Política Corporativa de Segurança da Informação

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

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

Índice

1. Definições 2
2. Introdução 3
3. Objetivos 4
4. Responsabilidade 4
5. Recursos Computacionais 7
6. E-mail Corporativo 9
7. Internet 9
8. Backup 10
9. Sanções 10
10. Gestão da Política 10
11. Disposições Finais 10

1.Definições

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

a) **Áreas Sensíveis:** Dependências onde do SERGUS há armazenamento e/ou processamento de informações confidenciais devendo seu acesso ser controlado. Tais áreas incluem, mas não se limitam a Datacenters, Arquivo Morto, Sala Cofre, Armários de Telecomunicações (Rack);

b) **Ativo de Informação**: Tudo aquilo que tem valor para a organização que contenha ou não informações do SERGUS, incluindo, mas não se limitando a, documentos impressos ou em formato eletrônico, processos, programas de computador, certificados digitais, recursos computacionais, computadores, notebooks, telefones celulares, pendrives, modens, modens 3G ou 4G, câmeras, smartfones e outros equipamentos portáteis;

c) **Ativos de Rede:** São equipamentos responsáveis pela comunicação de dados existente entre os computadores dos usuários e servidores;

d) **Backup:** Backup é um termo inglês que tem o significado de cópia de segurança;

e) **Classificação da Informação**: Atividade consiste na atribuição de grau de sigilo as informações em suporte físico ou digital e em sua forma verbal ou escrita;

f) **Copias de Segurança**: Reprodução de dados armazenados em arquivos, usualmente realizada em mídia removível para garantir a continuidade dos sistemas em caso de falhas;

g) **Gestor da Informação**: Usuário que exerce a função gerencial na estrutura organizacional do SERGUS que tenha criado, adquirido ou recebido em confiança determinada informação;

h) **Informação**: Patrimônio do SERGUS consiste nas suas informações ou informações sob a guarda, comercial, administrativa, estratégico, técnico, financeiro, mercadológico, legal de recursos humanos ou de qualquer outra natureza, bem como todas as informações adquiridas por associação, aquisição, licença, compra ou confiadas ao SERGUS por clientes e terceiros, 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 do SERGUS;

i) **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;

j) **Informação Interna**: Informação que somente poderá ser divulgada aos usuários, no ambiente interno do SERGUS, e consequentemente, não poderá ser divulgada ao público em geral;

k) **Informação pública**: Informação que não necessita de sigilo algum, podendo ser divulgada e publicada oficialmente para os usuários e público em geral;

l) **Linear Tape-Open (LTO):** é uma tecnologia de armazenamento de dados em fita magnética desenvolvida originalmente na década de 1990 como uma alternativa de

padrões abertos a formatos proprietários de fita magnética que estavam disponíveis na época (DLT);

m) **Perímetro de Segurança**: Barreiras de Segurança múltiplas e controles de acesso físico e logico implantados para proteger áreas sensíveis contra acesso não autorizado, danos e interferências, incluindo, mas não se limitando a, paredes, portas externas, fechaduras, controle de entrada por cartões, biometria, alarmes e firewalls;

n) **PSI:** Política de Segurança da Informação;

o) **Rotulagem da informação:** A Atividade consiste na colocação de rotulo em suporte físico ou digital para identificar a classificação da informação;

p) **Segurança da Informação:** Conjunto de medidas adotadas visando à proteção das informações de posse ou confiadas ao SERGUS resguardando sua confidencialidade (que sejam conhecidas somente por aqueles que estão autorizados a conhece-las), integridade (que seja correta e precisa) e disponibilidade (que seja acessível e utilizável por aqueles que estão autorizados), evitando seu uso indevido, inadequado, ilegal ou em desconformidade com a política. Desta forma, minimizando os riscos ao negócio, maximizando o retorno sobre os investimentos e as oportunidades de negócio;

q) **Servidor:** é um sistema de computação que fornece serviços a uma rede de computadores;

r) **Servidor de Produção:** Servidor que fornece serviços aos usuários finais (funcionários do Banco e clientes);

s) **Servidor de Desenvolvimento:** Servidor que fornece serviços aos analistas da Área de T.I. que estão desenvolvendo sistemas;

t) **Servidor de Homologação:** Servidor que fornece serviços aos analistas da Área de T.I. e Gestores ou Usuários que estão homologando sistemas;

u) **Servidor de Infraestrutura:** Servidor que fornece serviços aos analistas da Área de T.I. para monitorar e administrar os demais servidores;

v) **TI:** Tecnologia da Informação;

w) **Usuário:** Empregados com vínculo empregatício, aprendizes, estagiários, prestadores de serviços que, de qualquer forma, estejam alocados na prestação de serviços ao SERGUS, não importando o regime jurídico a que estejam submetidos e colaboradores em geral que, direta ou indiretamente, utilizem os sistemas ou tenham acesso às informações do SERGUS para o desenvolvimento de suas atividades profissionais.

