Banese

Política de Segurança da Informação e Cibernética

UNIDADE GESTORA: SUGER - Superintendência de Gestão de Riscos
ARSEC - Área de Segurança da Informação e Continuidade de Negócios

Aprovada pela Resolução da Diretoria nº 1278, de 06/02/2025 e Conselho de Administração em 31/01/2025.

SUMÁRIO

CAPÍTULO I – INTRODUÇÃO

A Política de Segurança da Informação e Cibernética é integrante do Sistema de Gestão de Segurança da Informação do Banco do Estado do Sergipe e define as regras de segurança da informação adotadas pelo Banese relacionadas à manipulação de suas informações e à utilização de sua infraestrutura tecnológica como também estabelece diretrizes que contemplam o programa de segurança da informação e riscos cibernéticos.

CAPÍTULO II – DEFINIÇÕES

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

ÁREAS SENSÍVEIS	Dependências do Banese onde 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 telecomunicação (*racks*).
ATIVO DE INFORMAÇÃO	Tudo aquilo que tem valor para a organização que contenha ou não informações do Banese, 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*, *modes*, *modens* 3G, câmeras, *smartphones* e outros equipamentos portáteis.
CLASSIFICAÇÃO DA INFORMAÇÃO	Atividade consistente na atribuição de grau de sigilo às informações em suporte físico ou digital e em sua forma verbal ou escrita, a qual podemos classificá-las como: confidencial, uso interno e pública.
COMITÊ DE CONFORMIDADE E ÉTICA - COMEC	Grupo de trabalho multidisciplinar permanente que tem por finalidade tratar questões ligadas à segurança da informação do Banese.

CONEXÃO (*LOGON*/*LOGIN*)	Ato de registrar-se em um sistema computacional restrito como, por exemplo, computadores, sistemas de informação, redes e 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.
DESCONEXÃO (*LOGOFF*/*LOGOUT)*	Ação de encerrar a sessão de um computador, rede ou aplicativo por meio de um comando apropriado.
GESTOR DA INFORMAÇÃO	Usuário que exerça função gerencial na estrutura organizacional do Banese que tenha criado, adquirido ou recebido em confiança determinada informação.
INFORMAÇÃO	Patrimônio do Banese consistente nas suas informações ou informações sob sua guarda, que podem ser de caráter bancário, comercial, administrativo, 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 Banese por clientes e terceiros, não importando se protegidas ou não de confidencialidade, em sua forma verbal ou escrita, em suporte físico ou digital, armazenada, trafegada ou em trânsito na infraestrutura tecnológica do Banese.
INFORMAÇÃO CONFIDENCIAL	Informação que possui caráter sigiloso, podendo ser comunicada apenas a usuários especialmente autorizados que necessitem conhecê-la para o desempenho de suas atividades profissionais, e que se divulgada indevidamente pode causar danos financeiros e morais ao Banese, bem como penalidades cíveis, criminais e trabalhistas aos responsáveis pela divulgação.
INFORMAÇÃO INTERNA	Informação que somente poderá ser divulgada aos usuários, no ambiente interno do Banese, e consequentemente, não poderá ser divulgada ao público em geral.
INFORMAÇÃO PÚBLICA	Informação que não necessita de sigilo algum, podendo ser divulgada e publicada oficialmente para os usuários e público em geral.

