BANCO GUANABARA

2025

Política De Segurança Cibernética

1 POLÍTICA DE SEGURANÇA CIBERNÉTICA

1.1 INTRODUÇÃO

A Segurança Cibernética, constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

A informação é um dos principais patrimônios do mundo dos negócios. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um negócio. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas. Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos ao Banco Guanabara, prejudicando seu crescimento e vantagem competitiva.

O uso da informação no Banco Guanabara envolve recursos computacionais e informações que necessitam estar permanentemente protegidos contra acessos indevidos, adulterações e ataques cibernéticos.

Atentos a isso, e como parte de um conjunto de medidas de segurança, fica imprescindível a implantação de uma Política de Segurança Cibernética, o alicerce dos esforços de proteção à informação do Banco Guanabara.

1.2 OBJETIVO

A Política de Segurança Cibernética tem como objetivo estabelecer os princípios, conceitos, valores e práticas que devem ser adotados na utilização dos recursos que tangem as informações acessadas pelos administradores, funcionários, prestadores de serviço e/ou outros colaboradores do Banco Guanabara na sua atuação interna e com o mercado. Esta política estabelece os requisitos a fim de proporcionar condições que assegurem a integridade, a confidencialidade e a disponibilidade, bem como a legalidade da informação.

O Banco Guanabara incorpora em seus valores corporativos a convicção de que o exercício de suas atividades e a expansão de seus negócios devem se basear em princípios éticos, os quais devem ser compartilhados por todos os seus Colaboradores. Na constante busca do seu desenvolvimento e da satisfação dos clientes, o Banco Guanabara busca transparência e cumprimento da legislação aplicável às suas atividades.

A publicação desta Política representa o compromisso de todos os que trabalham no Banco Guanabara com os valores e as práticas fundamentadas na integridade, confiança e lealdade. Portanto, a constante busca do desenvolvimento do Banco Guanabara e a defesa dos interesses dos clientes estarão sempre pautadas nas diretrizes aqui expostas.

1.3 DIRETRIZES GERAIS

Direitos de acesso são concedidos baseados na necessidade que um usuário possui para realizar suas atividades laborais. Por padrão será concedido o acesso mínimo necessário para que o usuário exerça suas atividades

profissionais (estratégia do privilégio mínimo) de acordo com dados informados pela área de RH e o gestor imediato do usuário.

Toda e qualquer credencial de acesso é pessoal e intransferível, sendo responsabilidade exclusiva do usuário a qual lhe foi atribuída. Desta forma, o usuário é integralmente responsável por sua utilização, incluindo qualquer ato irregular ou ilícito exercido por outro indivíduo e/ou organização de posse de sua credencial de acesso.

O Banco Guanabara se resguarda da má utilização, ou mesmo de uso de recursos do próprio empregado, terceirizados ou prestadores de serviços dentro das dependências da empresa, a fim de obter benefícios ou outros tipos de vantagens.

O Banco Guanabara se resguarda ao direito de monitoramento dos recursos computacionais para a verificação do correto seguimento das regras estabelecidas quanto à utilização da infraestrutura tecnológica do Banco Guanabara por parte dos usuários, sem, contudo, constituir quaisquer violações à intimidade, vida privada, honra ou imagem da pessoa monitorada.

Não haverá expectativa de privacidade na utilização da infraestrutura tecnológica e dos sistemas de informação do Banco Guanabara.

A infraestrutura tecnológica e as Informações Confidenciais têm caráter de ferramenta de trabalho e são disponibilizadas para os usuários desenvolverem suas atividades laborais, portanto, é proibida a utilização para fins particulares, exceto nos casos expressamente previstos.

Todas as Informações Confidenciais geradas, acessadas, manuseadas, armazenadas ou descartadas, seja por processo automático, mecânico ou manual por um usuário no exercício de suas atividades são de propriedade e/ou direito de uso exclusivo do Banco Guanabara, reservados todos os direitos de propriedade intelectual.

Ativos de informação de propriedade da Banco Guanabara devem ser utilizados em conformidade com o Código de Ética do Grupo Guanabara, cabendo aos usuários manter sigilo absoluto sobre as Informações Confidenciais.

Os usuários deverão receber treinamento/orientações sobre as melhores práticas de segurança da informação ao ser efetivado na empresa e, pelo menos, uma vez ao ano, independentemente de seu nível hierárquico.

Os usuários deverão manter suas mesas limpas, evitando deixar a vista documentos confidenciais ou que possam prover Informações Confidenciais (política da mesa limpa).

