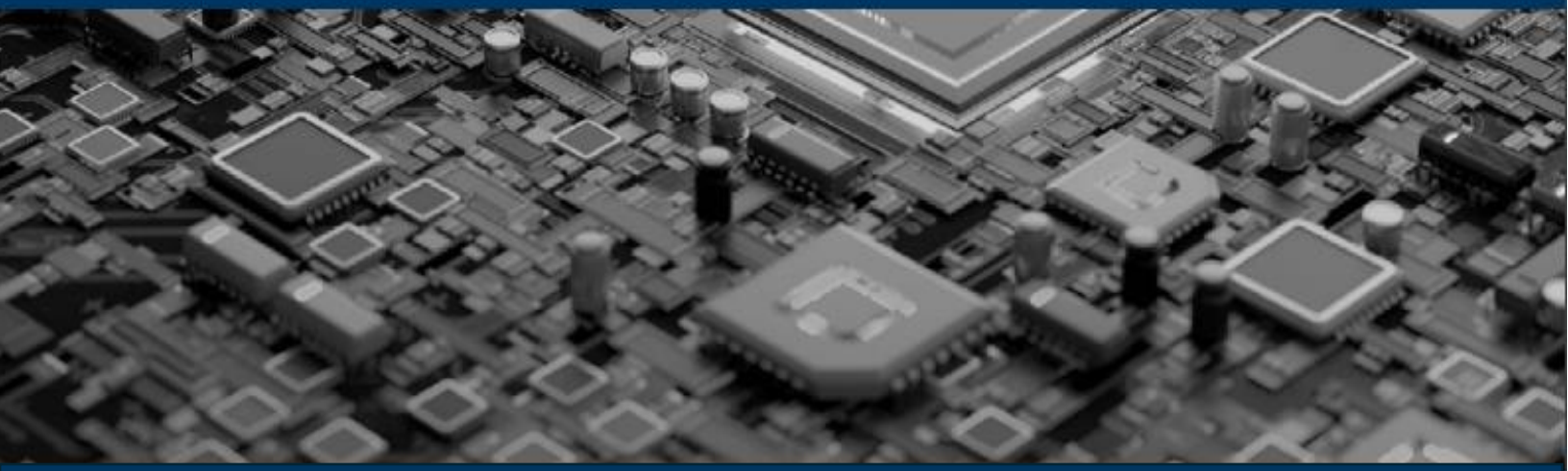
Goldman Sachs



GOLDMAN SACHS DO BRASIL BANCO MÚLTIPLO S.A.

GUIA DE SEGURANÇA CIBERNÉTICA

Versão 11.0
Março 2025

Índice

Introdução

A Goldman Sachs atribui grande importância à segurança da informação, incluindo a segurança cibernética, para se proteger contra ameaças externas e internos maliciosos. A estratégia de segurança cibernética da Firma prioriza a detecção, análise e resposta a situações de ameaça cibernética conhecidas, antecipadas ou inesperadas, gestão eficaz dos riscos cibernéticos e resiliência contra incidentes cibernéticos. A Firma se esforça continuamente para atender ou exceder as melhores práticas de segurança da informação do setor e aplicamos controles para proteger nossos clientes e a Firma. A Goldman Sachs mantém um programa formal de segurança cibernética estruturado em torno da Estrutura de Segurança Cibernética ("CSF") do National Institute of Standards and Technology ("NIST") e o respectivo Perfil de Segurança Cibernética

Este documento proporciona uma visão geral da abordagem da Firma em relação à segurança da informação e à segurança cibernética, e suas práticas para proteger dados, sistemas e serviços, que se alinham às cinco funções do NIST CSF: Identificar, Proteger, Detectar, Responder e Recuperar.

Embora as medidas de segurança da informação e segurança cibernética mudem naturalmente com o tempo e possam diferir entre a gama de serviços da Goldman Sachs, este documento fornece uma visão geral das nossas práticas de segurança. A Goldman Sachs não declara que este documento será apropriado ou adequado para os fins pretendidos.

Entre em contato com seu representante da Goldman Sachs se tiver dúvidas adicionais.

Governar

Governança e Supervisão de Riscos

Estrutura da Governança de Riscos

A Firma estabeleceu uma estrutura de gestão de risco empresarial que emprega uma abordagem abrangente e integrada à gestão de risco e foi projetada para permitir processos abrangentes de gestão de risco através dos quais os riscos são identificados, avaliados, monitorados e gerenciados. A estrutura de gestão de risco da Firma é construída em torno de três componentes principais: governança, processos e pessoas.

As unidades geradoras de receita da Firma, bem como Tesouraria, Engenharia, Gestão de Capital Humano, Operações e Soluções Corporativas e de Local de Trabalho, são consideradas a primeira linha de defesa. Eles são responsáveis pelos resultados das atividades geradoras de risco da Firma, bem como por avaliar e gerenciar esses riscos dentro do apetite de risco da Firma.

As funções de supervisão e controle de risco independentes da Firma são consideradas a segunda linha de defesa e fornecem avaliação, supervisão e desafio independentes dos riscos assumidos pela primeira linha de defesa, bem como lidera e participa de comitês de risco. As funções de supervisão e controle de riscos independentes incluem as Divisões de Risco e Compliance.

A Auditoria Interna é considerada a terceira linha de defesa, e o diretor de Auditoria Interna reporta ao Comitê de Auditoria do Conselho e administrativamente ao Diretor Executivo. A auditoria interna inclui profissionais com uma ampla gama de experiência em auditoria e no setor bancário, incluindo experiência em gestão de riscos. A Auditoria Interna é responsável por avaliar e validar de forma independente a eficácia dos principais controles, incluindo aqueles dentro da estrutura de gestão de risco, e fornecer relatórios oportunos ao Comitê de Auditoria do Conselho, à gerência sênior e aos reguladores.

As três linhas de estrutura de defesa promovem a responsabilidade dos responsáveis pelo risco de primeira linha, fornecem uma estrutura para o desafio eficaz da segunda linha e capacitam a revisão independente da terceira linha.

Cada uma das divisões da Firma é responsável por gerenciar os riscos tecnológicos que afetam seus aplicativos e outros ativos do sistema de informação.

Comitês de Governança

Em adição à estrutura da governança de riscos, a firma possui uma série de comitês que

supervisionam a implementação da estratégia e estrutura de gestão de risco de segurança cibernética. Esses comitês são informados sobre incidentes e riscos de segurança cibernética por membros designados do Risco de Tecnologia e Risco Operacional, que periodicamente reportam a esses comitês sobre o Programa. Esses comitês permitem o escalonamento formal e o reporte de riscos, apresentados pelo CISO e pela liderança de Risco de Tecnologia.

A seguir estão os comitês principais e grupos diretivos que supervisionam o Programa:

- O Comitê Global de Risco Operacional e Resiliência ‘’Firmwide Operational Risk and Resilience Committee” (FORRC) é globalmente responsável por supervisionar os riscos operacionais e busca garantir a resiliência comercial e operacional da Firma. Este comitê é copresidido pelo diretor administrativo da empresa para a EMEA e pelo chefe de risco operacional.

- O Comitê Global de Risco de Tecnologia ‘’Firmwide Technology Risk Committee” (FTRC) analisa questões relacionadas ao *design*, desenvolvimento, implantação e uso de tecnologia da informação. Este comitê supervisiona questões de segurança cibernética, bem como estruturas e metodologias de gestão de risco de tecnologia da informação, e monitora sua eficácia. Este Comitê é copresidido pelo diretor de segurança da informação e pelo diretor de tecnologia da Firma.

