assegurar que os problemas de sistemas de informação sejam identificados.

O monitoramento do sistema deve ser utilizado para checar a eficácia dos controles adotados e para verificar a conformidade com o modelo de política de acesso.

4.1 REGISTROS DE AUDITORIA

Registros de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos por um período acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.

Os registros (*log*) de auditoria devem incluir, quando relevante:

- Identificação dos usuários;
- Datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (*logon*) e saída (*logoff*) no sistema;
- Identidade do terminal ou, quando possível, a sua localização;
- Registros das tentativas de acesso ao sistema aceitas e rejeitadas;
- Registros das tentativas de acesso a outros recursos e dados aceitos e rejeitados;
- Alterações na configuração do sistema;
- Uso de privilégios;
- Uso de aplicações e utilitários do sistema;
- Arquivos acessados e tipo de acesso;
- Endereços e protocolos de rede.

Os registros (*log*) de auditoria podem conter dados pessoais confidenciais e de intrusos. Convém que medidas apropriadas de proteção de privacidade sejam tomadas. Quando

possível, convém também que administradores de sistemas e de rede não tenham permissão de exclusão ou desativação dos registros (*log*) de suas próprias atividades.

4.2 REGISTROS DE FALHAS

As falhas ocorridas devem ser registradas e analisadas sob demanda, e devem ser adotadas ações apropriadas. É importante que existam regras claras para o tratamento das falhas, incluindo:

- Análise crítica dos registros (*log*) de falha para assegurar que as falhas foram satisfatoriamente resolvidas; e
- Análise crítica das medidas corretivas para assegurar que os controles não foram comprometidos e que a ação tomada é autorizada.

Deve ser assegurada que a coleta dos registros de erros e alertas é permitida, caso essa função do sistema esteja disponível.

Registros de falhas e erros podem impactar o desempenho do sistema. Convém que cada tipo de registro a ser coletado seja permitido por pessoas competentes e que o nível de registro requerido para cada sistema individual seja determinado por uma análise/avaliação de riscos, levando em consideração a degradação do desempenho do sistema.

4.3 REGISTROS DE ADMINISTRADOR E OPERADOR

As atividades dos administradores e operadores do sistema devem ser registradas. Esses registros (*log*) devem incluir:

- A hora em que o evento ocorreu;
- Se o acesso resultou em sucesso ou falha;
- Informações sobre o evento (exemplo: arquivos manuseados, IP, porta de entrada da conexão) ou falha (exemplo: erros ocorridos e ações corretivas adotadas);
- Que conta e que administrador ou operador estava envolvido.

Os registros (*log*) de atividades dos operadores e administradores dos sistemas devem ser analisados criticamente caso ocorra algum incidente.

Um sistema de detecção de intrusos, gerenciado fora do controle dos administradores de rede e de sistemas, pode ser utilizado para monitorar a conformidade das atividades dos

administradores do sistema e da rede.

4.4 PROTEÇÃO DAS INFORMAÇÕES DOS REGISTROS

Os recursos e informações de registros (*log*) devem ser protegidos contra falsificação e acesso não autorizado.

Os controles implementados devem objetivar a proteção contra modificações não autorizadas e problemas operacionais com os recursos dos registros (*log*), tais como:

- Alterações dos tipos de mensagens que são gravadas;
- Arquivos de registros (*log*) sendo editados ou excluídos; e
- Capacidade de armazenamento da mídia magnética do arquivo de registros (*log*) excedida, resultando em falhas no registro de eventos ou sobreposição do registro de evento anterior.

Alguns registros (*log*) de auditoria podem ser guardados como parte da política de retenção de registros ou devido aos requisitos para a coleta e retenção de evidência.

Registros (*log*) de sistema normalmente contêm um grande volume de informações e muitos dos quais não dizem respeito ao monitoramento da segurança. Para ajudar a identificar eventos significativos para propósito de monitoramento de segurança, convém que a cópia automática dos tipos de mensagens para a execução de consulta seja considerada e/ou o uso de sistemas utilitários adequados ou ferramentas de auditoria para realizar a racionalização e investigação do arquivo seja considerado.

Registros (*log*) de sistema precisam ser protegidos, pois os dados podem ser modificados e excluídos e suas ocorrências podem causar falsa impressão de segurança.

4.5 MONITORAMENTO DO USO DO SISTEMA

Devem ser estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento devem ser analisados, criticamente, de forma regular.

O nível de monitoramento requerido para os recursos individuais deve ser determinado através de uma análise/avaliação de riscos. Convém que a organização esteja de acordo

com todos os requisitos legais relevantes, aplicáveis para suas atividades de monitoramento. As seguintes áreas devem ser consideradas:

- Acessos autorizados, incluindo detalhes como o identificador do usuário (ID de usuário), a data e o horário dos eventos-chave, tipo do evento, os arquivos acessados e os programas ou utilitários utilizados;
- Todas as operações privilegiadas, tais como o uso de contas privilegiadas (por exemplo: supervisor, *root*, administrador), a inicialização e finalização do sistema, e a conexão e desconexão de dispositivos de entrada e saída;
- Tentativas de acesso não autorizadas, tais como ações de usuários com falhas ou rejeitados, ações envolvendo dados ou outros recursos com falhas ou rejeitadas, violação de políticas de acesso e notificações para *gateways* de rede e *firewalls* e alertas dos sistemas proprietários de detecção de intrusos;
- Alertas e falhas do sistema, tais como alertas ou mensagens do *console*, registro das exceções do sistema, alarmes do gerenciamento da rede e alarmes disparados pelo sistema de controle de acesso; e
- Alterações ou tentativas de alterações nos controles e parâmetros dos sistemas de segurança.

O uso de procedimentos de monitoramento é necessário para assegurar que os usuários estão executando somente as atividades que foram explicitamente autorizadas. A análise crítica dos registros (*log*) envolve a compreensão das ameaças encontradas no sistema e a maneira pela qual isso pode acontecer.

4.6 SINCRONIZAÇÃO DOS RELÓGIOS

Os relógios de todos os sistemas de processamento da informação, dentro da organização ou do domínio de segurança, devem ser sincronizados de acordo com a hora oficial.

Onde um computador ou dispositivo de comunicação tiver a capacidade para operar um relógio (*clock*) de tempo real, convém que o relógio seja ajustado conforme o padrão acordado, por exemplo o tempo coordenado universal (*Coordinated Universal Time* – UTC) ou um padrão de tempo local. Como alguns relógios são conhecidos pela sua variação durante o tempo, convém que exista um procedimento que verifique esses tipos de inconsistências e corrija qualquer variação significativa.

A interpretação correta do formato data/hora é importante para assegurar que o *timestamp* reflete a data/hora real. Deve-se levar em conta especificações locais (por exemplo, horário de verão).

O estabelecimento correto dos relógios dos computadores é importante para assegurar a exatidão dos registros (*log*) de auditoria, que podem ser requeridos por investigações ou como evidências em casos legais ou disciplinares. Registros (*log*) de auditoria incorretos podem impedir tais investigações e causar danos à credibilidade das evidências. Um relógio interno ligado ao relógio atômico nacional via transmissão de rádio pode ser utilizado como relógio principal para os sistemas de registros (*logging*). O protocolo de hora da rede pode ser utilizado para sincronizar todos os relógios dos servidores com o relógio principal.