Política Corporativa de Gestão de Acesso

Unidades Gestoras: Diretor Superintendente – **DISUP**
Diretor Administrativo e Financeiro – **DIAFI**
Gerência de Tecnologia da Informação – **GETIN**
Assessoria de Controladoria e Gestão Riscos - **ASCOR**

Aprovado pelo Conselho Deliberativo do SERGUS em 16/01/2019

Índice

1. Definições 2
2. Introdução 2
3. Objetivo 3
4. Acesso Físico 3
5. Acesso Lógico 3
6. Acesso à Internet 4
7. Correio Eletrônico (E-MAIL) 5
8. Sanções 6
9. Documentos anexos 6
10. Gestão da Política 6
11. Disposições Finais 7

1.Definições

Na aplicação e interpretação dos conteúdos e condições contidos nesta Política, os termos abaixo relacionados terão os seguintes significados:

a) **Área Sensível**: Dependências do SERGUS onde há armazenamento e/ou processamento de informações confidenciais (sala dos servidores, ativos de rede e nobreak entre outros equipamentos de telecomunicação), devendo seu acesso ser controlado.

b) **Conexão (Login)**: Ato de registra-se em um sistema computacional restrito como, por exemplo, computadores, sistemas de informação, redes similares. É efetuado através do uso de credencial individual de acesso composta da combinação do código de usuário e senha de acesso. Após efetuar uma conexão bem-sucedida, o usuário é identificado pelo sistema e recebe permissões de acesso de acordo com o seu perfil de acesso.

c) **Desconexão (Logoff)**: Ação de encerrar a sessão de um computador, rede ou aplicativo por meio do comando apropriado.

d) **TIC:** Tecnologias de Informação e Comunicação;

e) **Informação**: Patrimônio do SERGUS, consiste nas suas informações de caráter comercial, administrativa, estratégico, técnico, financeiro, mercadológico, legal e recursos humanos ou de qualquer outra natureza, bem como todas as informações adquiridas por prestadores e ou empregados, aquisição, licença confiada ao SERGUS, não importa se protegidas ou não de confidencialidade, em sua forma verbal ou escrita, em suporte físico ou digital, armazenada, trafegada ou em transito na infraestrutura tecnológica de SERGUS.

f) **Informação Confidencial**: Informação que possui caráter sigiloso, podendo ser comunicada apenas a usuários especialmente autorizados que necessitem conhece-la para o desempenho de suas atividades profissionais, e que se divulgadas independente pode causar danos financeiros e morais ao SERGUS, bem como penalidade cíveis e criminais e trabalhistas aos responsáveis pela divulgação.

g) **Perfil de Acesso**: Conjunto de permissões que definem o acesso às informações e aos recursos do SERGUS, associado a um código de usuário (Login).

h) **Usuários**: Que tem apenas o direito de uso, são todos os acessos cedidos independentemente de pessoa, empregado, aprendiz estagiário, prestadores de serviço que, de qualquer forma, estejam alocados na prestação de Serviço ao SERGUS, não importando o regime jurídico a que estejam submetidos e colaboradores em geral que, direto ou indiretamente, utilizem de qualquer acesso as informações do SERGUS.

2.Introdução

Os acessos aos recursos de TIC somente serão permitidos mediante identificação e autenticação dos usuários, através de uma única conta de acesso e senha.
A senha vinculada a conta de acesso é pessoal e intransferível, sendo de responsabilidade do usuário manter a confidencialidade.
O usuário é responsável por todos os acessos realizados através da sua conta de acesso aos sistemas e a Rede Coorporativa, devendo zelar pelo sigilo da sua conta de acesso e senha, podendo ser responsabilizado pelos possíveis danos que o seu mau uso ocasione aos recursos de TIC da Instituição.

O usuário deve evitar a utilização da conta de acesso em mais de uma estação de trabalho ou computador portátil simultaneamente, ficando o Usuário titular da conta, responsável pelos riscos da utilização indevida de sua conta de acesso.

3.Objetivo

Esta política tem por objetivo estabelecer diretrizes para os acessos físicos e aos recursos de Tecnologia da Informação e Comunicações do SERGUS.

4.Acesso Físico

A instalação de processamento das informações críticas ou sensíveis do SERGUS, está devidamente identificada e restrita a acessos.
Caso sejam identificados outros riscos de acesso físico, o SERGUS poderá a seu critério incluir outros perímetros de segurança que se fizerem necessários.
Para o acesso à área sensível, empregados e demais pessoas autorizadas devem observar as seguintes disposições:

a) Enquanto em área sensível, as pessoas autorizadas devem portar identificação que exibam claramente seus dados e fotografia;

b) É resguardado o direito de inspeção de malas, maletas, mochilas e similares ou itens como computadores portáteis e dispositivos de vídeo/imagem antes de permitir a entrada ou saída do usuário ou terceiros da área sensível;

c) Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos na área sensível;

d) É vedado tentar obter ou permitir o acesso não autorizado a área sensível da Instituição. Caso usuário identifique ou suspeite de tentativas de acesso não autorizado deve reportar imediatamente para a Área de Segurança Responsável;

e) É proibido comer, beber ou fumar em qualquer área sensível ou nas proximidades dos equipamentos de tecnologias da informação da Instituição;

f) É vedada a retirada de qualquer equipamento de TI ou informação em suporte físico ou digital de áreas sensíveis a menos que formalmente autorizado.