- Grupo de Direção (*Steering Group*) do Escritório de Risco Digital "*Digital Risk Office*”(DRO) é um grupo subordinado sob o FTRC, com o mandato de supervisionar os riscos de Engenharia. O DRO fornece supervisão estratégica e direção do portfólio de Risco de Tecnologia e agiliza o escalonamento e as decisões enquanto compartilha informações entre os pilares sobre as principais iniciativas. Este grupo é copresidido pelo diretor de segurança da informação (CISO) e pelo diretor de tecnologia da Firma (CTO).

Programa de Segurança Cibernética e Segurança da Informação

Os processos de gestão de risco de segurança cibernética da Firma são integrados aos processos gerais de gestão de risco. A Firma estabeleceu um Programa de Segurança da Informação e Segurança Cibernética (“Programa”), administrado pelo Risco de Tecnologia dentro da Engenharia e supervisionado pelo CISO. O Programa foi desenvolvido para identificar, avaliar, documentar e mitigar ameaças, estabelecer e avaliar a conformidade com as exigências de segurança da informação, adotar e aplicar a estrutura de controle de segurança e prevenir, detectar e responder a incidentes de segurança. O Programa é revisado e modificado periodicamente para responder às mudanças de ameaças e condições.

Uma equipe de Risco Operacional dedicada, que se reporta ao CRO, fornece supervisão e consequente contestação do Programa, independentemente do Risco de Tecnologia, e avalia a eficácia operacional do Programa em relação às estruturas padrão do setor e limites de apetite de risco operacional aprovados pelo Conselho (*Board*). O processo da Firma para gerenciar riscos de segurança cibernética inclui os componentes críticos da estrutura de gestão de riscos, bem como o seguinte:

- Treinamento e educação, para permitir que os funcionários reconheçam as preocupações com informações e segurança cibernética e respondam de acordo;

- Gestão de identidade e acesso, incluindo gestão de direitos e acesso à produção;

- Segurança de aplicativos e software, incluindo gerenciamento de alterações de software, software de código aberto e backup e restauração;

- Segurança de infraestrutura, incluindo o monitoramento da rede quanto a vulnerabilidades conhecidas e sinais de tentativas não autorizadas de acessar dados e sistemas da Firma;

- Segurança de dispositivos móveis, incluindo seus aplicativos;

- Segurança de dados, incluindo criptografia e descodificação, segurança de banco de dados, exclusão de dados e descarte de mídia;

- Computação em nuvem, incluindo governança e segurança de aplicativos em nuvem e integração de dados de software como serviço;

- Operações de tecnologia, incluindo gestão de mudanças, gestão de incidentes, capacidade e resiliência; e

- Gestão de risco de terceiros, incluindo gestão e governança de fornecedores, segurança cibernética e resiliência de negócios nas avaliações de fornecedores.

Auditoria Interna

A divisão de Auditoria Interna da Firma é uma função independente que reporta ao Comitê de Auditoria do Conselho de Administração da Firma. A Auditoria Interna avalia de forma independente o ambiente de controle geral da Firma e aumenta a conscientização sobre os riscos de controle. A Auditoria Interna também comunica e relata a eficácia da governança, gestão de risco e controles da Firma que mitigam os riscos atuais e em evolução, enquanto monitora a implementação das medidas de controle da gestão.

Supervisão Regulatória e Auditoria Externa

A Goldman Sachs é regulada por diversas autoridades em todas as jurisdições em que operamos, incluindo (mas não limitado a):

• Americas: o Federal Reserve System dos EUA, o New York State Department of Financial Services (Departamento de Serviços Financeiros do Estado de Nova York), a Commodity Futures Trading Commission (Comissão de Negociação de Futuros de Commodities) dos EUA, a Securities and Exchange Commission dos EUA, o Consumer Financial Protection Bureau (Departamento de Proteção Financeira ao Consumidor) dos EUA,

• Europa, Oriente Médio e África (EMEA): o European Central Bank, a Autoridade Bancária Europeia, a Financial Conduct Authority (Autoridade de Conduta Financeira) do Reino Unido e a Autoridade Federal de Supervisão Financeira da Alemanha (BaFin), a Saudi Arabian Capital Markets Authority (Autoridade de Mercado de Capitais da Arábia Saudita), o South African Reserve Bank (Banco de Reserva da sul-Africano), o U.A.E. Securities and Commodities Authority (Autoridade de Valores Mobiliários e Commodities dos Emirados Árabes Unidos).

• Ásia-Pacífico: The Monetary Authority of Singapore (Autoridade Monetária de Singapura), the Japan Financial Services Agency (Agência de Serviços Financeiros do Japão), the Australian Securities and Investments Commission (Comissão de Valores Mobiliários e Investimentos Australianos), and the Hong Kong Monetary Authority (Autoridade Monetária de Hong Kong).

A PricewaterhouseCoopers LLP (PwC) é a empresa de auditoria externa responsável e realiza as avaliações de Controle de Organização de Serviços (SOC) 1 e 2 para negócios selecionados da Firma e testa independentemente controle aplicados .

Envolvimento no Setor

A Goldman Sachs é fundadora ou participante líder em muitas iniciativas importantes do setor, tanto em âmbito nacional como internacional. Nos Estados Unidos, essas parcerias incluem o Financial Services Sector Coordinating Council (Conselho de Coordenação do

Setor de Serviços Financeiros) (FSSCC), o Financial Services - Information Sharing and Analysis Center (Centro de Compartilhamento e Análise de Informações de Serviços Financeiros) (FS-ISAC), o Analysis and Resilience Center (ARC) for Systemic Risk (Centro de Análise e Resiliência de Risco Sistêmico), e a iniciativa “Sheltered Harbor”.

A Goldman sachs mantém relacionamentos diretos com entidades governamentais em todo o mundo. Nos Estados Unidos, a Firma colabora ativamente com o Federal Bureau of Investigations (FBI), o Departamento de Segurança Nacional (DHS) e a Agência de Segurança Cibernética e de Infraestrutura (CISA). A Firma também mantém parcerias internacionais, como a Cyber Security Information Sharing Partnership (CiSP – Reino Unido) e a Computer Emergency Response Team (CERT – Índia).

Além disso, a Goldman Sachs participa de esforços do setor para controlar os riscos tecnológicos, inclusive conforme coordenados pela Securities Industry and Financial Markets Association (Associação do Setor de Valores Mobiliários e Mercados Financeiros) (SIFMA), a Asia Securities Industry and Financial Market Authority (Autoridade do Setor de Valores Mobiliários e Mercado Financeiro da Ásia) (ASIFMA), a Association for Financial Markets in Europe (Associação de Mercados Financeiros da Europa) (AFME), o Bank Policy Institute (Instituto de Política Bancária) (BPI), a American Bankers Association (Associação de Bancos dos EUA) (ABA) e Australian Financial Markets Association (AFMA).

Políticas e Normas de Segurança da Informação e Segurança Cibernética

A Firma mantém políticas e padrões de segurança da informação e segurança cibernética que levam em consideração a segurança da informação e segurança cibernética, leis e regulamentos de privacidade de dados que são aplicáveis às jurisdições em que a Firma opera.