2.Introdução

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do SERGUS para proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

3.Objetivos

Estabelecer diretrizes que permitam a todos os colaboradores/funcionários, representantes do SERGUS ou qualquer outra empresa que esteja alocada no prédio do Instituto que se utilize da estrutura tecnológica, seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações do SERGUS quanto à:

a) Regulamentar e disciplinar as regras para o bom uso dos recursos computacionais, a fim de manter a disponibilidade, a integridade e a confidencialidade das informações do SERGUS e sua segurança;

b) Atribuir responsabilidade, definir direitos, deveres, expectativas de acesso e uso das informações e da infraestrutura tecnológica do SERGUS;

c) Criar uma cultura educativa empresarial de proteção as informações do SERGUS;

d) Estabelecer as recomendações para o uso racional de recursos computacional possibilitando a otimização do fluxo de informações pertinentes as tarefas executadas cotidianamente no SERGUS;

e) Definir mecanismo de controle e monitoramento para a utilização de recursos computacionais da rede corporativa do SERGUS;

f) Estabelecer as regras para a manipulação de informações do SERGUS, de seus fornecedores, relacionadas e clientes.

4.Responsabilidade

As responsabilidades relacionadas à Segurança da Informação são assim definidas:

4.1. Do SERGUS

a) Adotar medidas cabíveis para garantir a confidencialidade, integridade e disponibilidade das informações do Instituto;

b) Nomear membro para comissão que venha ser instalada em função de acordos de cooperação técnica, parcerias, e demais ações de interesse do Instituto;

c) Disponibilizar através de sua infraestrutura tecnológica os recursos computacionais necessários à realização das atividades laborais aos seus usuários;

d) Disponibilizar a todos os usuários suporte técnico permanente para auxiliá-los no uso da infraestrutura tecnológica do Instituto.

4.2. Dos Usuários

a) Cumprir as regras definidas na presente Política e quaisquer normas ou procedimentos adotados pelo SERGUS;

b) Responder pelos prejuízos advindos da inobservância das medidas relatadas nesta Política;

c) Adotar medidas cabíveis de segurança que estejam ao seu alcance, visando sempre proteger as informações do SERGUS;

d) Utilizar as informações do SERGUS exclusivamente para os objetivos do negócio e jamais para fins pessoais;

e) Manter informações e documentos confidenciais, em papel ou em mídias eletrônicas, protegidos e armazenados em gavetas, armários ou cofre, especialmente quando se ausentar de sua mesa de trabalho;

f) Ao usar computadores, ativar proteção de tela com bloqueio de senha, quando se ausentar de sua mesa de trabalho;

g) Durante o processo de afastamento ou desligamento, devolver quaisquer ativos de informação ao SERGUS que estejam em sua posse;

h) Encaminhar dúvidas e solicitar orientações, sempre que necessário, a área de TI do SERGUS;

i) Manter sigilo sobre todas as informações que venha a tomar conhecimento em virtude das suas atividades profissionais junto ao SERGUS, o que permanecerá em vigor e vinculará legalmente o usuário enquanto vigorar o regime jurídico a que estiver submetido, vigorando, ainda, após a eventual rescisão, a qualquer título, por qualquer das partes, de maneira permanente, sob pena do direito do SERGUS pleitear o ressarcimento das perdas e danos decorrentes da violação do sigilo pelo usuário, sem prejuízo das sanções legais;

j) Zelar e manter em segurança suas senhas de acesso aos sistemas de informação, incluindo a sua conta de rede, e à infraestrutura tecnológica do SERGUS, com os respectivos recursos autorizados que necessite para o desenvolvimento de suas atividades profissionais;

k) Informar imediatamente à área de TI qualquer suspeita de uso indevido de suas credenciais;

l) Comunicar de imediato à área de TI qualquer evento que coloque em risco a segurança das informações do SERGUS ou que viole esta Política.

4.3. Da Gestão de Pessoal

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI do SERGUS.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do SERGUS.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não

estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como aos termos da Norma Educacional.

