BANCO GUANABARA

POLÍTICA DE SEGURANÇA CIBERNÉTICA

VERSÃO 1.1

DEPARTAMENTO DE CONTROLADORIA E GESTÃO DE RISCOS
www.bancoguanabara.com.br

SUMÁRIO

1 OBJETIVO

A Segurança Cibernética tem o objetivo de garantir a confidencialidade, integridade e disponibilidade das informações e sistemas de informação.

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.

1.1 Abrangência

Esta política destina-se como normativo a todos os colaboradores internos e externos do Banco Guanabara bem como prestadores de serviços e consultores em geral que tenham qualquer contato com informações do Banco. Ao público em geral, esta política cumpre a função de informar dos principais temas de segurança da informação e como o Banco Guanabara empenha-se em atendê-los.

1.2 Referências

Esta política e a versão resumida da política “Segurança Cibernética” versão 002 e que está disponível para consulta apenas interna aos colaboradores internos, prestadores de serviços e consultores.

2 PROTEÇÃO DA CONFIDENCIALIDADE E PRIVACIDADE

Todas as informações confidenciais são de propriedade e/ou direito de uso exclusivo do Banco Guanabara, reservados todos os direitos de propriedade intelectual.

Os dados pessoais a que o usuário tiver acesso estão sob o abrigo da Lei 13.708/19 (LGPD) e são de exclusiva propriedade do titular indicado, cabendo ao Banco Guanabara o direito ao tratamento no limite do consentimento registrado.

Para ambos os casos os controles indicados deverão ser sempre aplicados de maneira a garantir a segurança e o tratamento adequado previsto.

3 COMPORTAMENTO SEGURO

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.

A navegação na internet deve ser consciente de forma a evitar sites de conteúdo impróprio e sites bloqueados pelos sistemas do Banco Guanabara.

A troca de mensagens por e-mail, WhatsApp, chat ou outras formas de comunicação não devem conter informações sigilosas ou sensíveis. Assuntos internos devem ser evitados em conversas e comunicações com elementos externos.

O descarte de documentos e ativos tecnológicos deve ser feito de tal forma a garantir que as informações ali contidas sejam destruídas sem opções de recuperação.

3.1 Comportamento em ambiente externo ao Banco Guanabara

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

Credenciais de acesso devem ser mantidas em locais seguros de forma a evitar o roubo, clonagem ou perda.

Nunca devem ser utilizadas redes públicas ou não controladas paras as conexões, tais como aeroportos, hotéis, centros de conferência, cafés etc. Em caso de necessidade, dê preferência ao uso de dados móveis do seu telefone.

4 POLÍTICA DE SENHAS

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

As senhas nunca devem ser compartilhadas sob nenhuma justificativa, independente da situação ou de com quem.

As senhas devem ser fortes e trocadas com regularidade, não sendo aconselhável a sua reutilização ou uso da mesma senha em sistemas diferentes. Senhas fortes são compostas por letras, números, caracteres especiais e devem obedecer aos padrões definidos pela área de Controladoria & Gestão de Riscos do Banco Guanabara.

É recomendado o uso de aplicativos do tipo “cofre de senhas” para a melhor gestão. É proibido gravar senhas em navegadores de internet ou em aplicações web através de funções como “lembrar de mim”, ou semelhante.

5 CONTROLES DE ACESSOS

5.1 Concessão de acessos

Será concedido o acesso mínimo necessário para que o usuário exerça suas atividades profissionais de acordo com dados informados pela área de RH e o gestor imediato do usuário.
Necessidade de acessos adicionais deverão ser solicitadas pelo gestor do colaborador e deverão ser submetidas ao processo de aprovação adequado.

5.2 Credenciais de acesso

Toda e qualquer credencial de acesso é pessoal e intransferível. Assim, o usuário é integralmente responsável por manter suas credenciais de maneira segura e nunca compartilhando-a com ninguém, sob nenhum pretexto ou justificativa.

Qualquer ato irregular ou ilícito com o uso de credenciais de acesso terá automaticamente as consequências atribuídas ao titular das credenciais.

Em caso de extravio, perda ou roubo das credenciais, o usuário deverá informar imediatamente ao seu gestor e ao departamento de RH para o devido cancelamento, bloqueio e eventual emissão de novas credenciais substitutas.

5.3 Controle de acesso lógico

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 usuários previamente autorizados, conforme disposto na versão interna da Política de Segurança Cibernética.
Os acessos aos sistemas do Banco Guanabara devem ser revistos a intervalos regulares e recorrentes de forma a verificar a validade e atualidade das permissões concedidas.

6 USO DOS ATIVOS DE INFORMAÇÃO

Os 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, portanto, é proibida a utilização para fins particulares, exceto nos casos expressamente previstos.

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.

6.1 Segurança de ativos tecnológicos

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, ficando automaticamente proibido o uso de qualquer dispositivo pessoal ou de terceiros que possa armazenar e/ou processar dados.

Qualquer exceção a esta regra deverá ser solicitada e formalmente aprovada ao nível de diretoria.

Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente atribuídos, 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.

Os ativos de tecnologia do Banco Guanabara não podem ser repassados, emprestados ou compartilhados com outras pessoas internas ou externas à empresa.