As políticas e normas são revisadas e aprovadas por órgãos de governança relevantes em toda a Firma. O Programa e a Política Global de Segurança da Informação e Segurança Cibernética da Firma são revisados anualmente. Outras políticas e normas da Firma são revisadas pelo menos a cada três anos, de acordo com os requisitos de revisão periódica da Firma. Análises adicionais podem ser desencadeadas por mudanças no ambiente de risco ou no cenário regulatório.

Um grupo dedicado de governança de políticas, composto por representantes de cada uma das divisões da Firma, mantém o processo para desenvolver, revisar, atualizar e desativar políticas e normas de segurança da informação e segurança cibernética.

As políticas e normas da Firma são baseadas em padrões reconhecidos do setor, incluindo aqueles definidos pelo Instituto Nacional de Padrões e Tecnologia (National

Institute of Standards and Technology, NIST), pelo Conselho Federal de Exame de Instituições Financeiras (Federal Financial Institutions Examination Council, FFIEC) e pelo Instituto de Risco Cibernético.

As políticas e normas da Firma estão disponíveis para os funcionários por meio de um compêndio interno.

Identificar

Avaliações de Risco

Avaliações de Risco

A Goldman Sachs acredita que a identificação de riscos e avaliações de controle relacionados é uma etapa crítica para fornecer ao Conselho e à gerência sênior transparência e percepção da gama e materialidade dos riscos enfrentados pela Firma. A Goldman Sachs possui um processo abrangente de coleta de dados, incluindo políticas e procedimentos em toda a Firma que exigem que os funcionáriosrelatem e encaminhem eventos de risco. A abordagem da Firma para identificação de risco e avaliação de controle é abrangente em todos os tipos de risco, é dinâmica e progressiva (forward-looking) para refletir e se adaptar ao perfil de risco em mudança e ao ambiente de negócios, aproveita a experiência no assunto e permite a priorização dos riscos mais críticos. Essa abordagem também abrange a avaliação de controle, liderada pela segunda linha de defesa, para analisar e desafiar o ambiente de controle e ajudar a garantir que ele apoie o plano estratégico de negócios da Firma.

A Firma realiza avaliações de risco para avaliar o desempenho do Programa de Segurança da Informação e Segurança Cibernética, para estimar o perfil de risco da Firma e para avaliar a conformidade com os requisitos regulatórios relevantes. A Goldman Sachs realiza avaliações periódicas de eficácia de controle por meio do processo de autoavaliação de controle e risco interno, bem como uma variedade de avaliações técnicas externas, incluindo testes de penetração externos e compromissos de “red team”, onde terceiros testam as defesas da Firma. Os resultados dessas avaliações de risco, juntamente com as descobertas de desempenho de controle, são usados para estabelecer prioridades, alocar recursos e identificar e melhorar controles.

Gestão de Ativos

Gestão de Ativos Tecnológicos

A Goldman Sachs mantém informações de ativos para hardware em inventários

gerenciados durante todo o seu ciclo de vida; esses inventários são usados para rastrear os atributos de cada ativo. A gestão de inventário compreende processos e controles manuais, incluindo o processo de integração do ativo, revisões periódicas e é regida por políticas e normas.

Ativos, que podem incluir hardware, software ou ativos virtuais, como máquinas virtuais, recebem responsáveis para auxiliar na governança. Os aplicativos da firma incluem classificações baseadas em seus riscos inerentes.

Proteger

Treinamento e Conscientização

Treinamento e Educação

A Goldman Sachs mantém um programa de treinamento em Segurança Cibernética para ajudar os funcionários a reconhecer as preocupações com informações e segurança cibernética e responder adequadamente. Este programa, em particular, proporciona aos funcionários conhecimentos e habilidades para impedir, identificar e escalonar riscos de segurança cibernética.

O treinamento em segurança da informação e privacidade é obrigatório para todo o pessoal da Goldman Sachs anualmente, incluindo os funcionários em período integral ou parcial, e terceirizados. Um treinamento adicional é fornecido para novos associados e pessoas que são transferidas dentro da Firma.

A Goldman Sachs realiza testes de phishing regularmente junto aos funcionários para avaliar seu conhecimento sobre ameaças cibernéticas em e-mails e o escalonamento adequado.

A Goldman Sachs incorpora tópicos de treinamento com base em diretrizes regulatórias, melhores práticas do setor e mudanças no ambiente de risco. Além disso, a firma oferece treinamento técnico para os funcionários de engenharia por meio de plataformas especializadas. Este treinamento inclui tópicos de segurança da informação, tais como, codificação segura, e princípios e atualizações de ameaças emergentes. A firma mantém processos para rastrear, mensurar e escalonar os funcionários que não participam de treinamentos, inclusive sobre segurança cibernética.

Gestão de Identidade e Acesso

Gestão de Identidade de Usuários

Os controles de acesso da Firma baseiam-se nos princípios gerais de nenhum privilégio

sem identidade, nenhum privilégio sem aprovação e acesso com privilégio mínimo. As autorizações são, portanto, apenas provisionadas quando proporcionais à função ou às funções do trabalho.

A Goldman Sachs verifica os antecedentes de funcionários, consultores e terceirizados. A identidade de um funcionário é posteriormente verificada no início do contrato de trabalho por meio de processos padrão de recursos humanos. Ao ingressar na Goldman Sachs, os funcionários assinam um acordo de não divulgação o qual exige que eles respeitem as políticas de proteção de informações dos clientes da Firma.

Um identificador único é atribuído a cada funcionário. Os funcionários estão proibidos de compartilhar suas informações de credenciais individuais, incluindo nomes de usuário e senhas.

Gestão de Permissões (Entitlements)

Autenticação e autorização são necessárias para aplicativos de alto risco. Os direitos associados a aplicativos críticos e sensíveis devem ser revisados pela gerência pelo menos anualmente. Podem ocorrer revisões mais frequentes para acesso privilegiado. Os direitos também podem ser revogados e/ou revisados quando o pessoal for transferido para novas funções ou departamentos dentro da Firma.

A Firma mantém um programa de segregação de funções como parte de sua estrutura de controle interno. A segregação de funções exige que o mesmo indivíduo não esteja em posição de iniciar, aprovar e reconciliar a mesma transação ou processo crítico. Um sistema automatizado é usado para monitorar as lojas de direitos e identificar violações nos requisitos de segregação de tarefas.

Quando um trabalhador deixa a Firma, o acesso às instalações da Firma e o acesso geral aos sistemas de informação são revogados.

Gestão de Acesso

A Goldman Sachs possui exigências de senha definidas e documentadas em uma norma formal. As exigências de senha incluem o estabelecimento de uma nova senha no login inicial, comprimento mínimo da senha, composição alfanumérica, expiração após um período definido, número máximo de tentativas de login sem sucesso antes do bloqueio, um histórico de senhas e um bloqueio por inatividade.

Quando necessário, a segregação de dados é realizada por meio de segregação lógica com controles de acesso em nível de dados. O acesso administrativo a sistemas que armazenam dados de clientes deve ser aprovado por gerentes autorizados.

A Firma mantém controles rígidos sobre o acesso aos ambientes de produção, incluindo autorizações de acesso, registro e limites de tempo de acesso. Como parte da segregação de funções da Firma, o acesso do pessoal tecnológico aos sistemas de produção requer pré-aprovação antes de o acesso ser concedido. Além disso, o acesso à produção é limitado a indivíduos autorizados, com prazo determinado, sujeito a

registro e revisão periódica, limitado às funções necessárias e monitorado regularmente, incluindo registro de pressionamento de teclas. As alterações feitas nos ambientes de produção estão sujeitas a revisões obrigatórias.