4.4. Da Tecnologia da Informação

a) Atualizar a Política de Segurança da Informação, de acordo com a legislação vigente, os avanços da tecnologia e as melhores práticas em segurança da informação, para posterior aprovação da Diretoria Executiva - DIREX;
b) Fazer cumprir esta Política;
c) Conduzir a gestão da Segurança da Informação;
d) Criar e revisar os procedimentos de segurança da informação;
e) Definir, selecionar, garantir a implementação e revisar os controles e/ou soluções técnicas aderentes aos requisitos de segurança da informação do SERGUS;
f) Registro, controle e acompanhamento das não-conformidades com a Política de Segurança da Informação;
g) Desenvolver, acompanhar a implantação e manter planos de continuidade da informação;
h) Identificar os riscos inerentes e residuais relacionados à segurança da informação;
i) Providenciar meios eletronicamente seguros para a transmissão e arquivamento das informações classificadas como confidenciais;
j) Analisar as solicitações de desbloqueio de sites, aprovadas anteriormente pelo gestor do setor requerente;
k) Coordenar a gestão de identidades, incluindo os processos de concessão, manutenção, revisão e suspensão de acesso dos usuários aos sistemas de informação e recursos computacionais do SERGUS;
l) Preservar a Segurança da Informação em ambientes compartilhados com outras instituições, através de acordos, cooperações técnicas, parcerias, e demais situações de interesse do SERGUS;
m) Manter todos os sistemas de informação em níveis aceitáveis de segurança da informação;
n) Monitorar a infraestrutura tecnológica para garantir o cumprimento desta Política;
o) Homologar e especificar os programas de computador autorizados a serem utilizados pelos usuários do SERGUS;
p) Configurar e garantir que o aviso legal seja exibido corretamente conforme procedimento adotado pelo SERGUS;
q) Guardar os manuais e mídias da infraestrutura tecnológica do SERGUS;
r) Realizar a manutenção dos programas de computador (softwares) do SERGUS;
s) Guardar as licenças de uso de programa de computador e de outros recursos computacionais do Banese.

4.5. Da Controladoria

a) Auditar o cumprimento da presente Política e quaisquer normas e procedimentos de Segurança da Informação adotados pela Instituição;

b) Apurar os incidentes de segurança da informação do SERGUS;

c) Promover ampla divulgação, orientação e treinamento da Política de Segurança da Informação para todos os usuários;

d) Emitir parecer com recomendações das ações disciplinares cabíveis no caso de descumprimento da Política de Segurança da Informação.

5.Recursos Computacionais

5.1. Equipamentos Físicos

O SERGUS disponibiliza para seus usuários equipamentos (computadores, notebooks, impressoras, dentre outros, também conhecidos como “hardwares”) exclusivamente para o desempenho de suas atividades profissionais.

O usuário deve observar as seguintes disposições quanto ao uso de hardwares do SERGUS:

a) É proibida a utilização para fins pessoais;

b) É proibida a utilização de hardware particular para desempenho de atividades profissionais, tais como, mas não se limitando a notebook, pen drive, smartphone, modem, modem 3G e câmera fotográfica/filmadora;

c) É proibida a conexão de hardware particular na rede do Banese;

d) É proibida a conexão de hardware pertencente aos fornecedores ou terceiros na rede local corporativa do Banese, exceto conexão à rede sem-fio de visitantes ou quando formalmente autorizado;

e) É proibida a alteração de qualquer hardware e/ou periférico de propriedade do SERGUS;

f) Os equipamentos devem ser utilizados com cuidado para garantir seu correto funcionamento;

g) O equipamento deve ser desligado no final do expediente ou em ausências prolongadas;

h) O usuário deve efetuar a desconexão (log off) da rede toda vez que não for mais utilizar o hardware ou for se ausentar por um período prolongado da estação de trabalho;

i) No caso de dúvidas, alteração ou manutenção contatar a área de TI.

5.2. Programas de Computador

Todos os programas de computador (também conhecidos como “softwares”) instalados na infraestrutura tecnológica do SERGUS são devidamente licenciados e homologados. Portanto, a violação desta Política acarretará responsabilidade exclusiva ao usuário.

O usuário fica ciente da obrigação de indenizar o SERGUS, caso a Instituição venha a suportar qualquer prejuízo em demandas judiciais ou administrativas movidas pelos titulares dos direitos autorais de softwares, incluindo as despesas com custos processuais e honorários advocatícios.

O usuário deve observar as seguintes disposições quanto ao uso de programas de computador no Banese:

a) É proibida a instalação de qualquer software na infraestrutura tecnológica do SERGUS, excetuando-se aquele usuário que tenha permissão expressa em razão de seu cargo;

b) É proibida a utilização, modificação, cópia ou transferência de software que viole quaisquer direitos do autor do programa de computador através da infraestrutura tecnológica do SERGUS;

c) É proibida a utilização de software na infraestrutura tecnológica do SERGUS que não seja expressamente autorizado pela Instituição ou que viole os direitos do autor do programa de computador;

d) É proibida a utilização de software que comprometa a segurança dos sistemas do SERGUS, tais como, mas não se limitando a, recuperador de senhas, descobridor de senhas, vasculhador de rede, mensagens instantâneas, http-proxy, socks2http, http-tunnels, clientes de áudio e vídeo MPEG Layer 3 e 4 (MP3 e MP4), clientes FTP;

e) Utilizar o papel de parede padronizado pelo SERGUS.