5.Acesso Lógico

O acesso lógico aos recursos tecnológicos do SERGUS é concedido mediante o uso de credenciais de acesso (código do usuário e senha de acesso), fornecido no ato de seu cadastramento. Ressaltamos que cada usuário possui o perfil com sua permissão especifica para cada tipo de Acesso.
O usuário deve observar as seguintes disposições quanto à utilização de credenciais de acesso, sistemas de informação e recursos tecnológicos do SERGUS:

a) É proibido acesso simultâneo com a mesma credencial de acesso;

b) É proibido compartilhar credenciais de acesso;

c) É proibido o acesso com credenciais de outro usuário ou terceiros;

d) É proibido inserir ou facilitar a inserção de dados falsos, bem como excluir ou alterar indevidamente dados da base de dados do SERGUS;

e) Na hipótese de transmissão de dados confidenciais que necessitem de fornecimento de senha para que o destinatário possa abrir o arquivo, está deverá ser transmitida separadamente à transmissão dos dados confidenciais;

f) É proibido o acesso de dispositivos moveis nos equipamentos tecnológicos do SERGUS, salva-se os casos autorizados formalmente.

6.Acesso à Internet

6.1.Rede Corporativa

A navegação na Internet deve ser feita exclusivamente para fins profissionais, visando assegurar o bom uso dos recursos do SERGUS, evitando o desperdício causado pelo fluxo de informações não pertinentes às tarefas laborais.
O usuário deve observar as seguintes disposições quanto ao acesso à Internet:
É proibida a navegação para fins pessoais ou que não guarde relação com a atividade profissional do usuário;

a) O usuário somente poderá iniciar a navegação na internet após a validação das credenciais de acesso (usuário e senha);

b) É proibida a navegação aos sites de caráter pornográfico, compartilhamento de arquivos, transferência de dados, terrorismo, drogas, crackers, propaganda política partidária, relacionamentos e rede sociais, esportes, webmail particular, serviços públicos de mensagens instantâneas como MSN, Yahoo! Messenger, ICQ, WhatsApp ou similares, jogos, gincanas, concursos on-line, violência, violação de direito autoral, áudio e vídeo, hobbies, religião, comércio eletrônico e qualquer outro que possa ferir a legislação. Salva-se os casos autorizados formalmente;

c) É proibida a navegação aos sites que possam comprometer, de alguma forma, a segurança jurídica e a integridade da infraestrutura tecnológica do SERGUS, conforme procedimento adotado pela Instituição;

d) Não serão franqueados acessos à Internet às funções meramente operacionais, tais como vigilantes, serviços gerais de limpeza e afins;

e) Somente poderá ser solicitada a liberação de site bloqueado quando existir comprovada necessidade de o usuário acessá-lo para o desenvolvimento de suas atividades profissionais;

f) A rede do BANESE é monitorada e verificada sempre que necessário, para atender a política de segurança do SERGUS e do BANESE.

6.2.Rede de Convidados

A navegação nesta rede será monitorada através de software de segurança, visando assegurar o bom uso dos recursos do SERGUS, evitando o desperdício causado pelo fluxo de informações não pertinentes às tarefas laborais.
O usuário deve observar as seguintes disposições quanto ao acesso à Internet via rede de convidados:

a) É proibida a navegação aos sites de caráter pornográfico, pornográfico infantil, terrorismo, drogas, crackers, violência, violação de direito autoral, áudio e vídeo, hobbies, religião, comércio eletrônico e qualquer outro que possa ferir a legislação;

b) É proibida a navegação aos sites que possam comprometer, de alguma forma, a segurança jurídica e a integridade da infraestrutura tecnológica do SERGUS, conforme procedimento adotado pela Instituição;

c) Caso seja comprovado mal-uso do serviço o mesmo poderá ser bloqueado e sujeito a processos administrativo ou judicial;

d) O uso dessas credencias devem ser guardadas em sigilo e seu uso pessoal e intransferível.

7.Correio Eletrônico (E-MAIL)

O e-mail é uma ferramenta institucional que deve ser utilizada apenas para comunicações eletrônicas relacionadas às atividades laborais, não sendo permitido seu uso para fins pessoais ou que não sejam de interesse do SERGUS.