Ao se afastar de seus computadores os usuários deverão efetuar o bloqueio de tela, evitando deixar a vista Informações Confidenciais ou permitir que pessoas não autorizadas realizem ações indevidas em seu nome.

1.4 ATRIBUIÇÕES E RESPONSABILIDADES

Os funcionários e prestadores de serviços diretamente contratados pelo Banco Guanabara devem aderir formalmente, comprometendo-se a agir de acordo com as políticas de Segurança Cibernética.

- **Usuário:** Funcionário do Banco Guanabara com vínculo empregatício ou terceirizado alocado na prestação de serviços, independente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar os recursos computacionais ou obter acesso às informações do Banco Guanabara para o desempenho de suas atividades profissionais;

- **Terceirizado ou terceiro:** Todo e qualquer indivíduo que não seja empregado (possua vínculo empregatício) do Banco Guanabara e que, para prestar o serviço para o qual ele ou a empresa a qual trabalhe foi contratada, precise de acesso a algum recurso computacional (hardware ou software) de propriedade do Banco Guanabara;

- **Gestor da Informação:** Usuário que exerça função gerencial, ocupando cargo permanente na estrutura organizacional do Banco Guanabara, e que tenha criado, adquirido ou recebido em confiança determinada informação;

- **Diretoria Executiva:** A Diretoria Executiva do Banco Guanabara, através do seu Diretor Presidente, Pedro Aurélio Barata de Miranda Lins, é responsável pela gestão centralizada de segurança cibernética, bem como do plano de ação de respostas a incidentes;

- **TI:** Responsável por coordenar e conduzir a gestão da segurança da informação armazenada ou trafegada através de algum recurso computacional;

- **Auditoria Interna:** Responsável por monitorar o cumprimento desta Política;

- **Jurídico:** Responsável por realizar pareceres sobre incidentes de Segurança da Informação sob o enfoque legal, com a finalidade de recomendar atualizações e/ou alterações que julgar cabíveis a esta Política. Deverá também fornecer suporte jurídico em relação ao tratamento legal da infração do dever de confidencialidade das Informações Confidenciais;

- **Comunicação:** Responsável por apoiar a divulgação e orientação desta Política para todos os usuários do Banco Guanabara. Deverá também observar nas mídias sociais ocorrências relacionadas ao comprometimento da Segurança das Informações do Banco Guanabara;

- **RH:** Responsável por coletar dos colaboradores durante o processo de contratação a assinatura do Termo de Responsabilidade e Confidencialidade com a Política de Segurança Cibernética;

- **Suprimentos:** Responsável por coletar dos terceirizados durante o processo de contratação a assinatura do Termo de Responsabilidade e Confidencialidade com a Política de Segurança Cibernética.

1.5 PRINCÍPIOS E DEFINIÇÕES

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: irrefutabilidade, autenticação e o controle de acesso. Os benefícios de

seguir estes princípios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos (ISO 27002 A.5.1.1).

- **Ativo:** Tudo que tenha valor para o Banco Guanabara;

- **Ativo de Informação:** Ativos do Banco Guanabara relacionados a conteúdo de informação e dados que tenham valor para a organização. Poderão ser de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal ou qualquer outra natureza, assim como quaisquer dados ou informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confinadas ao Banco Guanabara por parceiros, clientes, empregados e terceiros, não importando se protegidas ou não, de confidencialidade, em formato escrito ou verbal, físicas ou digitalizadas, armazenadas, trafegadas ou transitando pela infraestrutura computacional do Banco Guanabara, além dos documentos em suporte físico ou mídia eletrônica, transitados dentro e fora de sua estrutura física do Banco Guanabara;

- **Informações Confidenciais:** A expressão “Informações Confidenciais” e suas variações representam todas as informações e materiais, sem exceção, incluindo, sem se limitar a estes exemplos, tecnologia da informação, hardware, software, pesquisa e desenvolvimento de conhecimento, dados, banco de dados, protocolos e qualquer documentação ou documentos relacionados às atividades internas e externas do Banco Guanabara, disponibilizados ao usuário sejam eles expressos de forma oral, escrita ou através de qualquer outro meio;

- **Recursos Computacionais:** Equipamentos, softwares e demais ativos que constituem a infraestrutura computacional física e lógica do Banco Guanabara, tais como, mas não limitado a: computadores servidores, computadores para uso individual e coletivo, dispositivos móveis, equipamentos de armazenamento, equipamentos de encaminhamento e troca de informações, impressoras, equipamentos multifuncionais, suprimentos de informática e periféricos;

- **Rede de computadores:** Agrupamento de dispositivos ativos (computadores, comutadores, roteadores, entre outros) que utilizam regras de comunicação (protocolos) para o compartilhamento de informações e recursos entre si;

- **Sistemas de informação:** Conjunto de procedimentos estruturados, planejados e organizados que abrangem pessoas, máquinas e/ou métodos organizados para coletar, processar, transmitir e disseminar dados que representem informação para o usuário e/ou cliente. Sua execução pode ser manual ou automatizada.