A autenticação multifator (MFA) é necessária para qualquer acesso aos sistemas da Goldman Sachs fora da rede da Firma.

Segurança de Aplicativos e Software

Inventário Centralizado e Classificação de Risco

A Goldman Sachs utiliza um inventário centralizado para registrar as principais informações sobre os aplicativos. Cada aplicativo deverá completar um perfil de risco para determinar as exigências regulatórias e com base no risco. Assim, cada aplicativo recebe uma ou mais classificações de risco, as quais, por sua vez, são associadas aos controles e limites de resiliência específicos exigidos.

As classificações de risco deverão ser analisadas e atualizadas para cada aplicativo anualmente. Os riscos identificados nas avaliações anuais e trimestrais são registrados em inventários centralizados que detalham as principais informações sobre os aplicativos.

Software Development Controls

A Goldman Sachs possui um processo formal de Ciclo de Vida de Desenvolvimento de Software de Segurança (SSDLC), que é documentado e incorpora os portões de controle apropriados. Os requisitos de segurança de aplicativos e as avaliações associadas são incorporados em todo o SSDLC de forma ajustada ao risco. Exemplos de SSDLC e controles de segurança de aplicativos relacionados incluem revisões de projeto, revisões de código, teste de penetração e uso de scanners de teste dinâmico de segurança de aplicativos (DAST). Controles preventivos e detectivos fazem uso de testes de segurança de aplicativos estáticos (SAST), identificação de dependências vulneráveis e varredura de infraestrutura como código.

Os procedimentos da firma exigem que as alterações de produção sejam submetidas a testes e recebam aprovações autorizadas.

Várias aplicações em uso em toda a firma são desenvolvidas internamente. Padrões de segurança de aplicativos comparáveis são aplicados a aplicativos desenvolvidos internamente, componentes de software de código aberto e software de terceiros implantados na infraestrutura da Firma.

A política da firma estabelece que os dados confidenciais devem ser mascarados ou sujeitos a outros controles equivalentes antes de serem usados em ambientes de não produção. Os controles são implementados com base no perfil de risco do aplicativo, em conformidade com os requisitos legais, regulatórios ou contratuais de proteção de dados.

Testes de Segurança

A Goldman Sachs realiza anualmente testes de penetração, red team, equipe ofensiva defensiva conjunta (comumente chamada de “purple team”) e avaliações de equipe de caça para descobrir e avaliar a segurança de aplicações e infraestrutura, com foco em temas e riscos de alta prioridade.

Os aplicativos voltados para a Internet são verificados continuamente usando ferramentas DAST. A Firma mantém um programa de Bug Bounty e de divulgação responsável, cobrindo a maioria dos sites públicos do Goldman Sachs, que permite aos pesquisadores relatar vulnerabilidades por meio de um portal dedicado.

A metodologia de testes de penetração utilizada pela Goldman Sachs internamente e pelos seus fornecedores é baseada em diversas diretrizes do setor, como o Guia de Implementação do CREST STAR/CBEST, NIST SP800-115 e o Guia de Testes de Open Web Application Security Project (OWASP). A abordagem combina técnicas de avaliação manual e automatizada e o uso de ferramentas de avaliação proprietárias, comerciais e de código aberto em um processo consistente e que pode ser repetido.

Segurança da Infraestrutura

Gestão de Mudanças

A firma possui processos de gestão de mudanças para proteger a integridade e a disponibilidade dos produtos e serviços de tecnologia da Firma, minimizar incidentes relacionados a mudanças e melhorar as práticas operacionais.

As mudanças na infraestrutura de produção são gerenciadas usando sistemas de gestão de mudanças aprovados pela Firma e registradas. As alterações devem ser submetidas a avaliações de risco, testadas em ambientes de não produção e verificadas antes da aplicação de alterações aos sistemas de produção. Os resultados dos testes também devem ser registrados.

As normas da firma exigem que as alterações sejam registradas e autorizadas pelos aprovadores designados antes da implantação no ambiente de produção.

Implementações de mudanças devem ser verificadas para garantir que apenas as alterações pretendidas tenham sido feitas. Os resultados da verificação da mudança devem ser documentados e retidos em sistemas de gestão de mudanças autorizados pela Firma, de acordo com a política de retenção da Goldman Sachs.

Robustecimento e Gerenciamento da Configuração

A Goldman Sachs emprega gerenciamento de configuração para validar, do ponto de vista da segurança, que os sistemas da Firma continuam a funcionar de forma consistente conforme requerido pelo Programa..

Todos os sistemas são fortalecidos com base no risco ajustado para atender ou exceder os padrões do setor e são implementados utilizando práticas de segurança padrão, como restringir permissões de acesso a arquivos e o devido registro dos acessos.

Os discos rígidos em laptops fornecidos pela Goldman Sachs, os quais são usados somente para um pequeno número de finalidades de negócio específicas, são criptografados utilizando-se ferramentas padrão do setor.

Um bloqueio de tela por inatividade é imposto por uma política de configuração em todos os dispositivos.

Segurança de Rede

O ambiente de rede da Goldman Sachs foi criado para enfatizar a segurança e a resiliência, inclusive, através da implementação de múltiplas zonas de rede separadas por firewalls e outros controles. Intrusion Detection Systems (Sistemas de Detecção de Invasão -IDS) e Intrusion Prevention Systems (Sistemas de Prevenção de Invasão -IPS) são implementados no perímetro da rede para monitorar e bloquear atividades mal-intencionadas.

As interfaces de gerenciamento dos firewalls de perímetro, roteadores e outros dispositivos não podem ser acessados pela Internet. A Goldman Sachs assina serviços contínuos de monitoramento e mitigação de Distributed Denial of Service (Ataque Distribuído de Negação de Serviços) (DDoS) de vários provedores de serviços. Além disso, a Firma hospeda sua principal presença na Internet em Redes de Fornecimento de Conteúdo (CDN) com capacidade de mitigação e absorção de DDoS, que implementa a restrição de solicitações de rede para limitar o número de referências e solicitações feitas por endereços IP de clientes. Os alertas gerados pelas atividades de DDoS são monitorados e evitados conforme a necessidade.

O acesso sem fio à infraestrutura da Goldman Sachs somente é permitido a partir de dispositivos aprovados pela Firma, por meio de padrões de acesso à rede, como VPN (Virtual Private Network).

Monitoramento de Sistema e Gestão de Vulnerabilidade

A Goldman Sachs mantém um programa de gestão de capacidade, que estabelece um processo documentado para definir objetivos, escopo e requisitos de capacidade para serviços comerciais essenciais e dependências relacionadas.

A Firma possui um programa de gestão de vulnerabilidade abrangente, que inclui varreduras de vulnerabilidade frequentes dos ambientes de rede internos e externos utilizando uma varredura padrão do setor. A Goldman Sachs também contrata terceiros para analisar sua infraestrutura externa e fornecer resultados regularmente. As vulnerabilidades são resolvidas de forma ajustada ao risco, conforme estabelecido em uma norma formal.

A Firma possui um processo de tratamento definido para vulnerabilidades descobertas.

Cada vulnerabilidade recebe uma classificação de criticidade baseada em processos padrão do setor e alinhada com um plano de remediação. Os prazos para aplicação de patches nos sistemas são documentados em uma norma formal. Nos casos em que é identificada uma vulnerabilidade para a qual ainda não há patch disponível, a Firma avalia a adoção de controles compensatórios apropriados para minimizar a probabilidade de acesso não autorizado.

