1. Introdução

Este documento fornece um resumo das atividades e diretrizes de Segurança da Informação e Cibernética estabelecidos na estrutura de Governança de Riscos do HSBC Brasil, instituídos por intermédio da área de Riscos de Segurança da Informação *Information Security Risk* – ISR.

O objetivo da Segurança da Informação e Cibernética é proteger a **Confidencialidade**, a **Integridade** e a **Disponibilidade** dos ativos corporativos que incluem, mas não se limitam às informações, os sistemas, os bancos de dados e a arquitetura física e lógica de Tecnologia que mantem as operações do HSBC Brasil.

O HSBC Brasil direcionará seus melhores esforços em sua capacidade para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético ao qual suas operações está inserido. E sua Administração possui compromisso com a melhoria contínua com de procedimentos e controles relacionados com Segurança da Informação e Cibernética.

Os princípios de Segurança da Informação e Cibernética estão embasados em um grupo de diretrizes que contemplam Processos, Pessoas e Tecnologias que em conjunto, fornecem subsídios para segurança e proteção dos ativos corporativos e os dados e informações de clientes, fornecedores, empregados e qualquer outra parte interessada com as operações do HSBC Brasil.

Todas as áreas do HSBC Brasil (negócio, suporte e funções de controle) são responsáveis por proteger as informações do banco e auxiliar as áreas de Segurança da Informação; Segurança Cibernética e Riscos de Segurança da Informação na identificação de incidentes de segurança reais ou suspeitos.

Os clientes, fornecedores e demais partes interessadas, são responsáveis por proteger suas informações, credenciais de acesso aos sistemas do HSBC Brasil bem como utilizar sistemas e informações de maneira adequada, sem violar qualquer controle ou medida de proteção instituída pelo HSBC Brasil na provisão de seus acessos

As diretrizes de segurança e proteção, do HSBC Brasil estão em conformidade com os requerimentos do Grupo HSBC e com a Resolução nº 4.658 do Banco Central do Brasil.

2. Políticas para os Profissionais com Acesso a Sistemas e Informações

2.1. Classificação da Informação

Todas as informações do HSBC Brasil deverão ser classificadas com base nos potenciais riscos para o banco, seus clientes e partes relacionadas, de modo a proteger a confidencialidade e a integridade das informações do HSBC Brasil.

2.2. Rótulos de Documentos Classificados

Todos os documentos, inclusive e-mails, devem ser visivelmente rotulados quando gerados ou editados de maneira a informar a classificação da informação do documento. A classificação da informação deve ser realizada por todos os profissionais que criam e/ou alteram documentos e informações no HSBC.

2.3. Mesa Limpa e Tela Limpa

Todos os profissionais do HSBC Brasil são responsáveis por garantir que informações classificadas como *Internas, Restritas e Altamente Restritas* não sejam deixadas acessíveis por pessoas não autorizadas, bem como proteger fisicamente qualquer dispositivo eletrônico que possui informações corporativas.

2.4. Uso de Equipamentos e Sistemas do HSBC

Equipamentos e sistemas do HSBC devem ser usados apenas para propósitos de negócios autorizados.

2.5. Comunicação eletrônica – Uso de Internet e e-mail

O uso dos sistemas de comunicação eletrônicos disponibilizados pelo HSBC, incluindo a Internet, Intranet, e-mail e outros sistemas de mensagens devem estar em conformidade com as diretrizes de segurança que se aplicam tanto para as mensagens quanto para os anexos.

2.6. Trabalho Remoto

O Trabalho Remoto somente poderá ser realizado quando controles suficientes estiverem implementados para gerenciar todos os riscos identificados e treinamentos específicos forem completados.

O HSBC deve garantir segurança da conexão de rede através de suas ferramentas tecnológicas e o funcionário deve garantir um local de trabalho remoto seguro para o equipamento e informação do HSBC

2.7. Controle de Acesso aos Sistemas Computacionais

O acesso aos sistemas e informações do HSBC deve ser restrito ao pessoal autorizado, controlado por senhas secretas ou outras credenciais de segurança individuais e rastreáveis. O acesso aos sistemas deve ser justificado com base nos requisitos do negócio.

2.8. Treinamento e Capacitação em Segurança da Informação

Todos os profissionais que possuem acesso às informações por meio lógico e físico devem receber treinamento sobre os assuntos relacionados à segurança da informação a fim de disseminar a cultura em Segurança da Informação e Cibernética.