- **VLAN:** rede local que reúne um conjunto de máquinas de maneira lógica, não física. Neste tipo de rede há uma segmentação lógica (software) baseada em um agrupamento de máquinas graças a critérios dos endereços MAC, números de porta, protocolo e localização.

1.6 SEGURANÇA FÍSICA E LÓGICA

Segurança física é a forma de proteger equipamentos e informações contra usuários que não possuem autorização para acessá-los. Enquanto segurança lógica é um conjunto de recursos executados para proteger o sistema, dados e programas contra tentativas de acessos de pessoas ou programas desconhecidos. As duas formas de proteção são essenciais para lidar com as ameaças à informação.

Os equipamentos e instalações de processamento de informação críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso físicos e lógicos apropriados, incluindo proteção contra desastres e ameaças ambientais.

1.6.1 ESTAÇÕES DE TRABALHO

Apenas os equipamentos para estação de trabalho e software disponibilizados e/ou homologados pelo Banco Guanabara podem ser instalados e conectados à rede do Banco Guanabara. Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não podem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da empresa.

Estes recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções no Banco Guanabara ou para outras situações formalmente permitidas. O uso dos recursos de tecnologia do Banco Guanabara pode ser examinado, auditado ou verificado pela empresa, mediante autorização expressa da Diretoria, sempre respeitando a legislação vigente.

Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados. Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à área de Riscos e Controles Internos. É necessário que o gestor do usuário o autorize a usar o computador. Deve ser feita uma solicitação à área de Tecnologia, que autorizará tecnicamente e fará a liberação mediante a disponibilidade de recursos.

É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da área de Tecnologia. É desabilitado ao usuário implantar ou alterar componentes físicos no computador. A instalação ou utilização de software não autorizados pelos usuários constitui em crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, sujeitando os infratores à pena de detenção e multa. O Banco Guanabara não se responsabiliza por qualquer ação individual que esteja em desacordo com a Lei mencionada acima.

1.6.2 DATA CENTER

São instalações que possam oferecer proteção contra incêndio, inundações, impactos de alta intensidade, qualquer tipo de poluição, interferência eletromagnética, vibrações e outros. Abrange todo o ambiente onde os sistemas de informação estão instalados: prédio, portas de acesso, trancas, piso, salas, computadores.

Os sistemas críticos e essenciais ao negócio e toda a infraestrutura de suporte e segurança devem estar armazenados em estruturas de Data Center certificadas no nível Tier III ou superior, emitido pelo UpTime Institute, sediado em Santa Fé, NM, EUA.

1.6.3 PREVENÇÃO A PERDA DE INFORMAÇÕES

É diretriz que toda informação crítica e sensível de propriedade do Banco Guanabara seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

Para isto realizado, o Banco Guanabara, utiliza uma variedade de medidas que estejam de acordo com as necessidades da organização e da natureza dos sistemas de informação existentes. Para proteção da infraestrutura do Banco Guanabara contra um ataque externo, utilizamos ferramentas e controles contra: ataques que afetem a disponibilidade (DDoS), Spam, Phishing, ataques avançados persistentes (APT), Malware, invasão de dispositivos de rede e servidores, ataques de aplicação e scan externos.

No sentido de nos protegermos contra vazamento de informações, utilizamos diversas ferramentas preventivas contra vazamento de informação, instaladas em estações de trabalho, no serviço de correio eletrônico, no serviço de navegação WEB, no serviço de impressão, além de criptografia de disco em notebooks e solução de proteção de dispositivos móveis.

1.7 CONTROLE DE ACESSO

Contas e senhas são atualmente o mecanismo de autenticação mais usado para o controle de acesso a sistemas e serviços. É por meio de contas e senhas que os sistemas conseguem identificar os usuários, definir suas ações e registrar o que o usuário pode realizar.

Todos os usuários do Banco Guanabara para acessarem seus sistemas e informações, devem possuir um nome único de usuário e senha.

1.7.1 POLÍTICA DE SENHAS

Uma senha serve para autenticar uma conta de usuário, ou seja, é usada no processo de verificação da identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados, principalmente, pela simplicidade que possui, sendo utilizado em todos os sistemas e serviços tecnológicos do Banco Guanabara.