Solução de Desktop Virtual

A Goldman Sachs usa uma Infraestrutura de Desktop Virtual para desktops. Sob esse modelo, todos os usuários usam um dispositivo thin client para acessar seu desktop virtual hospedado em um centro de dados da GS.

O acesso remoto é fornecido através de uma conexão segura com um desktop virtual do usuário, por meio de uma autenticação multifatorial.

A infraestrutura virtualizada da Goldman Sachs é desenvolvida para oferecer um nível de controle equivalente àquele da infraestrutura local da Firma, independentemente da localização geográfica do acesso.

Os modelos de computação de desktop não virtual são conduzidos excepcionalmente, quando exigido pelas funções de negócios.

Segurança de Dispositivo de Usuário Final

Acesso Remoto Seguro para Funcionários

Os funcionários têm permissão para usar dispositivos corporativos emitidos ou seus dispositivos pessoais, BYOD (Bring Your Own Device) ao trabalhar remotamente para acessar com segurança os recursos da Firma.

A firma utiliza a proteção contra perda de dados (DLP) do gerenciamento de dispositivos móveis e outros controles de segurança para garantir que os dados permaneçam seguros em dispositivos móveis fornecidos pela Firma.

Além disso, a firma emprega uma estratégia de gerenciamento de aplicativos móveis (MAM) e defesa contra ameaças móveis (MTD) para BYOD. Esses controles de segurança MAM são projetados para proteger os dados dentro de um contêiner seguro. As informações da firma podem ser acessadas apenas por dispositivos pessoais devidamente corrigidos e seguros.

Os aplicativos móveis aprovados pela firma permitem que o pessoal envie e receba e-mails com segurança e acesse sites e documentos internos. Um conjunto limitado de aplicativos de terceiros permite que o pessoal realize atividades analíticas e/ou relacionadas aos negócios somente se esses aplicativos atenderem aos critérios de segurança da firma.

Os aplicativos móveis usados pela Firma geralmente utilizam uma variedade de recursos

de segurança, incluindo defesa contra ameaças móveis, lista de permissões de dispositivos, conexões de rede seguras, autenticação multifatorial, sandboxing, criptografia, registro de dispositivo necessário, patching de sistema operacional (SO) necessário, verificação de SO não desbloqueado ou enraizado e limpeza remota de dados.

O pessoal pode receber um dispositivo da Firma para fins comerciais específicos. Todos os dados em dispositivos fornecidos pela Firma são criptografados em repouso e em trânsito para acesso remoto e computação móvel.

Aplicativos Móveis de Cliente

A Goldman Sachs desenvolveu aplicativos móveis para que os clientes acessem as informações de dados de seu portfólio e às notícias do mercado e comuniquem-se de forma segura com os funcionários da Goldman Sachs. Os aplicativos móveis de cliente empregam controles de segurança adicionais padrão do setor, incluindo autenticação multifatorial (MFA), autenticação biométrica, e criptografia de dados em repouso e em trânsito.

Proteção de Dados

Governança de Dados

A firma possui uma estrutura de governança de dados que define como os dados da Firma e do cliente são regidos, incluindo como os dados são controlados quanto à qualidade no ponto de origem, agregação e publicação. A estrutura atribui responsabilidade pela qualidade dos dados e fornece a estrutura necessária para garantir que os dados sejam gerenciados adequadamente como um ativo.

Proteção contra Perda de Dados

Os controles de Data Loss Prevention (Prevenção de Perda de Dados - DLP) são projetados e implementados para evitar a saída de conteúdo da Firma que não se destine ao uso e distribuição externa. Tais controles incluem alertas proativos que notificam um remetente se um e-mail para um destinatário externo contém informações potencialmente sensíveis, tais como as informações de identificação pessoal (PII).

Além disso, a Goldman Sachs mantém a vigilância para identificar possíveis vazamentos de dados ou ameaças internas, incluindo o uso de técnicas de big data. O acesso a mídias removíveis, como unidades flash USB, CDs graváveis e funcionalidades administrativas locais e aprimoradas do sistema, é proibido por padrão. Quando o acesso a mídias removíveis é aprovado para finalidades de negócio específicas, esse acesso é estritamente controlado e de tempo limitado. Os dados não públicos armazenados em

mídias removíveis são criptografados.

O pessoal da Goldman Sachs não tem permissão para usar sistemas e funções de terceiros, tais como webmail ou ferramentas analíticas não aprovadas, para finalidades de negócio. Além disso, o pessoal da Goldman Sachs não pode utilizar os recursos da Firma para ter acesso a tais sistemas para uso pessoal. O acesso dos funcionários a websites e categorias selecionadas de websites é bloqueado ou limitado com base nas exigências regulatórias, de segurança da informação e de controle interno. Isso inclui redes sociais, compartilhamento de arquivos e webmail.

O time de Global Compliance supervisiona o programa de monitoramento e vigilância de comunicações eletrônicas da Firma, incluindo a revisão de alertas potencialmente indicativos de uma variedade de riscos, resultando em potencial não adesão aos requisitos regulatórios e/ou à política da Firma.

Criptografia

A Goldman Sachs criptografa informações pessoais sensíveis em trânsito e em repouso. Outros tipos de dados são criptografados ou protegidos com controles compensatórios baseados em considerações regulatórias, de segurança e contratuais.

A Goldman Sachs usa sólidos métodos de criptografia padrão do setor. Revisamos regularmente a força de todos os protocolos de criptografia. Soluções padrão da Goldman Sachs estão disponíveis para a criptografia de arquivos transferidos entre a Firma e terceiros. A criptografia de e-mails oportunistas, como a Transport Layer Security (Segurança da Camada de Transporte) (TLS), é habilitada com todos os clientes sempre que possível.

A criptografia de e-mail obrigatória é suportada e ativada por acordos mútuos. As principais atividades de geração e gestão ocorrem em um módulo de criptografia de hardware. O acesso às chaves de criptografia é pré-aprovado, limitado a pessoas autorizadas, sujeito a registro e monitorado regularmente.

Segurança de Dados

A Goldman Sachs possui um programa formal e estruturado de segurança de privacidade de dados que inclui controles e processos obrigatórios para todos os aplicativos e ativos que armazenam ou processam informações de identificação pessoal, incluindo ferramentas de computação do usuário final.

Este programa é continuamente atualizado de acordo com as leis e regulamentos aplicáveis e com os padrões internos da Firma. A Firma possui diretrizes de mesa limpa que instruem o pessoal a manter o espaço de trabalho livre de papéis que contenham dados confidenciais.

A Goldman Sachs implementou controles que bloqueiam as estações de trabalho dos usuários após um período de inatividade definido. Os funcionários são aconselhados a trancar as estações de trabalho quando estiverem fora de suas mesas.

A Goldman Sachs mantém controles para garantir a destruição segura de dados no final da vida útil de um dispositivo de armazenamento. A Firma implementou um programa para identificar sistemas em fim de vida útil, priorizar atualizações ou extinção desses sistemas com base na criticidade dos serviços suportados.

A mídia obsoleta é higienizada usando um conjunto padrão de ferramentas. A destruição da mídia física é realizada de acordo com procedimentos pré-definidos. O descomissionamento de ativos é gerenciado internamente por meio de processos de fluxo de trabalho, inventário e digitalização.