PERFIL DE ACESSO	Conjunto das permissões que definem o acesso à informação e aos recursos computacionais do Banese, associado a um código do usuário (*login)*.
PERÍMETROS DE SEGURANÇA	Barreiras de segurança múltiplas e controles de acesso físico e lógico implantados para proteger áreas sensíveis contra acesso não autorizado, danos e interferências, incluindo, mas não se limitando a, paredes, portas externas, fechaduras, controles de entrada por cartões, biometria, alarmes e *firewalls.*
REGISTRO (LOG)	Registro eletrônico de um evento ou ação. Todo registro é gravado em um arquivo, onde são armazenados registros de atividades envolvendo ações ou eventos originados em dispositivos equipados com sistemas operacionais de uso genérico ou especializado, aplicativos, sistemas de aplicativos ou serviços.
ROTULAGEM DA INFORMAÇÃO	Atividade consistente da colocação de rótulo em suporte físico ou digital para identificar a classificação da informação.
SEGURANÇA DA INFORMAÇÃO	Conjunto de medidas adotadas visando à proteção das informações de posse ou confiadas ao Banese resguardando sua confidencialidade (que sejam conhecidas somente por aqueles que estão autorizados a conhecê-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, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos. Desta forma, minimizando os riscos ao negócio, maximizando o retorno sobre os investimentos e as oportunidades de negócio.
SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)	Parte do sistema de gestão global, baseada em uma aproximação de risco empresarial, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação.
USUÁRIOS	Empregados com vínculo empregatício, aprendizes, estagiários, prestadores de serviços que, de qualquer forma, estejam alocados na prestação de serviços ao Banese, 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 Banese para o desenvolvimento de suas atividades profissionais.
ATAQUES *DDOS* E *BOTNETS*	Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição que vêm de muitos computadores infectados, *Botnets*, utilizados para criar e enviar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
ENGENHARIA SOCIAL	Termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.
FRAUDES EXTERNAS E INVASÕES	Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias ou sistemas, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.
MALWARE	Um código malicioso, programa malicioso, *software* nocivo, *software* malintencionado ou *software* malicioso (em inglês: *malware*, abreviação de "*malicious software*"), é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não). Ele pode aparecer na forma de código executável, scripts de conteúdo ativo, e outros *softwares*.
RISCOS CIBERNÉTICOS	Riscos de ataques cibernéticos, oriundos de *malwares*, técnicas de engenharia social, invasões fraudes externas desprotegendo dados, redes e sistemas da empresa que podem causar danos financeiros e/ou de reputação, ataques de rede (*DDoS* e *Botnets*).

CAPÍTULO III – PÚBLICO ALVO

Art. 1º A presente política aplica-se a todos os que têm ou tiveram algum tipo de vínculo com o Banese, incluindo acesso às informações e/ou à sua infraestrutura tecnológica, mesmo após o término do regime jurídico a que estavam submetidos, assim compreendidos: empregados, aprendizes, estagiários, prestadores de serviços, colaboradores.

CAPÍTULO IV – REGULAMENTAÇÃO ASSOCIADA

Art. 2º São documentos que fundamentam a presente política:

I- Código Civil, Código Penal, Consolidação das Leis do Trabalho;
II- Lei Federal nº 9.279/1996 (propriedade industrial);
III- Lei Federal nº 9.610/1998 (direitos autorais);
IV- Lei Federal nº 9.609/1998 (*software*);
V- Lei Federal nº 12.965/2014 (marco civil da Internet);
VI- Lei Complementar nº 105/2001 (sigilo bancário);
VII- Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados;
VIII- Resolução CMN nº 4.893/2021.

CAPÍTULO V – OBJETIVOS

Art. 3º A Política terá como principais objetivos:

I- Regulamentar e disciplinar as regras para o bom uso dos recursos computacionais, a fim de assegurar a confidencialidade, integridade e disponibilidade das informações do conglomerado prudencial Banese e de informações de terceiros por ele custodiadas contra acessos indevidos e transações não autorizadas assegurando ainda que as informações estarão disponíveis a todas as partes que possuem autorização, quando necessário;

II- Atribuir responsabilidades, definir direitos, deveres, expectativas de acesso e uso das informações e da infraestrutura tecnológica do Banese;

III- Estabelecer as recomendações para o uso racional de recursos computacionais possibilitando a otimização do fluxo de informações pertinentes às tarefas executadas cotidianamente no Banese;

IV- Definir mecanismos de controle e monitoramento para a utilização de recursos computacionais da rede corporativa Banese;