Uma senha deve ser bem elaborada, sendo difícil de ser descoberta (forte) e fácil de ser lembrada. Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la. Também não convém que você crie uma senha fácil de ser lembrada se ela puder ser facilmente descoberta.

Alguns elementos que você não deve usar na elaboração de suas senhas são:

- Qualquer tipo de dado pessoal: evite nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas (estes dados podem ser facilmente obtidos e usados por pessoas que queiram tentar se autenticar como você);

- Sequências de teclado: evite senhas associadas à proximidade entre os caracteres no teclado, como "1qaz2wsx" e "QwerTAsdfG", pois são bastante conhecidas e podem ser facilmente observadas ao serem digitadas;

- Palavras que façam parte de listas: evite palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas etc. Existem programas que tentam descobrir senhas combinando e testando estas palavras e que, portanto, não devem ser usadas;

Normalmente se gerencia muitas contas e senhas diferentes que precisamos memorizar e combinar para acessar todos os sistemas e serviços que utilizamos e que exigem autenticação.

Alguns importantes cuidados que devem-se tomar para se proteger ainda mais de possíveis danos as informações do Banco Guanabara são:

- Reutilizar as senhas: usar a mesma senha para acessar diferentes contas pode ser bastante arriscado, pois basta ao atacante conseguir a senha de uma conta para conseguir acessar as demais contas onde esta mesma senha foi usada;

- Procure não usar a mesma senha para assuntos pessoais e profissionais; jamais reutilize senhas que envolvam o acesso a dados sensíveis, como as usadas em Internet Banking ou e-mail;

- Procure não usar opções como "Lembre-se de mim" e "Continuar conectado": o uso destas opções faz com que informações da sua conta de usuário sejam salvas em cookies que podem ser indevidamente coletados e permitam que outras pessoas se autentiquem como você. Jamais as utilize em computadores de terceiros;

- Salvar as senhas no navegador Web: esta prática é bastante arriscada, pois caso as senhas não estejam criptografadas com uma chave mestra, elas podem ser acessadas por códigos maliciosos, atacantes ou outras pessoas que venham a ter acesso ao computador.

Alguns elementos que você deve usar na elaboração de suas senhas são:

- Números aleatórios: quanto mais ao acaso forem os números usados melhor, principalmente em sistemas que aceitem exclusivamente caracteres numéricos;

- Grande quantidade de caracteres: quanto mais longa for a senha mais difícil será descobri-la. Apesar de senhas longas parecerem, a princípio, difíceis de serem digitadas, com o uso frequente elas acabam sendo digitadas facilmente;

- Diferentes tipos de caracteres: quanto mais "bagunçada" for a senha mais difícil será descobri-la. Procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas. O uso de sinais de pontuação pode dificultar bastante que a senha seja descoberta, sem necessariamente torná-la difícil de ser lembrada.

Algumas dicas práticas que você pode usar na elaboração de boas senhas são:

- Selecione caracteres de uma frase: baseie-se em uma frase e selecione a primeira, a segunda ou a última letra de cada palavra;

- Utilize uma frase longa: escolha uma frase longa, que faça sentido para você, que seja fácil de ser memorizada e que, se possível, tenha diferentes tipos de caracteres. Evite citações comuns (como ditados populares) e frases que possam ser diretamente ligadas a você (como o refrão de sua música preferida);

- Faça substituições de caracteres: invente um padrão de substituição baseado, por exemplo, na semelhança visual ("w" e "vv") ou de fonética ("ca" e "k") entre os caracteres. Crie o seu próprio padrão pois algumas trocas já são bastante óbvias.

Existem serviços que permitem que você teste a complexidade de uma senha e que, de acordo com critérios, podem classificá-la como sendo, por exemplo, "muito fraca", "fraca", "forte" ou "muito forte". Ao usar estes serviços é importante ter em mente que, mesmo que tenha sido classificada como "muito forte", pode não ser uma boa senha caso contenha dados pessoais que não são de conhecimento do serviço, mas que podem ser de conhecimento de invasores.

As regras de criação ou alteração de senhas do Banco Guanabara segue o seguinte padrão, considerando-se até 3 destas 4 regras de formação da senha:

- Conter pelo menos uma letra minúscula;
- Conter pelo menos uma letra maiúscula;
- Conter números (0 a 9);
- Conter símbolos incluindo: ! @ # $ % ^ & * - _ + = [ ] { } | \ : ‘ , . ? / ` ~ “ < > ( ) ;
- Tamanho mínimo de 8 caracteres;
- Não é permitido usar partes do nome do funcionário;
- Mandatório alterar a senha a cada 90 dias.