A Firma retém registros por vários períodos, conforme necessário, para cumprir as leis e regulamentos aplicáveis e para estar em conformidade com suas políticas internas de retenção

Segurança Física

Medidas de segurança física são implementadas para proteger data centers e escritórios. Estas medidas incluem acesso por cartão, acesso biométrico, vigilância por vídeo, pessoal de segurança no local, controles ambientais e de gestão de visitantes.

O acesso físico é concedido com base na necessidade, alinhado aos controles de acesso em toda a Firma, aprovado por aprovadores de acesso designados e revisado periodicamente.

A separação física de equipes e escritórios é implementada com base em requisitos comerciais e regulatórios. O acesso aos data centers e escritórios é registrado eletronicamente por meio de cartão de acesso ou tecnologia biométrica.

Todos os visitantes devem apresentar documento de identificação com foto e ter um anfitrião confirmado antes de terem acesso aos escritórios da Firma ou às instalações do data center.

Os registros de visitantes são mantidos.

Os data centers críticos estão geograficamente dispersos e em diversas infraestruturas de serviços públicos e de energia. Estas instalações contam com pessoal de segurança de plantão 24 horas por dia e o acesso é limitado apenas ao pessoal de apoio essencial.

As instalações que apoiam os negócios da Goldman Sachs são protegidas contra riscos ambientais e quedas de energia pelos seguintes controles, quando aplicável: fonte de alimentação ininterrupta (UPS), geradores, unidades de ar-condicionado, sistemas de detecção e supressão de incêndio, sistemas de detecção de água, instalações resistentes a terremotos e projetos sísmicos.

Os padrões de segurança física são aplicados a todos os escritórios globalmente, incluindo locais de recuperação de negócios.

Segurança de Nuvem

Governança de Nuvem

A Goldman Sachs aproveita soluções baseadas em nuvem pública, privada e híbrida, quando apropriado, para determinados fins de computação, armazenamento e negócios. A Firma mantém um processo formal de governança e uma estrutura de controle para todos os aplicativos baseados em nuvem, que são documentados em normas formais.

A governança de risco está incorporada na estrutura global de governança em nuvem da Goldman Sachs para garantir a implantação e migração sustentáveis dos sistemas, aplicativos e dados em nuvem da Firma em ambientes de nuvem pública. Padrões formais se aplicam a recursos de nuvem com escopo para diversas ofertas, incluindo Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS).

Os ambientes de nuvem pública da Goldman Sachs são governados por comitês responsáveis por supervisionar os processos relevantes para a implantação e implementação da tecnologia de nuvem. Além do Comitê Global de Risco de Tecnologia e do Grupo de Direção de Risco de Engenharia mencionados anteriormente, os seguintes grupos supervisionam a segurança da nuvem:

- O Grupo Diretor de Governança de Nuvem Pública garante a conformidade com a norma Firmwide sobre Governança Global de Nuvem e supervisiona a governança ponta a ponta da adoção da nuvem.
- O Grupo Diretor de Riscos de Terceiros gerencia o processo de análise de risco do fornecedor, incluindo aceitação de risco e planos de correção para fornecedores de nuvem.

Controles e Avaliações na Nuvem

A Goldman Sachs estabeleceu controles definidos para aplicativos em nuvem, incluindo criptografia e controles compensatórios, autenticação rigorosa, acesso baseado em funções, registro centralizado, segmentação de rede e auditoria. O monitoramento contínuo do controle e as portas automatizadas de aplicação do controle são aproveitados para que os recursos baseados em nuvem detectem qualquer configuração incorreta. Os aplicativos hospedados na nuvem passam por uma avaliação formal de risco e revisão de arquitetura de acordo com o risco, usando um inventário de controle. Cada aplicativo deve preencher um perfil de risco para determinar os requisitos regulatórios e baseados em risco. As classificações de risco devem ser revisadas e atualizadas para cada aplicação anualmente. Os riscos identificados através de avaliações são registrados em inventários centralizados que detalham informações

importantes sobre aplicações e descobertas. A Firma estabeleceu procedimentos, processos de revisão e portas de controle para integração de dados em plataformas de software hospedadas na nuvem. Os provedores de serviços em nuvem estão sujeitos a uma revisão aprimorada de gerenciamento de fornecedores que abrange a entrega segura de serviços e disposições de auditoria, e devem satisfazer os requisitos de controle de nuvem pública da Firma.

Segurança para Inteligência Artificial

Segurança para Inteligência Artificial

Dados os desenvolvimentos tecnológicos em Inteligência Artificial Generativa (GenAI) e Grandes Modelos de Linguagem (LLMs), a Goldman Sachs está avaliando cuidadosamente sua abordagem à Inteligência Artificial (IA), pois ela ou seus fornecedores, clientes ou contrapartes terceirizados podem desenvolver ou incorporar tecnologia de IA em determinados processos, serviços ou produtos de negócios. Como tal, a Firma tem uma Política de Inteligência Artificial em toda a Firma que estabelece uma estrutura para reger o uso de IA em toda a Firma.

A firma aproveita um modelo federado para o desenvolvimento de casos de uso de IA para facilitar sinergias entre segmentos de negócios com experiência comercial e equipes de plataforma com experiência em GenAI. A governança e supervisão formal e divisional de toda a Firma garante a mitigação de riscos e o alinhamento com as metas de negócios, requisitos regulatórios, políticas da Firma e considerações de investimento.

O acesso a LLMs externos foi intencionalmente restrito pela Firma e não pode ser acessado a partir de sistemas da Firma ou usado para fins comerciais sem aprovação prévia.

Segurança para fornecedores

Segurança para fornecedores

Os fornecedores são vistos como uma extensão da Goldman Sachs. Como tal, a Firma possui uma política e um programa abrangente de gerenciamento de fornecedores em toda a Firma que documenta uma estrutura baseada em risco para gerenciar relacionamentos com fornecedores terceirizados, consistente com as orientações regulatórias e a política da Firma. A gestão de riscos de segurança da informação está integrada no processo de gestão de fornecedores da Firma, que abrange a seleção de fornecedores, integração, monitoramento de desempenho e gestão de riscos. Espera-se que os fornecedores projetem, implementem e mantenham controles de segurança da informação consistentes com as políticas e normas de segurança da Firma.

Os fornecedores que acessam as informações da Goldman Sachs são obrigados a passar

por uma avaliação inicial com base no risco ajustado. Posteriormente, a Firma realiza recertificações com uma amplitude e frequência determinadas pela classificação de segurança da informação de cada fornecedor, que é calculada com base em vários fatores, incluindo o tipo de dados armazenados e processados por um fornecedor específico.

Essas avaliações também podem incluir o uso de produtos de pontuação de mercado de terceiros para avaliar a postura de segurança dos fornecedores em relação à Internet. Todas as avaliações determinam a maturidade das práticas de segurança da informação, segurança cibernética e continuidade de negócios do fornecedor. As lacunas encontradas durante essas avaliações de due diligence são classificadas por risco, registradas e abordadas de acordo com as normas da Firma.

A Goldman Sachs realiza supervisão contínua dos fornecedores com base na criticidade do serviço específico de cada fornecedor para a Firma e nos resultados da avaliação de risco inicial. Os fornecedores críticos recebem maior foco e due diligence. As alterações no serviço prestado por um determinado fornecedor são identificadas como parte de um processo de supervisão padrão e podem desencadear uma avaliação de risco atualizada antes da Firma incorporar serviços adicionais.