V- Estabelecer as regras para a manipulação de informações do Banese, de seus fornecedores, empresas relacionadas e de clientes;

VI- Mitigar riscos cibernéticos mediante ações de prevenção, detecção e tratamento de ameaças, incidentes e vulnerabilidades nos ambientes físicos e lógicos;

VII- Asseverar a gestão de continuidade de seus negócios ao proteger os serviços críticos de interrupções causadas por falhas ou desastres relevantes;

VIII- Estimular uma cultura de segurança da informação e cibernética através de programas de capacitação e conscientização dos colaboradores, inclusive com avaliações periódicas;

IX- Estabelecer e melhorar de forma contínua os procedimentos relacionados à segurança da informação e cibernética.

CAPÍTULO VI – ABRANGÊNCIA

Art. 4º A Política abrange os seguintes requisitos:

I- Requisitos de segurança da informação, que consideram controles de proteção às informações do Banese;

II- Requisitos de segurança lógica, que consideram controles de acesso às informações do Banese em ambiente eletrônico;

III- Requisitos de segurança física, que consideram controles de acesso às informações e infraestrutura tecnológica do Banese em ambiente físico.

CAPÍTULO VII – SANÇÕES

Art. 5º A violação das regras definidas nesta Política acarretará penalidade disciplinar de acordo com a gravidade da falta cometida nos termos do Código de Conduta Ética do Banese, sem prejuízo da possibilidade de responder em Juízo, no caso de infração à legislação.

CAPÍTULO VIII –DIREITOS DE ACESSO

Art. 6º Quaisquer tipos de acesso, seja ele físico ou lógico possuem o devido controle, monitoramento e restrição quanto a sua permissão e seu privilégio que são revistos periodicamente e aprovados pelo gestor responsável, sendo os acessos cancelados ao término de sua finalidade.

Seção I – Acesso Físico

Art. 7º As instalações de processamento das informações críticas ou sensíveis do Banese serão mantidas em áreas seguras, protegidas por perímetro de segurança, ficando fisicamente protegidas contra o acesso não autorizado, danos e interferências.

Parágrafo único. Caso sejam identificados outros riscos de acesso físico, o Banese poderá, a seu critério, incluir outros perímetros de segurança que se fizerem necessários.

Art. 8º Quaisquer tipos de acesso, seja ele físico ou lógico possuem o devido controle, monitoramento e restrição quanto a sua permissão e seu privilégio que são revistos periodicamente e aprovados pelo gestor responsável, sendo os acessos cancelados ao término de sua finalidade.

Art. 9º Para o acesso às áreas sensíveis, empregados e demais pessoas autorizadas devem observar as seguintes disposições:

I- Enquanto em áreas sensíveis, usuários devem portar crachás de identificação que exibam claramente o nome e fotografia. Terceiros autorizados devem portar crachás temporários identificando claramente que os mesmos não são colaboradores do Banese;

II- Crachás de identificação, inclusive temporários, são pessoais e intransferíveis. Sob nenhuma circunstância será permitido o seu compartilhamento;

III- 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 de áreas sensíveis;

IV- Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;

V- É vedado tentar obter ou permitir o acesso não autorizado às áreas sensíveis da Instituição. Caso usuários identifiquem ou suspeitem de tentativas de acesso não autorizado devem reportar imediatamente para a Área de Segurança Patrimonial – ARSEP;

VI- É proibido comer, beber ou fumar em qualquer área sensível;

VII- É vedada a retirada de qualquer equipamento ou informação em suporte físico ou digital de áreas sensíveis a menos que formalmente autorizado;

VIII- É vedado o acesso de empregados do Banese a instalações com equipamentos de outras instituições em ambiente de uso compartilhado, ainda que sob a responsabilidade do Banese, a menos que formalmente autorizado.

Seção II – Acesso Lógico

Art. 10. O acesso lógico aos recursos computacionais do Banese é concedido mediante o uso de credenciais de acesso (código do usuário e senha de acesso) que são pessoais e intransferíveis e de uso exclusivo do usuário, que assume integral responsabilidade pela sua guarda e sigilo, bem como pelo uso indevido por terceiros.