Por motivo de segurança a conta é bloqueada após 05 tentativas de acesso com senha inválida.

1.7.2 PERMISSIONAMENTO

Conforme definido pela Matriz de Segregação de Funções do Banco Guanabara, será atribuído a cada conta de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação, única e exclusivamente as permissões definidas nesta Matriz. Sendo associado a um responsável identificável como pessoa física, sendo os usuários (login) individuais de funcionários internos de responsabilidade do próprio. Assim, é possível realizar a identificação dos detentores da informação para eventual responsabilização, se for o caso.

Todo acesso a sistemas, serviços e diretórios de informações do Banco Guanabara deve ser controlado. Somente poderão acessar tais sistemas, serviços e diretórios de informação os funcionários previamente autorizados pelos seus respectivos gestores, observado o disposto na Política de Segurança Cibernética.

O controle do acesso a sistemas de informações da Gestora levará em conta as seguintes premissas:

- Garantia do Gestor de que o nível de acesso concedido ao funcionário é adequado ao seu perfil (princípio do acesso mínimo);
- Cancelamento do acesso concedido a funcionários desligados, afastados ou que tenham sua função alterada na Gestora.

As informações referentes as permissões do funcionário deverão ser preenchidas pelo seu gestor direto e entregá-la a área de RH, comunicando esta necessidade, e a área de RH por sua vez, informará a área de Tecnologia validando os acessos que o funcionário terá direito e quais serão restringidos. A área de Tecnologia fará os devidos cadastramentos e informará ao funcionário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada imediatamente após o primeiro acesso.

Quando houver necessidade de acesso para usuários terceiros, sejam eles temporários ou não, a permissão de acessos será bloqueada tão logo este tenha terminado a sua prestação de serviço e/ou encerrado seu prazo de contrato. Havendo nova necessidade, poderá ser simplesmente solicitado novo acesso nas mesmas condições.

Periodicamente as áreas de controle do Banco Guanabara devem verificar a validade e atualidade das permissões concedidas.

1.7.3 CONTROLE DE IMPRESSÃO

Em todo o mundo, empresas de todos os tamanhos possuem várias impressoras e multifuncionais que são utilizadas para impressões confidenciais e não confidenciais. Na maioria das vezes não existem controles de quem está imprimindo e o que está imprimindo. Além do controle e monitoramento de uso, impressoras e multifuncionais também podem ser alvo de malware, *hacking* ou violação de dados.

As impressoras e multifuncionais são tradicionalmente vistos como dispositivos que não oferecem riscos as empresas, porém com o passar do tempo, as impressoras e multifuncionais tornaram-se mais sofisticadas e possuem conectividade de rede, disco rígido e armazenamento de memória, tornando-se dispositivos inteligentes que podem ser usados para obter acesso à rede e causar perdas irreparáveis para uma empresa.

Como diretriz a impressão de documentos sigilosos no Banco Guanabara será feita em impressoras dedicadas e associadas diretamente a um único funcionário com autorização para tal.

Existe o controle por sistema de bilhetagem que possibilita identificar o documento impresso e cópias realizadas por cada funcionário. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não-autorizado. Isto é, documentos esquecidos nas impressoras, ou com demora para retirada, ou até mesmo em cima da mesa, podem ser lidos, copiados ou levados por outro funcionário ou por alguém de fora da empresa.

Desta forma é conscientizado aos funcionários a devida guarda destes documentos em locais fechados e seguros ou mesmo o descarte e fragmentadora.

1.8 CONTROLE DE ATIVOS

São considerados ativos de segurança cibernética todos os elementos que contém informação de forma direta ou indireta do Banco Guanabara, ou mesmo que tenha alguma relação com a transmissão de informações.

Os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, e ter documentação e planos de manutenção atualizados. Todos os ativos de informação devem ser devidamente guardados, inclusive documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.

1.8.1 USO DOS ATIVOS

Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes do Banco Guanabara.

Todos os ativos de rede, incluindo cabeamento, devem ter acesso físico restrito e seguro, evitando a exposição a danos externos acidentais ou mesmo mal-intencionados.

O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção à regra. A porta USB dos ativos é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais. Neste caso, os modens móveis e os pen drives tem uso controlado.

Desta forma é implantado o bloqueio do acesso as portas USB dos ativos para proteção contra vírus e cópia indevida de dados. Para liberação das portas USB dos ativos é necessário justificar o uso e a aprovação do gestor do departamento do solicitante. Para notebooks de gerentes e cargos acima esta liberação é efetuada por padrão.