A política da Goldman Sachs exige que os fornecedores assinem disposições contratuais padrão antes de receberem informações confidenciais da Firma. Essas disposições têm requisitos específicos de controle de segurança da informação, que são negociados com fornecedores que armazenam, acessam, transmitem ou de outra forma processam informações confidenciais em nome da Firma durante a integração ou renovações de contrato, conforme aplicável.

Equipes dedicadas em toda a Firma são responsáveis por avaliações regulares e relatórios sobre os controles de segurança da informação dos fornecedores. Relatórios periódicos das principais métricas de gerenciamento de risco do fornecedor são fornecidos à gestão de negócios.

Detectar

Registro e Monitoramento Contínuo

Registro

A Goldman Sachs habilitou o registro de eventos importantes, incluindo falhas de login, atividade administrativa e atividade de alteração.

A gestão de arquivos de registro segue o princípio dos privilégios mínimos. Somente os processos de aplicação têm acesso escrito aos arquivos de registro. As contas do sistema somente têm acesso de leitura aos arquivos de registro.

Os registros são mantidos de acordo com a política da Goldman Sachs sobre retenção de

registros e requisitos legais e regulatórios. Os registros são mantidos no mínimo por 30 dias. A Goldman Sachs mantém controles para impedir que os registros contenham informações confidenciais, tais como as informações pessoais identificáveis (PII), credenciais de autenticação ou chaves de criptografia.

O registro de eventos de segurança é habilitado para permitir a análise forense do sistema e a análise de vigilância de Risco Tecnológico. Os registros de eventos de segurança são protegidos contra acesso não autorizado, modificação e substituição acidental ou deliberada.

Proteção contra Malware

O software antimalware padrão do setor é instalado em todos os *endpoints* e servidores Windows e na infraestrutura de e-mail da Firma.

Os alertas antimalware são monitorados por funcionários da Goldman Sachs. O malware é eliminado e, se necessário, os sistemas são reconstruídos.

Os arquivos de assinatura de malware são atualizados regularmente, no mínimo diariamente, por meio de solicitações automáticas a partir dos sistemas na rede da Firma.

As verificações de tempo de execução são realizadas em executáveis específicos para reduzir a possibilidade de exploração via malware. A permissão de listagem de aplicativos é implementada para detectar, relatar e prevenir a execução de malware.

A Goldman Sachs assina uma solução de pré-filtragem de e-mail para reduzir a quantidade de malware recebida por seu gateway de e-mails.

A Goldman Sachs utiliza um sistema de proteção de e-mail desenvolvido para impedir que spam, phishing e vírus cheguem às caixas de entrada dos funcionários.

A Goldman Sachs evita ativamente o spoofing por meio de uma política e um protocolo de autenticação de e-mail para impedir o spoofing de e-mails trocados entre a Firma e seus clientes. A Goldman Sachs também atribui uma score de impostor para cada e-mail, marcando os e-mails acima de um limite de classificação para quarentena e avaliação de possível spoofing.

A Goldman Sachs estabeleceu as principais métricas para definir uma linha de base para o monitoramento contínuo do estado do sistema e a detecção de anomalias no ambiente de produção da Firma. Critérios pré-determinados são aplicados a eventos de segurança para gerar alertas. Ferramentas de monitoramento estão em vigor para notificar o pessoal apropriado sobre problemas de segurança. Os alertas são classificados, priorizados e acionados por pessoal apropriado para correção oportuna com base na criticidade do negócio.

Monitoramento de Segurança e Detecção de Invasão

A Firma mantém um Hunt Team com especialistas dedicados, focados na identificação

proativa de atividades maliciosas anteriormente não detectadas e oportunidades para melhorar continuamente a postura de controle da Goldman Sachs. Além disso, o Hunt Team coleta inteligência sobre ameaças para identificar ativamente possíveis indicações de atividades de ameaças em toda a rede da Goldman Sachs.

A Goldman Sachs mantém processos de monitoramento para detectar atividades incomuns de forma tempestiva. A Firma coleta, analisa e correlaciona dados de eventos em toda a organização para realizar uma agregação centralizada em tempo real e impedir ataques cibernéticos multifacetados, aplicando uma série de sensores distribuídos em todas as áreas.

Periodicamente, a Goldman Sachs realiza simulações de ataques cibernéticos, microtestes, testes mensais e exercícios de simulação, para detectar falhas de controle no comportamento dos funcionários, políticas, procedimentos e recursos.

A Goldman Sachs autoriza e monitora as conexões com terceiros, e coleta e retém persistentemente as respectivas informações. A Goldman Sachs possui alertas automatizados para monitorar e impedir qualquer acesso não autorizado a um sistema crítico por parte de um fornecedor de serviços terceirizado.

A Goldman Sachs usa a inteligência contra ameaças para analisar as táticas, técnicas e procedimento, o que resulta no ajuste de controles para mitigar ameaças adversas emergentes. Isto resulta no ajuste dos controles para evitar ameaças adversas emergentes. A Goldman Sachs também compartilha a inteligência contra ameaças com os pares de seu setor, como uma abordagem para manter ativamente a mitigação de riscos coletiva, e aprimorar a segurança das conexões externas.

Ameaça Interna

A Goldman Sachs possui um programa estabelecido de ameaças internas para detectar e impedir atividades maliciosas e não intencionais realizadas por seus funcionários sem autorização.

A Firma utiliza uma variedade de controles telemétricos, de detecção e preventivos para lidar com ameaças internas, incluindo, entre outros, monitoramento de endpoints de usuários e gerenciamento de direitos.

Responder

Incidentes de Segurança

Gestão de Incidentes e Problemas

A firma mantém uma política e procedimentos de gestão de incidentes e problemas para mitigar riscos e proteger a confidencialidade, integridade e disponibilidade dos ambientes de produção da Firma, minimizando a interrupção dos negócios. A firma

estabeleceu procedimentos padronizados que permitem a gestão de incidentes, notificação e governança post-mortem.

Gestão de Incidentes de Segurança

A Goldman Sachs possui uma Global Cyber Defense and Intelligence Team (Equipe de Defesa e Inteligência Cibernética -GCDI) dedicada, responsável por detectar, investigar e responder as ameaças e incidentes de segurança da informação que têm um impacto potencial sobre a confidencialidade, integridade ou disponibilidade do ambiente de informações e tecnologia da Firma.

A GCDI mantém procedimentos para identificar e responder a incidentes de segurança da informação específicos e trabalha com outras áreas dentro da Goldman Sachs para conter, mitigar e remediar possíveis incidentes. Além disso, a GCDI mantém protocolos de encaminhamento para assegurar que os clientes, órgãos reguladores ou outras partes sejam adequadamente notificadas sobre quaisquer incidentes de segurança, quando exigido por leis, contratos ou regulamentos aplicáveis. A GCDI mantém ainda um centro dedicado de gerenciamento de ameaças que opera 24 horas por dia, 7 dias por semana.

A Goldman Sachs implementou um programa global de preparação para incidentes de segurança para apoiar o gerenciamento de incidentes de segurança. A Divisão de Risco Tecnológico conduz exercícios table top focados nos negócios com unidades de negócios e equipes regionais para avaliar seus processos, compreensão e prontidão, com supervisão da Divisão de Risco Operacional. Externamente, o programa abrange a participação das empresas no setor financeiro e em exercícios de cibersegurança do sector público-privado para garantir a preparação da Firma para a coordenação com outras instituições, mercados financeiros e agências governamentais relevantes.