Art. 11. O usuário deve observar as seguintes disposições quanto à utilização de credenciais de acesso, sistemas de informação e recursos computacionais do Banese (acesso lógico):

I- É proibido acesso simultâneo com a mesma credencial de acesso;

II- É proibido compartilhar credenciais de acesso ou o acesso aos sistemas de informação e senhas com outro usuário ou terceiro;

III- A criação de senhas de acesso deve obedecer ao disposto no procedimento adotado pelo Banese;

IV- A solicitação de criação/alteração de conta de acesso deverá ser feita à Central de Serviços, pelo gestor da área e, no caso de solicitação do próprio gestor, pela Diretoria a qual o mesmo esteja vinculado, de acordo com o procedimento adotado pelo Banese;

V- É proibida a tentativa ou o acesso ao sistema de informação não autorizado ou a outra conta de usuário que não a do próprio usuário;

VI- Usuários em processo de desligamento devem devolver suas credenciais ao Banese, que será imediatamente bloqueada na data do desligamento;

VII- É proibido inserir ou facilitar a inserção de dados falsos, bem como excluir ou alterar indevidamente dados corretos da base de dados do Banese;

VIII- É proibido o armazenamento, nos servidores de rede do Banese, de arquivos pessoais ou que não são de interesse, uso ou propriedade do Banco;

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

X- O Banese poderá, a qualquer momento, e sem prévio aviso, suspender, pelo período que julgar necessário, a conta de rede do usuário no caso de mau uso, risco aos sistemas ou por haverem indícios de conduta ilícita e/ou em desacordo com a presente Política.

Seção III – Acesso à Internet

Art. 12. A navegação na Internet deve ser feita exclusivamente para fins profissionais, visando assegurar o bom uso dos recursos do Banese, evitando o desperdício causado pelo fluxo de informações não pertinentes às tarefas laborais.

Art. 13. O usuário deve observar as seguintes disposições quanto ao acesso à Internet:

I- É proibida a navegação para fins pessoais ou que não guarde relação com a atividade profissional do usuário;

II- O usuário somente poderá iniciar a navegação após a validação de suas credenciais de acesso (código do usuário e senha de acesso);

III- É proibida a navegação aos sites de caráter pornográfico, pornográfico infantil, 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 *Skype*, *WhatsApp*, Telegram 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;

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

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

VI- 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, seguindo o procedimento adotado pela Instituição.

Seção IV – Acesso Remoto à Rede Corporativa (*Extranet e Home Office*)

Art. 14. O acesso remoto à rede corporativa do Banese (conexão através de VPN - Rede Privada Virtual) poderá ser concedido ao usuário que necessite se conectar remotamente para execução das atividades profissionais, a exclusivo critério do Banese, mediante autorização formal.

Art. 15. O usuário deve observar as seguintes disposições quanto ao acesso remoto:

I- A concessão de acesso será condicionada à extrema necessidade de trabalho do usuário e deverá ser solicitada conforme procedimento adotado pelo Banese;

II- O usuário será o único responsável por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade irregular exercida por outra pessoa de posse de seu acesso remoto, sendo responsável por seguir todas as medidas que garantam que pessoas não autorizadas não obtenham acesso remoto;

III- É proibido o acesso completo à rede do Banese, sendo os acessos segmentados de acordo com a atividade profissional desenvolvida pelo usuário;

IV- Somente será permitido o uso de dispositivos particulares para acesso através da VPN denominada Home Office, devendo atender aos requisitos de segurança pra conexões remotas estabelecidas pelo Banese;

V- Em caso de extravio, furto ou roubo do equipamento portátil que tenha o acesso VPN configurado, o usuário deverá informar o ocorrido imediatamente à ARSEC.

