	GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO	Data: 20/10/2022 Revisão: 23/03/2023
NSI-003		Uso Interno
Aprovador: Jose Ribamar Gabriel de Morais Junior		Elaborador: Marcos Johnny Rodrigues Rocha

1. Introdução

1.1. A Norma de segurança da informação complementa Política Geral de Segurança da Informação, definindo as diretrizes para garantir que o acesso aos ativos de informação ou sistemas de informação garanta níveis adequados de proteção.

2. Propósito

2.1. Estabelecer diretrizes para gestão de identidade e acesso aos ativos e sistemas de informação da AJCRED.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.

4. Diretrizes

4.1. Acesso a ativos e sistemas de informação

4.1.1. A AJCRED fornece a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa;

4.1.2. As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais;

4.1.3. Toda conta de acesso é de uso do usuário a qual foi delegada e intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso.

4.1.4. Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:

4.1.4.1. Não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pela AJCRED;

4.1.4.2. Não utilizar sua conta, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pela AJCRED;

4.1.4.3. Não compartilhar a conta de acesso e senha com outro usuário, colaborador e/ou terceiro;

4.1.4.4. Informar imediatamente a equipe de segurança caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, sistemas e/ou recursos computacionais da AJCRED;

4.1.5. Usuários que tem acesso autorizado a privilégios administrativas em sistemas de informação devem possuir uma credencial específica para este propósito. A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia;

4.1.6. Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração pelo CGSI e aplicação das sanções e punições previstas na Política Geral de Segurança da Informação, conforme a gravidade da violação.

4.2. Senha de acesso

4.2.1. As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais da AJCRED são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo;

4.2.2. A AJCRED adota os seguintes padrões para geração de senhas de acesso a seus ativos/serviços de informação ou recursos computacionais:

4.2.2.1. A equipe de tecnologia da informação será responsável por fornecer senhas de acesso inicial ao usuário, que deverá proceder com a troca imediata da mesma;

4.2.2.2. As senhas possuem validade, passado o prazo, os sistemas poderão solicitar automaticamente a troca da senha no período de 30 a 90 dias para renovação da senha.

4.2.2.3. As senhas associadas a contas com privilégio não-administrativo serão compostas usando uma quantidade mínima de 08 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;

4.2.2.4. As senhas associadas a contas que possuem privilégio administrativo serão compostas usando uma quantidade mínima de 15 (quinze) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;

4.2.2.5. Após 05 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário poderá ser bloqueada, assim permanecendo assim por, no mínimo, 30 (trinta) minutos;

4.2.2.6. Os sistemas de informação podem manter um histórico das últimas 03 (três) senhas utilizadas, não permitindo sua reutilização;

4.2.3. Quando criada uma senha, usuários devem estar atentos as seguintes recomendações:

4.2.3.1. Não utilizar nenhuma parte de sua credencial na composição da senha;

4.2.3.2. Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;

4.2.3.3. Não utilizar repetição ou sequência de caracteres, números ou letras;

4.2.3.4. Qualquer parte ou variação do nome da AJCRED;

4.2.3.5. Qualquer variação dos itens descritos acima como duplicação ou escrita invertida e não poderá usar as últimas senha já cadastradas, o usuário terá que efetuar um cadastro de uma nova senha diferencia das 3 última já utilizadas.

4.3. Autorização de acesso (privilégios de acesso)

4.3.1. A autorização e o nível permitido de acesso ativos/serviços de informação da AJCRED é feita com base em perfis que definem o nível de privilégio dos usuários.

4.3.2. O acesso à ativos/serviços de informação é fornecido a critério da AJCRED, que define permissões baseadas nas necessidades laborais dos usuários;

4.3.3. Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada colaborador. Solicitações deverão ser encaminhadas a equipe de tecnologia da informação.

4.3.4. Os usuários devem ainda observar as seguintes diretrizes:

4.3.4.1. A seu critério exclusivo, a AJCRED poderá ativar uma cota para armazenamento de arquivos em sua infraestrutura computacional local ou serviços de armazenamento remoto (nuvem). Caso o usuário necessite de mais espaço, deverá realizar uma solicitação ao departamento de tecnologia da informação;

4.3.4.2. É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais ou que não sejam de interesse da AJCRED tanto na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem);

4.3.4.3. Usuários não devem ter expectativa de privacidade quanto aos arquivos armazenados na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) da AJCRED.

