1. Propósito

Determinar as práticas para uso de credenciais de acesso aos recursos de TI da ALCE, assim como as questões de segurança referente às senhas de acesso à rede e sistemas.

2. Escopo

Esta norma cobre os aspectos referentes às credenciais de acesso à rede, sistemas corporativos e demais recursos de TI, disponibilizados ou utilizados pela instituição.

3. Política

3.1. Identificação Pessoal

- Toda credencial concedida para acesso à rede, sistemas e demais recursos de TI da ALCE é pessoal e intransferível, sendo o seu proprietário responsável pelas ações executadas.
- É expressamente vedado e sujeito a sanções o fornecimento de credenciais pessoais a outros colaboradores, funcionários ou terceiros.
- É expressamente vedado e sujeito a sanções a utilização de credenciais de acesso de terceiros, mesmo que com a autorização do dono das credenciais utilizadas.

3.2. Responsabilidade

- A cada portador de credenciais de acesso à rede e/ou sistemas, cabe:
  - Alteração da senha fornecida ao realizar o primeiro acesso após a criação de sua conta pela equipe de TI;
  - Criação e trocas periódicas de senha de acordo com esta política;
  - Não compartilhar em hipótese nenhuma sua credencial de uso pessoal;
  - A senha deve ser memorizada, não devendo ser anotada ou armazenada no computador de forma desprotegida (que possa ser facilmente identificada como senha e utilizada para acesso indevido);
  - Notificar imediatamente a equipe de TI caso suspeite de uso indevido de suas credenciais de acesso, respeitando os procedimentos de notificação de incidentes de segurança.

3.3. Usuários Críticos

- Para credenciais de rede consideradas críticas, cuja violação possa impactar em sanções legais à ALCE deverão obrigatoriamente adotar autenticação forte (multi-fator).

3.4. Senha de Acesso

- A senha de acesso aos recursos de TI da ALCE segue os seguintes critérios de formação:
  - Possuir no mínimo 08 caracteres incluindo letras, números e símbolos;
  - Deve ser alterada regularmente a cada 90 dias, não devendo reutilizar a última senha;
  - Não ser baseada em nada que alguém facilmente possa adivinhar, ou obter, usando informações pessoais como nomes, números de telefone e datas de aniversário;
  - Não deve ser igual ao login de acesso.
- A conta do usuário será bloqueada após 5 tentativas inválidas de acesso, sendo sua posterior liberação executada apenas mediante apresentação pessoal à área de TI e/ou solicitação formal gestor imediato ao gestor de TI.

3.5. Processo de Contratação

- A criação de novos usuários na rede deverá ser solicitada formalmente pelo gestor responsável pelo novo colaborador à área de Tecnologia, de acordo com procedimento estabelecido para este fim;
- O Gestor deverá solicitar à área de Tecnologia a criação de novos usuários em sistemas, recursos de TI, bem como, os tipos de permissões de acesso aos mesmos, sendo responsável pela adequação entre as permissões concedidas ao perfil do cargo desempenhado.

3.6. Verificação de Direitos de Acesso

- Caberá à Auditoria Interna realizar revisões semestrais nas credenciais de acesso existentes de forma a verificar o cumprimento desta política.
- Violações desta política deverão ser registradas como não conformidades, devidamente reportadas, registradas e corrigidas pelas áreas responsáveis.

3.7. Processo de Encerramento

- Cabe ao departamento de RH comunicar periodicamente ao gestor de cada área e ao departamento de TI o desligamento de funcionários e estagiários, bem como cabe à Gerência Administrativa informar o encerramento da prestação de serviços dos demais colaboradores terceirizados;
- É responsabilidade do gestor de cada área da ALCE solicitar à área de Tecnologia o encerramento das credenciais e privilégios de acesso imediatamente após o desligamento de um funcionário, estagiário ou terceirizado;
- A área de TI deverá suspender imediatamente os direitos de acesso à rede e sistemas através das credenciais do colaborador desligado, mantendo sua conta desabilitada por pelo menos 06 meses. Findo o prazo mencionado, as contas de acesso poderão ser apagadas.
- Devem ser removidos os privilégios de acesso a todos os sistemas e recursos dos colaboradores que foram desligados da organização.

3.8. Ausência Temporária

- Todas as credenciais de acesso que não sejam utilizadas por mais de 60 dias devem ser desabilitadas;
- Em caso de ausências temporárias, o Gestor responsável deve comunicar à área de Tecnologia a ausência, a fim de que suas credenciais de acesso à rede sejam desabilitadas. A área de Tecnologia deve ser comunicada na ocasião do retorno do colaborador, a fim de que seu acesso seja habilitado novamente.

3.9. Usuários Corporativos

- Na eventualidade da existência de usuários de acesso que identifiquem a ALCE como instituição, sem a possibilidade de criar contas individuais para colaboradores que representem a ALCE perante o emissor da credencial, o compartilhamento destas credenciais será permitido deste que:
    - O Comitê Gestor de Segurança seja previamente comunicado e aprove o compartilhamento das credenciais de acesso;
    - Sempre que um colaborador que possuía acesso à credencial for desligado, as senhas de acesso deverão ser imediatamente trocadas.

3.10. Monitoramento e Registro

A ALCE pode monitorar e registrar a utilização das credenciais de acesso à rede e sistemas, visando identificar possíveis abusos e melhorar continuamente sua política de concessão de acesso.

4. Sanções

Qualquer colaborador que violar esta norma estará sujeito a ações disciplinares conforme previsto no NC-013 - Manual de Sanções Administrativas.

5. Aprovação

Este documento foi aprovado em 16/08/2013 pela Presidência e é válido a partir da data de sua publicação para todos os colaboradores que utilizam recursos computacionais.

6. Definições

7. Histórico de Revisão

01/06/2012 – Criação da Norma