CAPÍTULO IX – USO DE RECURSOS COMPUTACIONAIS (*)

Seção I - Equipamentos Físicos (*)

Art. 16. O Banese disponibiliza para seus usuários equipamentos (computadores, impressoras, dentre outros, também conhecidos como "hardwares") exclusivamente para o desempenho de suas atividades profissionais.

Art. 17. O usuário deve observar as seguintes disposições quanto ao uso de *hardwares* do Banese:

I- É proibida a utilização para fins pessoais;

II- O uso de *hardware* particular para desempenho de atividades profissionais deverá ser restrito e atender o estipulado em normativos específicos; (*)

III- É proibida a conexão de *hardware* particular na rede do Banese;

IV- 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;

V- É proibida a alteração de qualquer hardware e/ou periférico de propriedade do Banese;

VI- Os equipamentos devem ser utilizados com cuidado para garantir seu correto funcionamento;

VII- O equipamento deve ser desligado no final do expediente ou em ausências prolongadas;

VIII- 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;

IX- No caso de dúvidas, alteração ou manutenção contatar a Central de Serviços.

Seção II – Programas de Computador

Art. 18. Todos os programas de computador (também conhecidos como "*softwares*") instalados na infraestrutura tecnológica do Banese são devidamente licenciados e homologados. Portanto, a violação desta Política acarretará responsabilidade exclusiva ao usuário.

Art. 19. O usuário fica ciente da obrigação de indenizar o Banese, 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.

Art. 20. O usuário deve observar as seguintes disposições quanto ao uso de programas de computador no Banese:

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

II- 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 Banese;

III- É proibida a utilização de *software* na infraestrutura tecnológica do Banese que não seja expressamente autorizado pela Instituição ou que viole os direitos do autor do programa de computador;

IV- É proibida a utilização de software que comprometa a segurança dos sistemas do Banese, 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;

V- Utilizar o papel de parede padronizado pelo Banese.

Seção III – Equipamentos Portáteis (*)

Art. 21. Os equipamentos portáteis, tais como, mas não se limitando a *notebook*, *smartphone*, *pendrive*, câmera fotográfica/filmadora, modem 3G e quaisquer outros que permitam armazenamento ou transmissão de dados serão preferencialmente disponibilizados pelo Banese, a seu exclusivo critério, mediante autorização formal, para execução das atividades profissionais. A utilização de equipamentos portáteis particulares deverá atender o estipulado em normativos específicos. (*)

Art. 22. A entrada e a saída de informações do Banese através do uso destes equipamentos serão controladas e autorizadas formalmente conforme procedimento adotado pela Instituição.

Art. 23. O usuário deve observar as seguintes disposições quanto ao uso de dispositivos portáteis:

I- É proibida a utilização para fins pessoais;

II- É proibida a utilização de equipamentos portáteis particulares para o desenvolvimento das atividades profissionais;

III- É proibida a cópia ou transferência de informações ou dados de propriedade do Banese para equipamentos portáteis;

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

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

VI- O usuário deve empregar todos os cuidados necessários para que não haja utilização indevida ou vazamento de informações através dos equipamentos portáteis;

VII- 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;

VIII- 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.

Seção IV - Impressoras Multifuncionais e Equipamentos de Reprografia (*)

Art. 24. 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 Banese ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

Art. 25. O usuário deve observar as seguintes disposições quanto ao uso de impressoras multifuncionais e equipamentos de reprografia:

I- O usuário deverá utilizar a modalidade de impressão com senha de autorização imputada nos equipamentos disponibilizados pelo Banese; (*)

II- O usuário é responsável pela correta utilização dos equipamentos e deverá comunicar a ARINF caso seu acesso não atenda o procedimento adotado pelo Banese; (*)

III- O usuário deve retirar imediatamente da impressora multifuncional ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia; (*)

IV- A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada; (*)
V- Se houver necessidade de transmissão, de informação classificada como confidencial, o usuário deve seguir o procedimento adotado pelo Banese.