4.4. Autorização de acesso à rede corporativa.

4.4.1. Cada colaborador terá um único usuário para acesso a rede corporativa.

4.4.2. A identificação dos usuários serão conforme nomenclatura definida pelo setor Segurança da Informação, contendo nome e sobrenome.

4.4.3. O acesso do usuário será limitado a informação e recursos necessários para cumprir suas funções de trabalho.

4.4.4. A concessão de acesso será revisada regularmente para garantir que seja necessária e adequada para as necessidades do trabalho.

4.4.5. A empresa realizará auditorias regulares de acesso à rede para garantir que o acesso seja restrito aos funcionários autorizados e que as credenciais de usuário sejam mantidas seguras. Qualquer atividade suspeita será investigada e relatada às autoridades apropriadas.

4.4.6. O acesso à rede corporativa deve estar em conformidade com todas as leis e regulamentos aplicáveis, incluindo as leis de privacidade de dados. A empresa se reserva o direito de revogar o acesso de qualquer funcionário que viole esta política ou as leis aplicáveis.

4.4.7. Os funcionários terão acesso a treinamento de segurança em rede, que inclui orientações sobre o uso adequado da rede corporativa e a importância da segurança da informação.

5. Papéis e Responsabilidades

5.1. GESTOR DA INFORMAÇÃO

5.1.1. É responsabilidade dos colaboradores apontados como Gestor da Informação:

5.1.1.1. Autorizar a concessão e revogação de acesso a ativos/sistemas de informação sob sua responsabilidade;

5.1.1.2. Autorizar a concessão e o controle de acesso administrativo a ativos/sistemas de informação sob sua responsabilidade;

5.1.1.3. Realizar a revisão periódica de autorizações de acesso e credenciais de acesso a ativos/sistemas de informação sob sua responsabilidade.

5.2. DEPARTAMENTO PESSOAL

5.2.1. É responsabilidade do departamento pessoal (Recursos Humanos):

5.2.1.1. Reportar em tempo hábil o desligamento de empregados da AJCRED a equipe de tecnologia da informação para que contas de acesso possam ser revogadas;

5.2.1.2. Apoiar a gestão de identidades enviando relatórios periódicos sobre colaboradores desligados ou que mudaram de posição na AJCRED;

5.2.1.3. Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação fornecendo informações sobre os empregados.

5.3. GESTORES E COORDENADORES

5.3.1. É responsabilidade dos gestores e coordenadores:

5.3.1.1. Solicitar a equipe de tecnologia da informação a concessão de acesso novos empregados ou empregados que necessitem de novos acessos conforme mudanças em suas atividades laborais;

5.3.1.2. Solicitar a equipe de tecnologia da informação concessão de acesso a terceiros/prestadores de serviços contratados justificando a necessidade de acesso a ativos/sistemas de informação;

5.3.1.3. Informar a equipe de tecnologia da informação quando ao encerramento do contrato com parceiros/substabelecidos contratados que tenham a ativos/sistemas de informação.

5.4. GERENCIA DE TECNOLOGIA DA INFORMAÇÃO

5.4.1. É responsabilidade da gerência de tecnologia da informação:

5.4.1.1. Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários de empregados, parceiros/substabelecidos;

5.4.1.2. Conceder, quando autorizado, o acesso aos usuários de empregados, parceiros/substabelecidos, conforme indicado pelos gestores da informação;

5.4.1.3. Revogar, quando solicitado, o acesso dos usuários de empregados, parceiros/substabelecidos, conforme indicado pelos gestores da informação;

5.4.1.4. Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação dos usuários de empregados, parceiros/substabelecidos fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.

6. Sanções e Punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do comitê Gestor de Segurança da Informação.

8. Gestão da Política

8.1. A presente política foi aprovada no dia 20 de outubro de 2022.

Jose Ribamar Gabriel de Morais Junior

Socio Diretor

Marcos Johnny Rodrigues Rocha

Analista de Sistema