Política de Controle de Acesso Lógico

Histórico de Revisões		
Data	**Revisão**	**O que foi revisado**
08/07/2022	00	Elaboração da nova versão de procedimento com base nos requisitos das normasISO9001:2015 e ISO14001:2015

ÍNDICE

1. Fontes de Referência

- ABNT ISO / IECGuia73:2005 – Gestão de Riscos – Vocabulário / Recomendações para uso em normas;
- ISO / IEC 13335-1:2004 – Information tech no logy – Security techniques – Management of information and communications technology security – Part1: Concepts and models for information and communictions technology security management;
- ISO / IEC27001:2005 - Information technology – Security techniques – Information security manage-ments systems – Requirements;
- Código de Prática para a Gestão da Segurança da Informação (NBR ISO/IEC27002:2007);

2 Conteúdo

2.1 Em casos de inviabilidade técnica de implementação dos critérios abaixo, os motivos devem ser registrados e aprovados pela Área Tecnologia da Informação, assim como novos critérios específicos por sistema, equipamento ou serviço devem ser criado se documentados.

2.2 Acesso Lógico

2.2.1 O acesso a quais quer ativos ou informações deve ser controlado,ao menos, por mecanismos de identificação, autenticação individual (ex.: usuário e senha) e monitoração, devendo o acesso ser negado por padrão.

2.2.2 A concessão de acesso a quais quer sistemas ou equipamentos do Estaleiro Mauá deve acontecer apenas mediante autorização formal do gestor funcional do profissional requisitante.

2.2.3 A concessão de acesso aos sistemas do Estaleiro Mauá deve ser feita através de conta de usuário a cada um profissional a serviço do Estaleiro Mauá, devendo ser usada somente por esta.

2.2.4 A concessão ou mudança de privilégios de acesso deve ser concedida somente para os recursos estritamente necessários às atividades a serem exercidas, dentro dos privilégios mínimos cabíveis.

Privilégios de acesso aos ativos tecnológicos do Estaleiro Mauá devem ser reavaliados, periodicamente, pelo gestor dos ativos junto ao gestor funcional do profissional relacionado, verificando-se a necessidade da manutenção das concessões, sob o suporte da Área Tecnologia da Informação.

2.2.6 É vetado o acesso, sem a devida autorização, a informações e equipamentos de outros profissionais.

2.2.7 Contas de usuário e perfis de acesso, conforme periódica autorização tanto dos gestores funcionais quanto dos gestores dos ativos relacionados, devem ser devidamente documentados.

2.2.8 Gestores funcionais, em conjunto com a Área de Gestão de Recursos Humanos do Estaleiro Mauá, devem informar aos responsáveis por prover acesso lógico, as mudanças de privilégios de acesso dos usuários aos recursos tecnológicos, de acordo com admissões, promoções, remanejamentos ou demissões.

2.2.9 Contas de usuário com responsabilidade de comunicação entre sistemas ou de iniciação de

serviços tecnológicos não devem poder fazer logon interativo, sobre tudo estiver em perfil privilegiado.

2.2.10 Contas de usuário que permitam a execução de programas com privilégios de segurança de outro usuário, através de participação em grupos privilegiados ou aplicativos específicos (ex.: *Unix Sudo*), devem ter uma senha diferente de todas as outras pertencentes ao mesmo usuário.

2.2.11 Somente profissionais devidamente capacitados e autorizados devem ter acesso privilegiado, total e irrestrito aos ativos tecnológicos do Estaleiro Mauá.

2.2.12 O acesso a equipamentos e sistemas, sobretudo através de contas de usuário de perfil privilegiado (ex.: administrador), deve ser restrito a um número reduzido de usuários, devidamente treinados e formalmente autorizados pelos gestores destes ativos.

2.2.13 O processo de acesso e autenticação a equipamentos críticos, sobretudo dispositivos de segurança (ex.: *firewalls*), deve ser através de tráfego criptografado (ex.: *kerberos, ssh*), para evitar, pela varredura da rede, a identificação da conta de usuário e senha relacionada em texto claro.