5.3. Equipamentos Portáteis

Os equipamentos portáteis, tais como, mas não se limitando a notebook, smartphone, pen drive, câmera fotográfica/filmadora, modem 3G e quaisquer outros que permitam armazenamento ou transmissão de dados somente poderão ser utilizados pelos usuários se disponibilizados pelo SERGUS, a seu exclusivo critério, mediante autorização formal, para execução das atividades profissionais.

A entrada e a saída de informações do SERGUS através do uso destes equipamentos serão controladas e autorizadas formalmente conforme procedimento adotado pela Instituição.

O usuário deve observar as seguintes disposições quanto ao uso de dispositivos portáteis:

a) É proibida a utilização para fins pessoais;

b) É proibida a utilização de equipamentos portáteis particulares para o desenvolvimento das atividades profissionais;

c) É proibida a cópia ou transferência de informações ou dados de propriedade do SERGUS para equipamentos portáteis;

d) O usuário não deve deixar equipamentos móveis fora do alcance em locais públicos onde haja acesso de múltiplas pessoas;

e) O usuário não deve permitir que terceiros não autorizados utilizem ou tenham acesso às informações ou dados transportados nos equipamentos portáteis;

f) O usuário deve empregar todos os cuidados necessários para que não haja utilização indevida ou vazamento de informações através dos equipamentos portáteis.

g) É obrigatória a utilização de travas de proteção, de forma a manter o mesmo sempre travado, em suas mesas de trabalho ou salas de reunião, principalmente quando o mesmo estiver sem uso;

h) Caso o equipamento portátil, em especial Notebooks, necessite ser transportado através de automóvel, o mesmo deverá ser transportado e armazenado no porta-malas do veículo. Não é permitido o transporte e armazenamento em banco dianteiro, traseiro ou debaixo dos mesmos. Também não é permitido manter este tipo de equipamento armazenado em porta-malas por longos períodos.

5.4. Impressoras Multifuncionais e Equipamentos de Reprografia

O uso das impressoras multifuncionais e de equipamentos de reprografia (fotocopiadoras) deve ser feito exclusivamente para impressão de documentos ou outras informações que sejam de interesse do SERGUS ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

O usuário deve observar as seguintes disposições quanto ao uso de impressoras multifuncionais e equipamentos de reprografia:

a) O usuário deve retirar imediatamente da impressora multifuncional ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações do SERGUS, classificadas como interna ou confidencial;

b) A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada.

6.E-mail Corporativo

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 Instituto ou seus Patrocinadores.

Todas as contas de e-mail disponibilizadas pelo Banese aos usuários deverão obedecer ao formato padrão adotado pela Instituição, incluindo, mas não se limitando a, assinatura padrão e aviso legal conforme descrito na Política Corporativa de Gestão de Acesso.

7.Internet

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. Conforme descrito na Política Corporativa de Gestão de Acesso.

8.Backup

8.1. O SERGUS dispõe de ferramenta de backup automático, realizando periodicamente a cópia dos seus discos objetivando constituir cópia de segurança dos dados, conforme descrito em procedimento adotado pela Instituto.

8.2. Os usuários poderão solicitar a restauração de informações, dados e arquivos através de cópias de segurança seguindo as recomendações descritas no Manual de Procedimento.

8.3. É responsabilidade exclusiva dos usuários armazenar arquivos nas unidades de armazenamento recomendadas pelo SERGUS. Arquivos armazenados fora dessas unidades não serão incluídos no processo de cópias de segurança e não poderão ser recuperados.

9.Sanções

As penalidades referentes a esta política estão no Código de Ética do SERGUS e as normas de segurança da nossa rede corporativa do Banco Banese.
A violação das regras definidas nesta política acarretara a penalidade disciplinar de acordo com a gravidade da falta cometida onde os responsáveis pela área de TI juntamente com a diretoria deveram analisar o tipo de penalidade.
As penalidades referentes a segurança da informação foram revisadas seguindo o Código de Ética do SERGUS e as normas de segurança da nossa rede corporativa do Banco do Estado de Sergipe S.A. - Banese. Assim sendo, cabe a Diretoria Executiva do SERGUS com base na denúncia apresentada pela Gerência de Tecnologia da Informação - GETIN, após ouvidas as partes envolvidas, a análise e a aplicação da Penalidade, conforme abaixo especificado.

10.Gestão da Política

A gestão desta Política ficará a cargo da Diretoria Administrativa e Financeiras - DIAFI através da Área de Tecnologia da Informação.

11.Disposições Finais

11.1. Atualizações desta Politica

Compete a Área de Tecnologia Informação, propor a revisão ou alteração do texto desta Política, no mínimo anualmente, podendo ser revisado em período inferior caso seja pertinente, devendo submetê-lo à aprovação da Diretoria Executiva – DIREX, a quem caberá a análise dos casos omissos;

11.2. Uso Interno

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.