2.9. Cópias de segurança (Backup) e recuperação de backup

Cópias de segurança e procedimentos de recuperação de backup devem ser implementados para garantir que os dados, sistemas e aplicativos permaneçam disponíveis e sejam restauráveis de maneira e em

tempo adequados, permitindo às operações do negócio serem restauradas pela operação de TI em casos de perda ou corrupção de dados, exclusão acidental ou intencional ou outro evento destrutivo.

2.10. Uso de Equipamentos Pessoais para Trabalhos ao HSBC

O HSBC Brasil não permite o uso de dispositivos pessoais para atividades profissionais relacionadas ao banco.

2.11. Descarte/Deleção de Informações físicas e eletrônicas

Informações classificadas como *Internas, Restritas ou Altamente Restritas* em sua forma física e eletrônica devem ser descartadas de maneira segura, após o término de seu ciclo de vida ou após não serem mais requeridas ao negócio.

Dispositivos adequados como fragmentadoras de papel ou outros dispositivos devem ser utilizados de acordo com o formato que a informação está disposta.

2.12. Proteção de Equipamentos Fora das Dependências do Banco

Todo equipamento levado para fora das dependências do banco, incluindo computadores móveis, mídias ou dispositivos de armazenamento, celulares e smartphones devem ser protegidos contra roubo ou perda.

3. Políticas Técnicas de Segurança da Informação e Cibernética

3.1. Violações de Segurança da Informação e Gestão de Incidentes

Todo profissional e outros grupos de trabalho devem reportar imediatamente qualquer violação ou suspeita de violação para seu *Line Manager*, gestor do cotnrato e para o time de Resposta a Incidentes de Segurança Cibernética e BIRO para garantir que as ações adequadas e tempestivas sejam para identificar e gerenciar qualquer risco resultante da violação e remediar qualquer problema decorrente da violação.

Os fornecedores de serviços relevantes devem comunicar o HSBC Brasil sobre os incidentes que impactem as operações do banco, ocorridos em seus respectivos ambientes para registro e acompanhamento. Detalhes sobre investigações de causas desses incidentes e impactos na operação do banco devem fazer parte das comunicações.

3.2. Registros (Logs) de Eventos de Segurança de e Monitoração

Os registros de eventos de segurança de devem ser capturados, revisados e monitorados para identificar atividades maliciosas, não autorizadas ou anormais.

A retenção dos registros de eventos de Segurança de devem ser adequada aos requerimentos previstos em lei e requisitos internos do Grupo HSBC

3.3. Configurações de Segurança – *Hardening* (Baselines)

Todos os serviços e privilégios existente em dispositivos, hardware ou software devem ser revisados e desabilitados caso não sejam requeridos. Isto é particularmente importante para dispositivos expostos à Internet. Esta política se aplica a todos os hardwares e softwares do HSBC.

3.4. Controles de Antivírus e Anti-malware

Todos os sistemas onde se aplicar, devem possuir solução de antivírus e *anti-malware* aprovada pelo grupo. Estas soluções devem ser mantidas atualizadas.

Casos de infecção de vírus e ataques de *malwares* devem ser tradados como incidentes de segurança e gerenciados adequadamente.

3.5. Certificados Digitais e Controles Criptográficos

O uso de criptografia de dados e certificados digitais deve ser considerado para mitigar riscos de exposição de dados durante armazenamento e transmissão de informações no formato eletrônico.

3.6. Criptografia de Sistemas e Chaves Criptográficas

Onde criptografia de dados está implementado, métodos de distribuição e gerenciamento de chaves criptográficas deve ser usada sempre que possível ao invés de métodos de distribuição e controle manuais.

3.7. Conectividade com a Internet

O uso de Internet deve possuir controles para proteção das informações do negócio quando adotada como plataforma de negócios.

3.8. Gestão de Vulnerabilidades

A Administração deve promover a execução tempestiva de atualizações de segurança, disponibilizada pelos fornecedores de software e hardware (firmwares), de modo a reduzir riscos de ataques ao ambiente do HSBC Brasil, bem como do Grupo HSBC por meio de exploração de vulnerabilidades conhecidas.

Procedimentos de controle e monitoração que incluem a verificação frequente do ambiente tecnológico devem ser adotados para assegurar que o parque de ativos de computador esteja dentro dos níveis de risco adequados e definidos pela Administração.

4. Desenvolvimento Seguro e Manutenção de Sistemas

Os requisitos de segurança para sistemas de TI devem ser gerenciados durante todas as etapas do desenvolvimento de sistemas.

O desenvolvimento e manutenção de sistemas e aplicativos deve ser realizado em ambiente segregado daquele utilizado para operações em produção ou teste.

Dados de produção não podem ser utilizados em ambientes de desenvolvimento e testes.