É implantado o bloqueio do acesso à sites de armazenamento de dados em nuvem (cloud) e o bloqueio de sistemas de gerenciamento de computador a distância.

Ativos particulares e de terceiros para serem usados dentro da rede do Banco Guanabara, precisam previamente serem avaliados pela área de Tecnologia, para serem verificadas, uso de antivírus, Firewall ativo, atualização do antivírus e existência de vírus.

1.8.2 RESPONSABILIDADES

Todos têm um responsável que responde organizacionalmente pela sua utilização, sendo responsável por qualquer avaria que não seja por incidentes de causas naturais.

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos podendo danificar e corromper dados.

Cada funcionário é responsável pelo uso dos ativos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados.

Os ativos de tecnologia do Banco Guanabara, disponibilizados para os funcionários, não podem ser repassados para outra pessoa interna ou externa à empresa.

É responsabilidade da área contratante encaminhar os ativos de terceiros sob sua responsabilidade para verificação e aprovação de uso na rede do Banco Guanabara pela área de TI.

Ao identificar quaisquer irregularidades no ativo de tecnologia o funcionário responsável por ele, deve comunicar imediatamente à área de Tecnologia.

Nos casos em que houver violação destas diretrizes, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis.

1.9 COMPORTAMENTO SEGURO

É muito importante também para a segurança cibernética, a adoção de boas práticas de comunicação verbal dentro e fora da empresa. Deve-se ter cuidado ao tratar de assuntos da empresa dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

1.9.1 AMBIENTE INTERNO

O controle de acesso é uma parte central da segurança de uma empresa do ponto de vista da segurança cibernética. Por isso, é fundamental que ao entrar e permanecer nas dependências do Banco Guanabara seja utilizado de forma visível o seu crachá. Câmeras de gravação de vídeo foram instaladas nas dependências do Banco Guanabara para garantir a sua segurança.

Cuidado com o lixo que você produz. O lixo pode ser uma fonte de informações para pessoas mal-intencionadas. Destrua os documentos que contenham informações sensíveis, pessoais ou do Banco Guanabara antes de descartá-los.

Cada tarefa desenvolvida nos sistemas do Banco Guanabara precisa ter um responsável. A única forma de saber o responsável por cada atividade é através da identificação do funcionário feito com a sua identificação (nome

de usuário e senha), que é de sua responsabilidade. Portanto, cuidado com seus dados, seja na rede ou nos sistemas, pois sua identificação serve para garantir que você é realmente quem está usando esse acesso.

Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você, porém, a responsabilidade por tudo que ela fizer será sua. Não escreva a senha em local público ou de fácil acesso.

É proibido reproduzir nos sistemas, serviços e nas dependências do Banco Guanabara quaisquer materiais recebidos pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

Deve-se também estar ciente que uma mensagem de correio eletrônico do Banco Guanabara é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

É proibido criar, copiar ou encaminhar mensagens ou imagens utilizando os sistemas e serviços tecnológicos do Banco Guanabara que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Empresa, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem do Banco Guanabara;
- Sejam incoerentes com o nosso Código de Ética.

Adote um comportamento seguro:

- Não compartilhe nem divulgue sua senha a terceiros;
- Não transporte informações confidenciais do Banco Guanabara em qualquer meio (CD, DVD, pendrive, papel, fitas etc.) sem as devidas autorizações e proteções;
- Não abra mensagens de origem desconhecida;

- Armazene e proteja adequadamente documentos impressos e arquivos eletrônicos que contêm informações confidenciais;
- Siga corretamente a política para uso de internet e correio eletrônico estabelecida pelo Banco Guanabara.

Mantenha a “mesa limpa” e a “tela limpa”. Ao deixar sua estação de trabalho, faço o bloqueio desta ou desative seu identificador de acesso. Nenhuma informação confidencial deve ser deixada à vista em sua mesa de trabalho, seja em papel ou em quaisquer dispositivos, eletrônicos ou não. Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

1.9.2 AMBIENTE EXTERNO

Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais etc.).

Não discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de texto, exceto quando encaminhadas ao Banco Guanabara.

Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora da empresa ou próximos a pessoas desconhecidas. Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento as pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a empresa. Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome do Banco Guanabara.

No ambiente externo, é melhor ficar atento:

- Ao falar sobre informações restritas ou segredos profissionais em um lugar público ou por telefone tenha cuidado especial. Frequentemente, as pessoas são o elo mais fraco na segurança da informação de uma empresa;

- Quando seu equipamento viajar com você, evite deixá-lo por muito tempo sozinho em uma sala ou mesa e atenção redobrada em lugares públicos. Qualquer pen drive ou conexão de rede pode conter dados valiosos.

