Política de Segurança Cibernética

State Street Brasil S.A Banco Comercial

Agosto/2024

Declaração da Política

A política de Cibersegurança Global (GCS) da State Street centra-se nos três objetivos para proteger a tecnologia e os ativos de dados contra ameaças e vulnerabilidades de segurança: Confidencialidade, Integridade e Disponibilidade.

Escopo

Esta política abrange todas as informações e dados residentes em todas as plataformas e sistemas de processamento de dados de propriedade, alugados ou gerenciados pela State Street Brasil ou por provedores terceirizados.

Framework de Segurança Cibernética

Esta política está alinhada à estrutura do *National Institute of Standards and Technology (NIST)* (Versão 1.1), que estabelece cinco "funções" principais para organizações de segurança cibernética: Identificar, Proteger, Detectar, Responder, Recuperar.

Os objetivos estratégicos para cada função são delineados nesta política e apoiados pelas Normas GCS que estabelecem diretrizes mínimas detalhadas para desempenho operacional, sistemas de gerenciamento, mitigação de riscos e prestação de serviços.

As categorias do NIST por função são:

Identificar: essa função auxilia o banco a entender seus riscos de segurança cibernética, identificando seus ativos, ambiente de negócios e requisitos legais. Ela também suporta o desenvolvimento de uma estratégia de gerenciamento de riscos.

Proteger: essa função se concentra na implementação de medidas de proteção para prevenir ataques cibernéticos. Ela cobre, entre outros assuntos, o controle de acesso, o treinamento de conscientização da equipe e a segurança de dados.

Detectar: trata de atividades para identificar eventos de segurança cibernética. O objetivo é detectar esses eventos o mais rápido possível.

Responder: essa função se concentra em tomar medidas após a detecção de um evento de segurança cibernética. O objetivo é limitar os danos causados pelo evento.

Recuperar: essa função se concentra em retornar às operações normais após um evento de segurança cibernética. O objetivo é restaurar sistemas e capacidades o mais rápido possível.

Funções e Categorias da Estrutura de Segurança Cibernética (NIST)				
Identificar	**Proteger**	**Detectar**	**Responder**	**Recuperar**
✓ Gestão de Ativos ✓ Ambiente de Negócios ✓ Governança ✓ Avaliação de Risco ✓ Estratégia de Gestão de Riscos ✓ Gestão de Riscos da Cadeia de Suprimentos	✓ Gerenciamento de Identidades e Controle de Acesso ✓ Conscientização e Treinamento ✓ Segurança de Dados ✓ Processos e Procedimentos de Proteção de Informações ✓ Manutenção ✓ Tecnologia de Proteção	✓ Anomalias e Eventos ✓ Monitoramento Contínuo de Segurança ✓ Processos de Detecção	✓ Planejamento de Resposta ✓ Comunicações ✓ Análise ✓ Mitigação ✓ Melhorias	✓ Planejamento de Recuperação ✓ Melhorias ✓ Comunicações

Conscientização e Educação em Segurança Cibernética

O State Street Brasil mantem um portal dedicado à segurança cibernética, contendo informações e orientações sobre:

- Prevenção de fraudes e golpes
- Boas práticas de segurança
- Utilização segura dos canais de atendimento

A instituição também promove campanhas de conscientização e disponibiliza outros materiais educativos para reforçar a importância da segurança cibernética e auxiliar clientes e usuários na proteção de seus dados e transações.