CAPÍTULO X – *E-MAIL*

Art. 26. 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 Banese.

Art. 27. 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.

Art. 28. O usuário deve observar ainda as seguintes disposições quanto ao uso de *e-mail*:

I- A conta de *e-mail* corporativa será monitorada pelo Banese;

II- A conta de *e-mail;*

III- Corporativa deverá ser utilizada, exclusivamente, para o envio e recebimento de mensagens relacionadas à atividade profissional do usuário;

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

V- É proibido o acesso *ao e-mail* particular (*webmail)* através da infraestrutura tecnológica do Banese; 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 terceiros ou o Banese, causar excessivo tráfego na rede ou sobrecarregar a infraestrutura tecnológica, incluindo a prática de *spam*;

VI- 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;

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

VIII- É proibido enviar mensagens contendo informação do Banese, independentemente da classificação, para conta de e-*mail* particular (*webmail*) do próprio usuário;

IX- É proibida a interceptação ou alteração do conteúdo da mensagem de terceiros;

X- 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;

XI- É proibido o envio de *e-mail*s aos clientes do Banese, exceto se expressamente autorizado pela Diretoria responsável;

XII- As contas de *e-mail* departamentais serão vinculadas a um grupo de usuários, sendo de exclusiva responsabilidade desta qualquer ocorrência relacionada à conta departamental.

CAPÍTULO XI – ENVIO E RECEBIMENTO DE ARQUIVOS

Art. 29. Cada usuário é responsável pelos arquivos que recebe e envia através da infraestrutura tecnológica do Banese e deve observar as seguintes disposições:

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

II- É proibido o envio de informações do Banese classificadas como interna ou confidencial a fornecedores e/ou terceiros;

III- É proibido o envio de arquivos com conteúdo que violem direitos de terceiros, ou que possam causar prejuízos, a terceiros ou ao Banese;

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

V- É proibida a inserção ou disseminação de arquivos que contenham vírus;

VI- Serão bloqueadas automaticamente as extensões e *e-mails* contendo linguagem dinâmica que podem gerar risco à segurança das informações do Banese, conforme procedimento adotado pela Instituição.

CAPÍTULO XII – MONITORAMENTO DE ATIVOS

Art. 30. Todos os equipamentos disponibilizados pelo Banese para os usuários desenvolverem suas atividades profissionais são de propriedade do Banco e têm caráter de ferramenta de trabalho, sendo expressamente proibida a utilização para fins particulares.

Art. 31. Assim, toda a infraestrutura tecnológica do Banese, bem como todos os dados trafegados ou armazenados nesta infraestrutura, incluindo conta de *e-mail* corporativa e navegação em sites da Internet estão sujeitos ao monitoramento, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada, visando resguardar a segurança das informações e atender a requisitos legais e normativos do Banese. Dessa forma:

I- O usuário fica ciente da inexistência de expectativa de privacidade na utilização da infraestrutura tecnológica do Banese e, para reforçar tal inexistência, será exibido um aviso legal antes de permitir o acesso do usuário aos recursos computacionais e sistemas de informação;

II- O Banese fará uso de câmeras de segurança instaladas em suas dependências, ficando resguardada a dignidade humana do usuário, sendo vedada a instalação de câmeras de filmagem nos banheiros e lavabos;

III- A filmagem descrita nesta Política tem por objetivo assegurar segurança física do usuário e a segurança patrimonial do Banese, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa filmada, o que o usuário tem ciência expressamente neste ato;

IV- As imagens captadas dentro das dependências do Banese serão arquivadas conforme procedimento adotado pela Instituição e mantidas em caráter estritamente confidencial, somente podendo ser divulgadas em caso de infração às regras constantes das Políticas do Banese e/ou infração de legislação vigente;

V- Guarda de Registro - Todas as atividades desenvolvidas com a utilização da infraestrutura tecnológica do Banese serão registradas para eventual fim judicial, além de análise ou auditoria, por um período de 03 (três) anos ou conforme requerido pela legislação vigente e aplicável. Essas atividades incluem, mas não se limitam a acesso à rede, armazenamento de arquivos, informações, registros de envio e de recebimento de mensagens eletrônicas, acesso e navegação à Internet e impressão.