2.2.14 Usuários padrão (*default*), pré-definidos pelo fabricante, com perfil privilegiado (ex.: *administrator, guest*) devem ser renomeados ou desabilitados e, a princípio, não utilizados. Novos usuários com perfil semelhante, nome distinto e não relacionado com as funções pretendidas devem ser criados e usados.

2.2.15 Não deve ser permitido o acesso, através da rede, a equipamentos críticos, sobretudo dispositivos de segurança, através de contas de usuário de perfil privilegiado único (ex.: root), já que estas impedem saber, com exatidão, a identidade do usuário conectado. A conexão remota deve acontecer por usuários básicos, e o acesso comutado para os privilégios requeridos após a conexão estabelecida.

2.2.16 Deve haver um segmento de rede específico e contas de usuário específicas definidos para a administração remota de equipamentos críticos, sobretudo dispositivos de segurança, para que o acesso possa ser facilmente identificado e credenciado, conforme cadastro de usuários e redes permitidas nos equipamentos destino.

2.2.17 Contas de usuário de equipamentos ou sistemas, sobretudo as de perfil privilegiado, não devem ser compartilhadas. No caso de extrema e comprovada necessidade de compartilhamento (ex.: root), os profissionais e os motivos técnicos relacionados devem ser minuciosamente detalhados, devendo, sempre que houver mudanças na equipe, as senhas serão alteradas.

2.2.18 Contas de usuário de perfil privilegiado (ex.: root) devem ser usadas apenas para tarefas que exijam este poder, devendo, para tarefas específicas e rotineiras, ser criados ou utilizados usuários com acesso o mais simples e restrito possível.

2.2.19 O assesso remoto originado de redes externas para quaisquer equipamentos ou sistemas do Estaleiro Mauá deve ser disponibilizado, somente, através de:

- Conexões seguras (ex.: uso de VPN);
- Soluções homologadas autorizadas;
- Autenticação e validação de equipamentos conforme padrões de segurança pré-definidos pelo Estaleiro Mauá.

2.3 Senhas

Aplicações, desenvolvidas ou adquiridas, devem seguir padrões de segurança, como:

- Suporte a autenticação individual de usuários;
- Armazenamento e transmissão criptografada desenhas;
- Armazenamento das senhas em arquivos separados dos dados da aplicação;
- Armazenamento de senhas em pastas restritas com acesso direto apenas pelo sistema;
- A digitação desenhas não deve exibir o conteúdo do que está sendo escrito, devendo os caracteres originais serem trocados por símbolos;
- Exercício de funções de um funcionário por outros em conhecimento das senhas do primeiro;
- Suporte a protocolos de autenticação e requisitos de segurança–certificação digital, autenticação centralizada (ex.: radius, tacacs, kerberos, ldap, x509).

2.3.2 Todos os profissionais a serviço do Estaleiro Mauá com acesso aos sistemas internos, incluindo-se empregados, terceirizados, são responsáveis pelas suas senhas, devendo zelar pela sua criação e guarda adequada;

2.3.3 Se necessário, requerimentos fortes de autenticação e segurança, o acesso deve ser feito através de uma combinação de autenticação por conta de usuário e autenticação por mídia (ex.: *token*ou*smartcard*);

2.3.4 Contas de usuário ou mídias de autenticação x.: *token*ou*smartcard* devem ser concedidas e usadas apenas por um único profissional correlacionado a elas.

2.3.5 PINs elacionados às mídias de autenticação, como senhas, não devem ser revelados ou compartilhados.

2.3.6 Senhas de contas de usuários de perfil privilegiado (ex.: administrador) ou com responsabilidade de comunicação entre sistemas não devem ter prazo de expiração.

2.3.7 Todas as senhas, sejam estas para acesso privilegiado a sistemas (ex.: administrador windows, cisco enable, root, etc) ou para uso de serviços básicos (ex.: rede, internet, e-mail, etc), devem ser alteradas periodicamente.