Inteligência de Combate a Ameaças

A Goldman Sachs reconhece que os agentes de ameaças cibernéticas têm como alvo as redes, vendedores, fornecedores e o pessoal da Firma, juntamente com o setor financeiro mais amplo, a fim de conduzir fraudes, roubar informações proprietárias e/ou perturbar a capacidade da Firma de conduzir negócios e apoiar seus clientes e consumidores.

A equipe de Análise de Ameaças Cibernéticas (CTA) da GCDI é responsável por proteger a Firma contra adversários externos, identificando proativamente ameaças cibernéticas relevantes, avaliando o risco que essas ameaças representam para os ativos da Firma e trabalhando com o pessoal da Divisão de Engenharia e das unidades de negócios afetadas para proativamente reduzir ou mitigar o risco para a Goldman Sachs.

A inteligência de segurança e as informações sobre ameaças são obtidas de provedores de serviços de inteligência terceirizados, consórcios industriais, monitoramento interno, bem como de fontes públicas e governamentais.

Seguro Cibernético

A Goldman Sachs mantém uma política de seguro cibernético que cobre seus custos diretos com incidentes de segurança, bem como as notificações de clientes aplicáveis e os serviços de monitoramento de crédito, quando necessário. Essa política também inclui uma cobertura para questões relacionadas a Interrupções do Negócio. A política de segurança cibernética da Firma é apoiada por um grupo de seguradoras.

Continuidade do Negócio e Resiliência Tecnológica

Continuidade do Negócio

A Goldman Sachs estabeleceu uma estrutura de Planejamento de Continuidade do Negócio para garantir sua preparação na hipótese de interrupções em suas operações.

O Programa de Resiliência de Negócio da Goldman Sachs é composto pelos seguintes elementos-chave: Gestão de Crise, Requisitos de Continuidade do Negócio, Resiliência Tecnológica, Soluções de Recuperação de Negócios, Garantia e Melhoria de Processos/Avaliação Contínua. A descrição do Programa de Resiliência de Negócio (incluindo Recuperação de Desastres) da Firma está disponível em seu website.

A Goldman Sachs desenvolveu Planos de Continuidade de Negócios (BCP) para lidar com interrupções operacionais. Os planos devem ter coordenador(es) de BCP identificados que desenvolvem e mantêm o BCP atribuído e garantem os requisitos de teste. Os BCPs devem ser revisados e atualizados pelos Coordenadores de BCP e certificados pelos Proprietários de BCP na frequência exigida pelos padrões da Firma. Cada unidade de negócios identifica as suas atividades críticas, os ativos dependentes (pessoas, instalações, sistemas e terceiros) que suportam essas atividades e o impacto que uma interrupção desses ativos dependentes teria nas atividades da unidade de negócios.

Como parte do BCP, a unidade de negócios deve concluir a análise de impacto nos negócios. Os Coordenadores BCP identificam a criticidade, os objetivos de tempo de recuperação, as dependências e as estratégias de recuperação de seus processos principais. Esses processos determinam o tipo de garantia necessária para registrar a integridade, por exemplo, testes de recuperação de pessoas, testes de failover de aplicativos, treinamento, simulações de table top.

A estratégia de mitigação de riscos de continuidade de negócios da Goldman Sachs inclui capacidades de resiliência, como local próximo, local remoto, trabalho em casa e capacidades de recuperação dispersas, quando apropriado, a fim de mitigar riscos e enfrentar ameaças à região. As instalações de recuperação de locais remotos da Firma residem em redes de energia e serviços públicos diferentes dos locais principais dos escritórios.

A Goldman Sachs realiza extensos testes de preparação para continuidade de negócios, incluindo testes de failover de tecnologia, instalações de recuperação de pessoas, trabalho em casa e transferência regional. A Firma também participa de testes em nível

industrial com as principais bolsas de valores, agências governamentais e autoridades locais. As divisões da Firma realizam micro-exercícios, bem como cadeia de comando e testes de notificação automática. +

Os Centros de Gestão de Crises que operam 24 horas por dia, 7 dias por semana em todas as regiões permitem à Firma monitorar seu ambiente, executar procedimentos de gestão de crises pré-estabelecidos e coordenar respostas a incidentes em todo o mundo.

Backup e Recuperação de Dados

Os processos de manutenção de registros, backup de dados e recuperação da Firma são executados usando um sistema empresarial padrão do setor. Existem processos para identificar, encaminhar e remediar exceções, conforme apropriado. Os backups de dados são gravados em uma plataforma imutável baseada em disco para fins de recuperação. Periodicamente, quando possível, os dados são gravados em mídia de fita criptografada e enviados para locais externos para armazenamento.

A Firma testa regularmente a capacidade dos aplicativos de fazer failover para data centers alternativos como parte do programa de testes do BCP. As solicitações de recuperação orientadas pelo usuário são simplificadas por meio de um sistema de emissão de tíquetes. Tentativas de recuperação de dados de backup são registradas.

Resiliência Tecnológica

A Goldman Sachs possui um programa robusto de resiliência tecnológica para garantir que os aplicativos internos e os componentes que dependem da infraestrutura demonstrem o nível adequado de resiliência e recuperação com base na criticidade do negócio. Tais controles incluem:

• Dispersão de processamento (redução de dependência de local único);

• Resiliência de rede, telecomunicações e acesso remoto (múltiplos pontos de redundância e resiliência);

• Tecnologia regional operando independentemente de aplicativos críticos para o mercado;

• Inventário e hierarquização dos aplicativos de negócio (objetivos de tempo de recuperação);

• Inclusão de dependências tecnológicas em todos os planos de unidades de negócio

aplicáveis ;• Testes de resiliência.

Com base nos requisitos de negócios, muitos aplicativos críticos são implementados e testados em vários centros de dados para garantir uma operação perfeita caso um centro de dados sofra uma interrupção.

A Goldman Sachs participa de iniciativas de testes do setor financeiro, nos locais onde são oferecidas, para exercer capacidades de conectividade alternativas e para

demonstrar uma capacidade de operar por meio de uma continuidade de negócios significativa e/ou evento de desastre utilizando sites de backup e unidades de recuperação alternativas.

A Firma mantém uma estrutura documentada e um programa de recuperação para identificar e mitigar incidentes de destruição cibernética, como ransomware, incluindo coordenação entre partes interessadas internas e colaboração com partes externas, como autoridades policiais e reguladores.

Nossas Expectativas sobre Suas Práticas de Segurança da Informação

Práticas de Segurança da Informação de Clientes

A segurança da informação é responsabilidade de todos e frequentemente envolve a cooperação entre as instituições financeiras e seus clientes. Embora procuremos fornecer o máximo de segurança possível para os serviços oferecidos, confiamos em sua adoção dos controles padronizados de segurança da informação para o uso de dados e sistemas compartilhados entre você e a Goldman Sachs, por exemplo:

• Alinhar os controles de segurança da informação e controles de segurança cibernética aos padrões internacionais, tais como o NIST Cybersecurity Framework, Center of Internet Security (CIS) Critical Controls e a ISO 27001.

• Garantir que apenas os usuários autorizados tenham acesso aos dados da Firma.

• Proteger as credenciais de autenticação, tais como nome de usuário e senha, de usuários autorizados a acessar os dados da Firma.

• Proteger os computadores usados nas interações com a Goldman Sachs usando ferramentas como software antimalware, firewall e sistemas operacionais atualizados.

• Notificar a Goldman Sachs em caso de qualquer comprometimento, real ou suspeito, de seus dados ou sistemas.