CAPÍTULO XIII – CERTIFICAÇÃO DIGITAL

Art. 32. O Banese fornecerá, a seu exclusivo critério, certificado digital ao usuário de acordo com a necessidade da atividade profissional desenvolvida. O certificado digital é pessoal e intransferível.

Art. 33. O usuário deve observar as seguintes disposições quanto à utilização do certificado digital:

I- O usuário deverá zelar pela guarda e conservação sigilosa de seu certificado digital, bem como pela sua senha;

II- O uso indevido de certificado digital por terceiros não eximirá a responsabilidade do usuário, em virtude de sua culpa na guarda do mesmo e da sua respectiva senha.

CAPÍTULO XIV – CÓPIAS DE SEGURANÇA

Art. 34. O Banese 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 Instituição.

Art. 35. Os usuários poderão solicitar a restauração de informações, dados e arquivos através de cópias de segurança seguindo as recomendações descritas no procedimento utilizado pelo Banese.

Art. 36. É responsabilidade exclusiva dos usuários armazenar arquivos nas unidades de armazenamento recomendadas pelo Banese. Arquivos armazenados fora dessas unidades não serão incluídos no processo de cópias de segurança e não poderão ser recuperados.

CAPÍTULO XV – PROCEDIMENTOS E CONTROLES

Seção I – Proteção do Ambiente

Art. 37. De forma a proteger o ambiente do Banese, são estabelecidos padrões regulamentares internos conforme relacionados abaixo:

I- São atribuídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações como forma de assegurar que a infraestrutura tecnológica de redes locais e internet estejam seguras;

II- São constituídos planos de ações e respostas a incidentes para o efetivo gerenciamento no monitoramento, detecção, tratamento e repostas a incidentes para minimizar o risco a falhas e a administração segura de redes de comunicações e plataformas sistêmicas;

III- São gerenciados os serviços contratados de processamento e armazenamento de dados e informações em nuvem conforme estabelecido em circular normativa interna para dispor sobre a Contratação de Serviços de Processamento e Armazenamentos de Dados e de Computação em Nuvem no País ou exterior.

Seção II – Gestão de Riscos de Segurança da Informação

Art. 38. O Banese periodicamente avalia e trata riscos de segurança da informação e cibernética, para assegurar o envolvimento dos gestores da informação, apoio na tomada de decisão e escolha da opção de tratamento ao risco identificado.

Art. 39. O modelo de gestão de riscos de Segurança da Informação do Banese, está suportado pelo seguinte modelo de governança:

I- Gestão de Vulnerabilidades;
II- Gestão de Incidentes de Segurança da Informação;
III- Gestão de Controle de Identidade e Acessos;
IV- Gestão de Continuidade do Negócios;
V- Governança de Riscos.

Seção III – Gestão de Vulnerabilidades

Art. 40. O Banese realiza através de procedimentos específicos e ferramentas, a varredura, monitoramento e correção de vulnerabilidades relacionadas à Segurança da Informação em seu ecossistema empresarial e tecnológico, o qual, fazem parte, pessoas, ativos de infraestrutura, sistemas operacionais e aplicações.

Art. 41. Tais ações visam assegurar o tratamento efetivo de vulnerabilidades, através da tomada de ações tempestivas e coordenadas, a fim de minimizar os efeitos de sua ocorrência e prevenir incidentes que utilizam as vulnerabilidades como vetor de ataque.

Seção IV – Gestão de Incidentes de Segurança da Informação

Art. 42. O Banese alinhado ao seu plano de resposta a incidentes, realiza o tratamento de incidentes de Segurança da Informação que venha afetar a confidencialidade, integridade e disponibilidade das informações, sistemas e serviços relevantes da instituição.