1.10 SEGURANÇA DA INFORMAÇÃO

Segurança da Informação consiste na preservação da confidencialidade, integridade e disponibilidade da informação. O fundamento da segurança da informação é estabelecer um conjunto de regras e diretrizes que permitam um nível de segurança aceitável diante das ameaças existentes à informação.

1.10.1 PRIVACIDADE DOS DADOS

A proteção e privacidade de dados dos clientes refletem os valores do Banco Guanabara e reafirmam o seu compromisso com a melhoria contínua da eficácia do processo de Proteção de Dados.

Quanto às informações de nossos clientes, são obedecidas as seguintes determinações:

- São coletadas de forma ética e legal, para propósitos específicos e devidamente informados;
- Somente serão acessadas por pessoas autorizadas e capacitadas para o seu uso adequado;
- Poderão ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados;
- As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente serão fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações.

1.10.2 MANUTENÇÃO DE REGISTROS E LOGS

O Banco Guanabara mantém os logs de acesso à rede e sistemas, e verifica regularmente, quaisquer desvios de padrão no uso de computadores, arquivos em rede, sistemas, serviços ou acessos que não sejam autorizados pela política de segurança cibernética.

1.10.3 CLASSIFICAÇÃO DAS INFORMAÇÕES

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a empresa ou pessoa. Além do que está armazenado nos computadores, a informação também está impressa em relatórios, documentos, arquivos físicos, ou até mesmo repassada através de conversas nos ambientes interno e externo.

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

O Banco Guanabara segue os critérios a seguir:

- Pública: É uma informação do Banco Guanabara ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade dela;

- Interna: É uma informação do Banco Guanabara que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços;

- Confidencial: É uma informação crítica para os negócios do Banco Guanabara ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais ao Banco Guanabara ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores;

- Restrita: É toda informação que pode ser acessada somente por usuários do Banco Guanabara explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

1.10.4 CONSCIENTIZAÇÃO

O Banco Guanabara promove a disseminação dos princípios e diretrizes de Segurança Cibernética por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação e seus controles.

1.11 TRATAMENTO DAS INFORMAÇÕES

É diretriz que toda informação de propriedade do Banco Guanabara seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

A informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

1.11.1 CÓPIA DE SEGURANÇA

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria das informações do Banco Guanabara, deve-se realizar cópias de segurança das informações críticas ao negócio:

- A cópia de segurança das informações críticas é feita de forma centralizada no ambiente dos equipamentos de servidores corporativos dedicados para esta função, sob a responsabilidade da área de Tecnologia;

- A área de Tecnologia fornecerá o serviço de recuperação de informações críticas, a partir de arquivos de cópia de segurança, cumprindo parâmetros de nível de serviço previamente estabelecido;

O Banco Guanabara conta com um serviço e estrutura de cofre lacrado seguro e com acesso restrito, onde as mídias das cópias de segurança são armazenadas inicialmente e controladas através de registro eletrônico. Em periodicidade quinzenal e segundo regras estabelecidas na política de Backup/*Restore*, mídias são encaminhas para o armazenamento definitivo por empresa especializada nesta área. Este processo é auditado periodicamente pela área de Tecnologia com o intuito de verificar se as normas estão sendo cumpridas, para que as mídias e seus conteúdos não sejam violados ou danificados.

As mídias elencadas pela política para descarte são encaminhadas a empresa especializada que possui um procedimento de eliminação dos dados e destruição física da mídia, possibilitando a emissão de certificado adequado com as normas estabelecidas para esta atividade.

1.11.2 PROCEDIMENTOS PARA TERCEIROS

Fornecedores, prestadores de serviços e parceiros, também podem representar uma fonte significativa de Riscos de Segurança Cibernética.

Toda informação relacionada às operações do Banco Guanabara, gerada ou desenvolvida nas suas dependências ou remotamente, se contratado nesta modalidade de trabalho, durante a execução das atividades de prestador de serviços, constitui ativo desta instituição financeira, essencial à condução de negócios, e deve respeitar as mesmas políticas de segurança e ter o mesmo tratamento das informações produzidas pelo Banco Guanabara.

É necessária uma proteção contratual para controle e responsabilização no caso de uso da prestação de serviços de terceiros, garantindo proteção caso sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção do Banco Guanabara em processos de mudança.

Os colaboradores terceiros do Banco Guanabara devem ser treinados periodicamente sobre os conceitos da Segurança Cibernética, através de um programa efetivo de conscientização.