6.2 Armazenamento externo e móvel

É implantado o bloqueio do acesso as portas USB dos ativos para proteção contra vírus e cópia indevida de dados. Exceções devem ser justificadas e aprovadas.

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.

7 SEGURANÇA FÍSICA

Os acessos às instalações físicas do Banco Guanabara são restritos e monitorados. Todos os colaboradores devem estar devidamente identificados e visitantes devem estar sempre acompanhados por um colaborador responsável. O acesso de visitantes é restrito a áreas comuns e não críticas do banco.

Os sistemas críticos e essenciais ao negócio e toda a infraestrutura de suporte e segurança estão armazenados em estruturas de Data Center próprio do Banco Guanabara e que foram certificadas no nível Tier III ou superior, emitido pelo UpTime Institute, sediado em Santa Fé, NM, EUA. Mais detalhes em https://uptimeinstitute.com/tiers.

7.1 Mesa e tela limpas

As mesas, bandejas de impressão e qualquer outra área de tratamento de informações confidenciais devem ser mantidas livres, evitando deixar informações sigilosas sem o devido cuidado e controle.

Ao se afastar de seu computador, o usuário deverá sempre efetuar o bloqueio de tela. Em caso de uso fora das instalações do Banco Guanabara, o usuário deverá manter-se discreto e com o seu computador preso a um local fixo com cabo de segurança.

8 CONTROLE DE IMPRESSÕES

Como diretriz, a impressão de documentos sigilosos no Banco Guanabara será feita em impressoras dedicadas cujo acesso é restrito somente a pessoal autorizado.

Existe o controle por sistema de bilhetagem que possibilita identificar o documento impresso e cópias realizadas por cada funcionário.

Documentos impressos devem ser protegidos contra perda, reprodução e uso não-autorizado, devendo ser recolhidos imediatamente das bandejas de impressão e mantidos em local de acesso controlado.

9 CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações devem ser classificadas de acordo com os critérios de confidencialidade estabelecidos e conforme as necessidades relacionadas ao negócio, ao compartilhamento ou à restrição de acesso e os impactos no caso de utilização indevida das informações.

A percepção de confidencialidade pode variar conforme o tempo, portanto a classificação deve ser revista periodicamente conforme a natureza da informação.

O Banco Guanabara segue os critérios a seguir:

- Pública: Informação disponível para divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional.
- Interna: Informação cujo acesso de indivíduos externos deve ser evitado, mas pode ser acessada sem restrições por todos os empregados e prestadores de serviços.
- Confidencial: Informação crítica para o Banco Guanabara ou seus clientes e parceiros. É sempre restrita a um grupo específico de pessoas pré-definidas pelo responsável interno da informação.
- Restrita: Informação exclusiva ao usuário do Banco Guanabara explicitamente indicado pelo nome ou por área a que pertence.

10 PROCESSAMENTO E ARMAZENAMENTO DE DADOS EM NUVEM

Conforme a Resolução nº 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 que adota procedimentos efetivos para a aderência às regras previstas na regulamentação em vigor.

11 FORMAÇÃO E TREINAMENTO

Sempre que disponibilizado, os colaboradores deverão atender aos treinamentos e ações de conscientização em segurança da informação e temas correlatos, conforme a indicação de sua gestão.

Todos os colaboradores devem passar por ao menos uma sessão de conscientização em segurança da informação por ano.

12 PROCEDIMENTOS PARA TERCEIROS

Toda informação gerada ou compartilhada com parceiros, fornecedores e prestadores de serviços deve respeitar as mesmas políticas de segurança e ter o mesmo tratamento das informações produzidas pelo Banco Guanabara.

É necessária uma garantia contratual para controle e responsabilização no caso de uso da prestação de serviços de terceiros, garantindo proteção caso sejam a fonte das vulnerabilidades ou exposições a riscos dos ambientes do Banco Guanabara.

Os colaboradores terceiros do Banco Guanabara que atuem no cotidiano do Banco devem ser treinados periodicamente sobre os conceitos da segurança cibernética, através de um programa efetivo de conscientização promovido internamente.

13 MONITORAMENTO

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.

Os recursos computacionais de uso individual podem também ser monitorados para verificações da aplicação das regras de segurança. Este monitoramento não deve ser interpretado como violação à intimidade, vida privada, honra ou imagem da pessoa monitorada uma vez que os objetos monitorados são de propriedade do Banco Guanabara.

O Banco Guanabara realizará testes periódicos de segurança para os seus sistemas e serviços, visando identificar prematuramente vulnerabilidades e reduzir riscos de segurança aos seus sistemas de informação.

14 IRREGULARIDADES, VIOLAÇÕES E INCIDENTES

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.

Os funcionários e colaboradores do Banco Guanabara deverão comunicar à área de Controladoria & Gestão de Riscos quaisquer falhas observadas às normas de segurança cibernética que tenham conhecimento, ainda que apenas sob suspeita.

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.

15 VIGÊNCIA E VALIDADE

A presente Política de Segurança Cibernética passa a vigorar a partir da data de sua homologação e publicação, sendo válida por 12 meses ou se em caso de revisão em período inferior.