Art. 43. O modelo de gestão de incidentes utilizado pelo Banese inclui também ações de testes de cenários de incidentes, em conjunto com o Plano de Continuidade de Negócios, testes de intrusão que buscam especificamente a prevenção e o tratamento de incidentes a serem adotados pela instituição.

Seção V – Gestão de Controle de Identidade e Acessos

Art. 44. O Banese dispõe de procedimentos específicos para Gestão de Identidade e Acessos, integrado com os principais sistemas da instituição, para automatização da criação, concessão e revogação de direitos de acesso, controlando quem é autenticado (fez *login*) e autorizado (tem permissões) para usar os sistemas da instituição.

Seção VI – Gestão de Continuidade do Negócios

Art. 45. O Banese dispõe de procedimentos específicos, conforme estabelecido na política de Gestão de Continuidade de Negócios (GCN) e, periodicamente, realiza simulações de cenários relacionados a indisponibilidade operacional e incidentes de ataques cibernéticos, com o objetivo de minimizar impactos e recuperar perdas de ativos da informação, após possíveis incidentes considerados críticos, utilizando-se de uma gama de fatores como: ambiente externo, operações, colaboradores chave, mapeamento de processos críticos, análise de impacto aos negócios e testes recorrentes de recuperação de desastres.

Seção VII – Governança de Riscos

Art. 46. O Banese dispõe de uma estrutura de Riscos Corporativos, composto por executivos responsáveis pelas áreas de controle, mantendo uma agenda de reuniões mensais do Comitê de Ética e Conformidade – COMEC, o qual delibera, dentre outros, assuntos relacionados à Segurança Informação que incluem Riscos Tecnológicos e Cibernéticos.

Seção VIII– Disseminação da Cultura de Segurança da Informação

Art. 47. O Banese realiza treinamentos e ações de conscientização periódicos para todos colaboradores, prestadores de serviços e clientes.

Seção IX – Processamento e Armazenamento de Dados e de Computação em Nuvem

Art. 48. A contratação de serviços de processamento e armazenamento de dados e computação em nuvem pelo Banese deve atender aos requisitos previstos em circular normativa interna e devem atender as regulamentações por completo os serviços considerados como relevantes pela instituição que:

I- Causem impacto "Alto" ou "Crítico" ao negócio devido ao não atendimento da confidencialidade, integralidade ou disponibilidade;

II- Façam uso de informações classificadas como confidencial.

CAPÍTULO XVI – GESTÃO DA POLÍTICA

Art. 49. A gestão desta Política ficará a cargo da Diretoria de Finanças, Controles e Relações com Investidores - DIFIC através da Superintendência de Gestão de Riscos – SUGER e Área de Segurança da Informação e Continuidade de Negócios – ARSEC.

CAPÍTULO XVII – DISPOSIÇÕES FINAIS (*)

Art. 50. Os casos omissos serão avaliados pelo COMEC ou Diretoria Executiva, conforme o caso.

Art. 51. O colaborador do Banese poderá encaminhar, por escrito, propostas para alteração do texto da Política Corporativa de Segurança da Informação e Cibernética, que deverão ser submetidas à análise da Área de Segurança da Informação e Continuidade de Negócios – ARSEC em conjunto com o Comitê de Ética e Conformidade – COMEC, a quem compete atualizar e emitir parecer opinativo à Diretoria Executiva – DIREX, a qual deverá submeter à aprovação final ao Conselho de Administração - CONAD. Esta Política deverá ser revisada, no mínimo anualmente.

Art. 52. Todos os colaboradores Banese e coligadas devem conhecer e cumprir as diretrizes dispostas nesta Política. (*)

Art. 53. 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.

Art. 54. Quaisquer indícios de irregularidades no cumprimento das determinações desta política serão alvo de investigação interna e devem ser comunicadas imediatamente se reportando por escrito a ARSEC que fará análise e encaminhamentos necessários.

(*) Alterado em relação à versão anterior.