1.11.3 PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

A computação em nuvem pode ser considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações de serviços externos, envolve determinados riscos que devem ser levados em conta, demandando certos cuidados proporcionais a esta nova identificação de ameaças.

Deve-se adotar práticas de governança corporativa e de gestão proporcionais à representatividade e relevância do processamento e armazenamento de informações críticas em nuvem e aos riscos a que estejam expostos.

Também será necessário a verificação da capacidade do prestador de serviço assegurar o cumprimento da legislação e da regulamentação vigente, sua aderência a certificações exigidas e o acesso da empresa contratante aos dados e às informações a serem processadas e/ou armazenadas. A garantia da confidencialidade, integridade, disponibilidade e a recuperação dos dados e das informações deve ser fornecida pelo prestador de serviços em nuvem contratado. Também deve ser garantido ao Banco Guanabara o acesso às informações e recursos de gestão adequados ao monitoramento dos serviços prestados.

Os dados do Banco Guanabara devem ser identificados e segregados por meio de controles físicos e lógicos pelo prestador de serviço. Medidas de segurança para a transmissão e armazenamento dos dados devem ser estabelecidos em contrato com o fornecedor de serviços em nuvem.

O Banco Guanabara deve possuir recursos e competências necessárias para a adequada gestão dos serviços a serem contratados.

Conforme a Resolução 4.658/2018 do Banco Central do Brasil, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, o Banco Guanabara assegura-se procedimentos efetivos para a aderência às regras previstas nesta regulamentação em vigor.

1.12 MONITORAMENTO E TESTES

O Banco Guanabara realizará o monitoramento e testes periódicos de segurança para os sistemas e serviços de informações críticas anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Mecanismos de monitoramento devem ser implementados, de forma a verificar a efetividade da política de segurança cibernética e identificar eventuais incidentes, detectando as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

1.12.1 REGISTROS DE AUDITORIA

Compreendendo a auditoria como elemento essencial em termos de solução de gestão dentro de uma empresa, a área de Tecnologia mantém por pelo menos 1 ano, registros de acesso e utilização das informações críticas dos sistemas e serviços tecnológicos do Banco Guanabara.

1.12.2 MONITORAMENTO DOS SISTEMAS

O ambiente de tecnologia do Banco Guanabara será monitorado, por meio de indicadores e geração de históricos:

- uso da capacidade instalada da rede e dos equipamentos;
- tempo de resposta no acesso à internet e aos sistemas críticos;
- de períodos de indisponibilidade no acesso à internet e aos sistemas críticos;
- de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- das atividades durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

1.12.3 SEGMENTAÇÃO DA REDE CORPORATIVA

O Banco Guanabara aplica segmentação de rede, com VLAN para empregados, VLAN para visitante e uma segregação entre estações de trabalho e os servidores das soluções sistêmicas do ambiente. A autenticação na rede corporativa se dá via AD (*Active Directory*), exclusivo do Banco Guanabara.

1.12.4 REGISTRO DE FALHAS E GESTÃO DE MUDANÇAS (GMUD)

O Banco Guanabara faz uso de um sistema de registro de ocorrências de todos os incidentes críticos ocorridos, e através dele estão mapeados para consulta a descrição do incidente, as suas consequências e as ações que foram tomadas.

A área de Tecnologia é responsável por participar, documentar, homologar e implementar toda e qualquer alteração seja de acesso, hardware e software ou que tenha impacto direto no negócio ou operacional do Banco Guanabara. As solicitações devem ser encaminhadas do gestor responsável pela solicitação para área de Tecnologia, e tais mudanças devem ser registradas em sistema para acompanhamento histórico.

Os funcionários do Banco Guanabara deverão comunicar à área de Controladoria & Gestão de Riscos quaisquer falhas observadas às normas de segurança cibernética que tenham conhecimento. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

1.13 VIGÊNCIA E VALIDADE

Periodicamente, a Política de Segurança da Informação do Grupo Guanabara será avaliada, para que sejam feitos os ajustes necessários para sua boa e efetiva aplicação e a Política será revisada a cada 02 (dois) anos ou em período inferior, sempre que se fizer necessário.

1.14 REFERÊNCIAS

- Resolução 4.658/2018; https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf
- Resolução 4.557/2017; https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50344/Res_4557_v1_O.pdf
- ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos; https://www.abntcatalogo.com.br/norma.aspx?ID=306580
- ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação; https://www.abntcatalogo.com.br/norma.aspx?ID=306582
- LEI Nº 13.709/2018; e http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm