1 Política de Gerenciamento de Cibersegurança - Brasil

2 Objetivo

A política define os requisitos básicos para prevenir, detectar e responder a riscos e ameaças de cibersegurança.

O objetivo desta Política é garantir que funcionários e administradores mantenham foco adequado no nível de segurança das informações em todo o Credit Suisse Brasil, de modo a assegurar que:

- a cibersegurança tenha prioridade máxima;
- ativos de informação com classificação de segurança tenham proteção adequada;
- a segurança das informações, incluindo controles de cibersegurança, tenha governança efetiva;
- avaliações de risco de cibersegurança sejam parte integrante da estrutura de entrega de soluções.

3 Público-alvo

Esta política se aplica a todos os funcionários, estagiários e contratados do Banco de Investimentos Credit Suisse (Brasil) S.A. e suas subsidiárias (coletivamente, “Credit Suisse Brasil”).

Os requisitos para a proteção dos dados e das informações do Credit Suisse Brasil, conforme estabelecidos nesta política, também devem ser estipulados e cumpridos sempre que parceiros externos e terceiros (inclusive consultores, trabalhadores contingentes, contratados ou prestadores de serviços) prestarem serviços para o Credit Suisse Brasil, ou em seu nome.

4 Responsabilidades

O Credit Suisse Brasil e seus funcionários devem observar os seguintes princípios de cibersegurança:

- proteger o Credit Suisse contra riscos e ameaças de cibersegurança;
- compreender e cumprir obrigações legais, regulatórias e gerenciais;
- observar os princípios de segurança das informações atinentes à confidencialidade, integridade e disponibilidade das informações;
- restringir o acesso com base no princípio da "necessidade de saber" e da "necessidade de ter";
- identificar controles de segurança das informações de acordo com práticas definidas de gerenciamento de risco;
- operar controles de segurança das informações de forma padronizada;
- relatar riscos residuais e de segurança das informações.

A diretoria do Credit Suisse Brasil é responsável por:

- definir e garantir a execução da estratégia de gerenciamento de risco de segurança das informações;
- revisar normas e políticas de Tecnologia da Informação (TI) relevantes, para garantir que controles mínimos de segurança das informações sejam incorporados localmente;
- monitorar o cumprimento das políticas de segurança das informações, em parceria com o departamento de TI.

O autor é responsável pela documentação desta política, pela atualização das informações sempre que necessário e também pela sua revisão anual, para confirmação de sua validade até que seja revogada.

5 Medidas disciplinares

Violações desta política podem resultar em medida disciplinar, até (inclusive) demissão.

Violações das obrigações legais ou regulatórias poderão ser relatadas para autoridades externas e poderão resultar em penas criminais, cíveis ou regulatórias.

6 Princípios e controles de segurança da informação

Segurança das informações consiste na proteção das informações e dos sistemas de informação contra acesso, uso, divulgação, disrupção, modificação ou destruição não autorizados, a fim de garantir sua confidencialidade, integridade e disponibilidade.

Esta política apresenta os princípios que devem ser seguidos para o uso aceitável e adequado de hardware, software, sistemas, aplicativos, dados, instalações e redes de tecnologia da informação, bem como equipamentos de telecomunicações com base em exigências e objetivos de controle de segurança das informações para proteger os ativos de Tecnologia da Informação do Credit Suisse.

6.1 Classificação e gerenciamento de dados

As informações devem ser classificadas nos seguintes níveis: secretas, confidenciais, internas, irrestritas e públicas, de acordo com a confidencialidade e as proteções necessárias.

Os riscos e impactos de vazamentos de informações devem ser identificados.

Uma abordagem baseada em risco para a prevenção contra o vazamento de informações também deve ser aplicada a todas as outras informações não públicas.

Contratos e/ou outras medidas adequadas devem ser firmados para a troca, a transferência, o armazenamento ou o processamento seguros dos dados classificados como internos, ou classificação superior, entre o Credit Suisse Brasil e partes externas.

6.2 Controle de acesso

O acesso a informações deve ser restrito com base nos negócios ou nas funções que os usuários precisam desempenhar.

As contas de usuários devem ser gerenciadas de acordo com um processo definido de administração de usuários.

Um identificador único deve ser designado a cada um dos usuários.

Para tipos de contas de usuários que exigem senhas, deve-se definir regras de gerenciamento de senhas para cada tipo de conta.

Procedimentos devem ser estabelecidos para garantir a adição e a modificação tempestiva e específica dos acessos adequados às atribuições dos usuários. A desativação/exclusão de contas de usuário deve ser feita de forma tempestiva.

6.3 Gerenciamento de vulnerabilidade técnicas

Controles devem ser estabelecidos para prevenção, detecção e recuperação de ameaças, tais como:

- Remoção de componentes não utilizados e sujeitos a vulnerabilidades;
- Uso adequado e efetivo da criptografia para proteger a confidencialidade e integridade das informações;
- Procedimentos de bloqueio de instalação de software não padrão;
- Uso de software, ferramentas ou utilitários restrito apenas aos autorizados pelo Credit Suisse;
- Soluções para proteção contra malware configuradas para que monitorem continuamente os sistemas e arquivos de computador e identifiquem características da presença ou atividade de malware;
- Mecanismos para detectar acessos não autorizados a redes e serviços de rede.

6.4 Segurança das operações

Os sistemas e os aplicativos devem ser projetados para garantir que os controles de segurança das informações sejam implementados e testados e não possam ser contornados.

Os ambientes de desenvolvimento, teste e laboratório devem estar física ou logicamente separados do ambiente de produção.

Os proprietários dos sistemas devem se assegurar de que os registros de auditoria das atividades de usuários, as exceções e os eventos de segurança das informações serão produzidos pelos sistemas e retidos de forma segura por um período definido.

Cópias de *back-up* de informações e de *softwares* do ambiente produção devem ser feitas, e a eficácia dos procedimentos de restauração deve ser testada regularmente.

A segurança física também deve ser considerada para proteção dos sistemas de informação,

6.5 Treinamento e conscientização sobre segurança da informação

Os funcionários do Credit Suisse Brasil devem receber treinamento regular sobre segurança das informações e cibersegurança, conforme for adequado e relevante para as habilidades, responsabilidades e funções de cada um.

O treinamento poderá incluir:

- *eLearnings* (com avaliação ao final do conteúdo e percentual mínimo para aprovação);
- testes de simulação de *phishing*;
- conversas e palestras;
- documentos e comunicação corporativa.

Os clientes podem consultar nossas dicas de segurança on-line ao acessar os sites:

- www.cshg.com.br/seguranca
- br.credit-suisse.com/seguranca

6.6 Tratamento e controle de dados de Clientes

Todo dado de Cliente deve ser classificado como confidencial e seguir os procedimentos e controles internos adequados para esta classificação.

Deve ser considerado dado de Cliente, dados que direta ou indiretamente se referem ou divulgam dados de identificação sobre um potencial cliente, uma conta de cliente já existente ou anterior, considerando relacionamentos tanto com pessoa física ou jurídica.

6.7 Contratação de serviços relevantes prestados por Terceiros

Devem ser realizadas avaliações de riscos para contratação de Terceiros que prestam serviço relevantes. E isto, inclui a revisão de seus controles de segurança, incluindo governança de risco, compliance e a capacidade para prover continuidade de seus serviços. E é esperado que os controles de segurança da informação sejam consistentes com os requisitos e políticas do Credit Suisse.

De acordo com o risco, o Terceiro também pode ser submetido à avaliações de outros departamentos do Credit Suisse, conforme aplicável.

7 Tratamento de incidentes de segurança da informação

Os incidentes de Segurança da Informação devem ser reportados e, quando necessário, escalados a alta gerência de forma tempestiva.

Um incidente deve ser acompanhado e monitorado durante todo o seu ciclo de vida por meio do registro de eventuais alterações em seu status ou prioridade e deve ser processado de acordo com os marcos estabelecidos no ciclo de vida do processo.

Medidas devem ser tomadas para evitar que incidentes de segurança se espalhem, para proteger o Banco contra futuras exposições a incidentes similares e para verificar a propagação de incidentes.

As medidas de resolução e recuperação fazem parte do registro do incidente e devem ser documentadas.

O departamento Jurídico deve ser informado sobre o gerenciamento de incidentes de segurança que infrinja efetiva ou potencialmente as leis e/ou os regulamentos locais; e deverá estar diretamente envolvido nos casos em que o relato de problemas de segurança for uma exigência legal ou regulatória.

O Credit Suisse compartilha incidentes relevantes com as demais instituições financeiras de forma segura e correta por meio do *Financial Services Information Sharing and Analysis Center* (FS-ISAC), consórcio setorial dedicado a reduzir o risco cibernético no sistema financeiro global.

O Credit Suisse possui um processo de resposta a incidente estabelecido, que inclui reporte e escalonamento para comitês e áreas devidas. Quando necessário, a informação é escalonada aos reguladores, auto reguladores e clientes impactados.

8 Glossário

CS – Credit Suisse Brasil.

Disponibilidade – Garantia de acesso a informações e seu uso de maneira tempestiva e confiável.

Confidencialidade – Preservação das restrições autorizadas sobre o acesso a informações e sua divulgação, incluindo os meios para proteger a privacidade individual e as informações exclusivas.

Cibersegurança – O processo que consiste em proteger informações pela prevenção, detecção e resposta a ataques.

Segurança das informações – No contexto do Credit Suisse, segurança das informações, que inclui cibersegurança, consiste na preservação das seguintes propriedades das informações:

- Confidencialidade;
- Integridade;
- Disponibilidade.

Incidentes de segurança – Violação ou ameaça iminente de violação de políticas de segurança digital, políticas de uso aceitável ou práticas de segurança comuns.

Integridade – Proteção contra modificação ou destruição inapropriada de informações, o que inclui garantir o não repúdio e a autenticidade das informações.

Malware – Código malicioso que causa danos ou permite a subversão de sistemas. Exemplos tradicionais de códigos maliciosos incluem vírus, worms, Cavalos de Tróia e scripts de ataque; e os exemplos mais recentes incluem applets maliciosos em Java e controles ActiveX.