O usuário deve observar ainda as seguintes disposições quanto ao uso do e-mail:

a) A conta de e-mail corporativa será monitorada pelo BANESE;

b) A conta de e-mail corporativa deverá ser utilizada, exclusivamente, para o envio e recebimento de mensagens relacionadas à atividade profissional do usuário;

c) A troca de e-mail deve ser restrita às unidades/usuários que justifiquem a necessidade;

d) É proibido o acesso ao e-mail particular (webmail) através da infraestrutura tecnológica do BANESE;

e) É proibida a inscrição do e-mail corporativo em listas de tráfego não relacionadas ao uso profissional, bem como o envio de todo e qualquer tipo de corrente, circulares, propaganda, boatos, política, conteúdo impróprio ou pornográfico e afins, ou, ainda, qualquer tipo de mensagem que possa prejudicar o SERGUS, BANESE e ou terceiros;

f) É proibido causar excessivo tráfego na rede ou sobrecarregar a infraestrutura tecnológica, incluindo a prática de spam;

g) É proibido o envio de mensagens que contenham assuntos sobre violência, terrorismo, vídeo, áudio, ameaça, difamação, calúnia, injúria, racismo, pornografia infantil, além de qualquer outro conteúdo ilegal, ofensivo ou imoral;

h) É proibido forjar qualquer mensagem eletrônica ou se fazer passar por outrem, que não o próprio usuário, titular do e-mail corporativo;

i) É proibido enviar mensagens contendo informação do SERGUS ou BANESE, independentemente da classificação, para conta de e-mail particular (webmail) do próprio usuário, salva-se os casos expressamente autorizados;

j) É proibida a interceptação ou alteração do conteúdo da mensagem de terceiros;

k) O envio de mensagens para listas de grande abrangência é restrito à Presidência, Diretoria Executiva, secretárias da Diretoria Executiva e aos Gestores da Informação. Entende-se como lista de grande abrangência, grupos de e-mail corporativos que contenham qualquer conjunto de endereços eletrônicos extensos, salva-se os casos expressamente autorizados;

l) É proibido o download de qualquer arquivo executável, com extensões .exe, .com, .scr ou outras que possam conter vírus;

m) É proibido o envio de informações do SERGUS e ou BANESE classificadas como interna ou confidencial a fornecedores e/ou terceiros;

n) É proibido o envio de arquivos com conteúdo que violem direitos de terceiros, ou que possam causar prejuízos, ao SERGUS, BANESE e ou terceiros, salva-se os casos expressamente autorizados;

o) É proibido o envio de arquivos com conteúdo de caráter ilegal, ofensivo ou imoral;

p) É proibida a inserção ou disseminação de arquivos que contenham vírus;

q) Serão bloqueadas automaticamente as extensões e e-mails contendo linguagem dinâmica que podem gerar risco à segurança das informações do SERGUS ou BANESE, conforme procedimento adotado pela Instituição.

Ressaltamos que o correio eletrônico do BANESE é monitorado e verificado sempre que necessário, para atender a política de segurança do SERGUS e do BANESE.

8.Sanções

As penalidades referentes a esta política estão descritas no Código de Ética do SERGUS e nas normas de segurança do Banco BANESE.

9. Documentos anexos

a) FACER – Formulário de Inclusão, Alteração, Bloqueio e Exclusão de Usuário na Rede;

b) FACES – Formulário de Inclusão, Alteração, Bloqueio e Exclusão de Usuário no Sistema;

c) FACEC – Formulário de Inclusão, Alteração, Bloqueio e Exclusão de Usuário no Correio Eletrônico;

d) TECEQ – Termo de Custódia de Equipamento de TI;

e) TECPO – Termo de Cumprimento das Políticas de TI;

f) REPAT – Relação de Pessoas com Acessos Autorizados.

10. Gestão da Política

A atualização desta Política e seus documentos anexos compete a área de Tecnologia da Informação propor a revisão ou alteração do texto desta Política juntamente com seus documentos e a realização de testes de auditoria dos acessos dos usuários, no mínimo anualmente, podendo ser revisado em período inferior caso seja pertinente, devendo submetê-lo à aprovação da Diretoria Executiva, a quem caberá a análise dos casos omissos.

Esta política como os documentos que nelas são citados estão disponíveis no GSERGUS, Sistema de Gerenciamento SERGUS, como também na área de Compliance da Instituição. A gestão desta Política ficará a cargo da Diretoria Administrativa e Financeiras - DIAFI junto com a área de Tecnologia da Informação.

11. Disposições Finais

Em caso de incidentes que afetam a segurança dos ativos ou o descumprimento das Normas e Políticas do SERGUS e BANESE ou em casos de quebra de segurança da informação por meio de recursos de TI, o usuário deverá imediatamente informar a área de TI formalmente através do formulário, para tomar as providências necessárias a sanar a causa do problema, podendo, inclusive, executar as sanções prevista nesta política.

O conteúdo desta Política é exclusivamente de uso interno, ficando proibida a reprodução e o fornecimento de seu todo, parte ou anexos a terceiros, à exceção dos legalmente habilitados, ou em caso de expressa autorização superior.

As Políticas de Acesso, Segurança da Informação e o Código de Ética do SERGUS, deverão ser apresentadas ao usuário pela área de Gestão de Pessoa, assim que solicitar o cadastro do novo usuário e de imediato preencher o Termo de Responsabilidade, pelo qual o usuário deve assinar o documento demonstrando sua ciência.