2.3.8 Senhas de acesso privilegiado (ex.: administrador windows, cisco enable, root, etc), sobretudo de ativos críticos, devem ser trocadas, ao menos, bimestramente, quando da mudança de equipe ou da ocorrência de incidentes de segurança relacionados.

2.3.9 Senhas de acesso para uso de serviços básicos (ex.: rede, internet, e-mail, etc) devem ser trocadas, ao menos, a cada 90 dias, com avisos de expiração e requisição automática de troca ao usuário feita pelo sistema.

2.3.10 Senhas de acesso, quando armazenadas, devem sê-lo, apenas na forma criptografada e com acessores trito (ex.: unixshadow), de forma não comprometer sua confidencialidade e integridade.

2.3.11 Senhas iniciais devem ser temporárias, para serem trocadas no próximo processo de logon, devendo o envio ser feito através de mecanismo seguro (ex.: e-mailcriptografado) e, apenas, ao usuário

relacionado.

2.3.12 Serviços, sistemas e equipamentos diferentes devem ter uma senha específica para cada um, sobretudos e relacionadas a perfis privilegiados.

2.3.13 Senhas originais de equipamentos e sistemas, disponibilizadas pelo fabricante do hardware ou software, devem ser modificadas antes da instalação definitiva.

2.3.14 Senhas não devem ser recicladas, escritas, preenchidas em formulários externos ou reveladas a quem quer que seja, mesmo gerentes, administradores, parceiros de trabalho, assistentes.

2.3.15 Senhas usadas no EISA não devem ser reutilizadas em serviços pessoais externos (ex.: senhas bancárias).

2.3.16 Mais de 3 (três) tentativas de autenticação sem sucesso deve implicar no bloqueio da conta de usuário correspondente, a liberação sendo efetuada, apenas, por solicitação formal do gestor funcional ou superior hierárquico responsável.

2.3.17 Senhas devem ser de fácil lembranças da digitação pelo dono, mas de difícil dedução por outros. Senhas devem ser elaboradas, conforme os seguintes critérios de segurança:

- Tamanho mínimo de 8 (oito) caracteres para serviços básicos seu usuário (ex.: acesso a e-mail, rede, internet, sistemas de informações);
- Tamanho mínimo de 14 (catorze) caracteres para perfis privilegiados e/ou administrativos, sobre tudo de sistemas críticos (ex.: dispositivos de segurança);
- Uso de:

- Letras Maiúsculas (ex.: A, B, C, etc);
- Letras Mínúsculas (ex.: a, b, c, etc);
- Caracteres Especiais (ex.: #, &, ?, etc);
- Números (ex.: 1, 2, 3, etc).

- Uso de caracteres especiais, sobre tudo no início e fim;
- Uso de boas práticas para formação desenhas, como:

Método1:

- Crie uma frase longa que só você saiba (o número de palavras deve ser igual ao tamanho da senha – 8 ou 14 caracteres);
- Retire uma letra de cada palavra (ex.: a primeira letra) e
- Forme então uma palavra incompreensível

que será sua senha.

Método2:

Crie sua senha baseado na escolha de uma frase ou palavra e defina seu código, baseado em erros de ortografia, sons outro casos caracteres originais por outros (ex.: letras por números e vice-versa), como:

- Ç□SS;
- B□&;

➢ Z□2.

2.3.19. A elaboração de senhas devem seguir boas práticas, como as seguintes:

- Não derivar de dados, preferências ou documentos pessoais suas ou de pessoas próximas, como:

- Nomes próprios ou familiares (ou partedeles);

- Datas (ex.: aniversários);

- Endereços e telefones;

- Números de identidade, CPF e placas de carro;

- Livros, filmes, músicas, slogans, etc;

- Não derivar de termos ou situações que lembrem o EISA ou suas atividades profissionais.

- Não constar em dicionários (de quais quer idiomas, inclusive português, alemão e inglês);

- Não compor-se de muitos caracteres repetidos ou de sucessão lógica e previsível (ex.: 123456);

Não se basear na transformação ou inversão de palavras (ex.: Ktgoria, suineserf, etc).