## Sumário

## 1. OBJETIVO

Estabelecer as diretrizes, os controles e as responsabilidades necessárias para proteger a infraestrutura tecnológica, sistemas da companhia contra as ameaças cibernéticas, garantindo a continuidade dos serviços financeiros, proteção dos dados de clientes e o cumprimento da Resolução BACEN nº 4.893/2021. São objetivos dessa Política:

**1.1.** Resguardar a companhia quanto à confidencialidade, integridade e disponibilidade das informações;

**1.2.** Assegurar a segurança das redes e dos sistemas de informação, independentemente da sua localização, em função da conectividade existente;

**1.3.** Acompanhar, apoiar e monitorar as medidas de proteção, detecção, resposta e recuperação dos recursos críticos;

**1.4.** Desenvolver planos e ações de comunicação para os riscos de Segurança Cibernética;

**1.5.** Fomentar a gestão segura dos ativos de hardware, software e redes de comunicações;

**1.6.** Direcionar a implementação de controles e processos internos para atendimento aos requisitos de Segurança Cibernética;

**1.7.** Eliminar, transferir, reduzir ou mitigar os riscos de perdas financeiras de clientes e parceiros, de participação no mercado ou de qualquer outro impacto negativo ao negócio, que seja resultado de uma falha de Segurança Cibernética; e

**1.8.** Estimular uma cultura de Segurança Cibernética através de programas de capacitação e conscientização dos colaboradores, inclusive com avaliações periódicas.

## 2. APLICABILIDADE

Esta política se aplica integralmente à Open Co e à Geru SCD, salvo as disposições específicas indicadas em documentos complementares. Esta Política se aplica a todos os colaboradores, prestadores de serviços, parceiros, terceiros e demais partes que possuam acesso aos sistemas e informações da Open Co, independentemente de sua localização ou função. A Política também se estende ao uso de tecnologias e recursos de computação em nuvem.

## 3. REFERÊNCIAS

**3.1.** **ABNT NBR ISO/IEC 27001:2022;**

**3.2.** **ABNT NBR ISO/IEC 27002:2022**

**3.3.** **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)**

**3.4.** **Política de Segurança da Informação (POL-SEG-001)**

**3.5.** **Política de Gestão Integrada de Riscos (POL-SCD-10/22)**

**3.6.** **Política de Compras (POL-GOV-001)**

**3.7.** **Norma de Segurança para Serviços em Nuvem (NOR-TEC-005)**

**3.8.** **Norma de Gestão de Incidentes de Segurança da Informação (NOR-SEG-003)**

**3.9.** **Norma de Uso de Criptografias (NOR-TEC-006)**

**3.10.** **Resolução do BCEN nº 4.893 de 26 de fevereiro de 2021**

**3.10.1.** Resolução BCB nº 85 (Política de segurança cibernética)

**3.10.2.** Resolução BCB nº 342 (Incidentes de segurança)

## 4. TERMOS E DEFINIÇÕES

**4.1.** **Confidencialidade:** Garantia de que as informações sejam acessíveis apenas as pessoas autorizadas;

**4.2.** **Integridade:** Garantia de que os dados estão íntegros e não sofreram alterações;

**4.3.** **Disponibilidade:** Assegurar que as informações e os sistemas estejam acessíveis e utilizáveis sob demanda por pessoas autorizadas;

**4.4.** **Incidente de Segurança Cibernética:** Evento que compromete a CID das informações da Open Co;

**4.5.** **Computação em nuvem:** Tecnologia que permite o uso de recursos de armazenamento e processamento de dados em servidores remotos, acessíveis via internet.

## 5. RESPONSABILIDADES

### 5.1. Responsável por Cibersegurança

**5.1.1.** Estabelecer, aprovar e monitorar a aplicação desta norma, garantindo a sua conformidade com as exigências internas de segurança e as melhores práticas de mercado.

### 5.2. Equipe de Segurança da Informação

**5.2.1.** Implementar os controles de segurança;

**5.2.2.** Monitorar o ambiente cibernético;

**5.2.3.** Realizar as análises de risco; e

**5.2.4.** Responder prontamente a incidentes.

### 5.3. Colaboradores e Terceiros:

**5.3.1.** Seguir as diretrizes desta política;

**5.3.2.** Reportar qualquer atividade suspeita ou incidente de segurança e participar de treinamentos de cibersegurança;

**5.3.3.** É responsabilidade de todos reportar imediatamente qualquer atividade suspeita ou incidente de segurança, fomentando uma cultura de transparência e não retaliação para garantir a rápida resposta.

### 5.4. Controles Internos

**5.4.1.** Realizar avaliações regulares para verificar a eficácia dos controles de segurança e a conformidade com esta política.

## 6. DIRETRIZES

**6.1.** A área de Segurança da Informação deve:

**6.1.1. Gestão de Ameaças Cibernéticas**

6.1.1.1. **Avaliar as Vulnerabilidades e Riscos**: Realizar as avaliações periódicas de vulnerabilidades e riscos cibernéticos para identificar e mitigar as potenciais ameaças; e

6.1.1.2. **Abordagem Baseada em Risco**: Priorizar as medidas de segurança e proteção com base na criticidade e no impacto dos riscos identificados.

**6.1.2. Configuração Segura de Sistemas e Redes**

6.1.2.1. **Padrões de Configuração Segura**: Estabelecer e manter padrões de configuração segura para os servidores, dispositivos de rede e sistemas operacionais;

6.1.2.2. **Desativação de Serviços Desnecessários**: Desativar os serviços desnecessários e reforçar as permissões de acesso para minimizar as superfícies de ataque; e

6.1.2.3. **Firewall e IPS**: Utilizar os firewalls e sistema de prevenção de intrusões (IPS) para proteger as redes da Open Co contra os acessos não autorizados e atividades maliciosas**.**

#### 6.1.3. Proteção de Dados e Criptografia

6.1.3.1. **Criptografia de Dados**: Implementar a criptografia para proteger os dados sensíveis em repouso e em trânsito, com base na classificação de sensibilidade dos dados definida pela Open Co e conforme a Norma de Uso de Criptografias (NOR-TEC-006);

6.1.3.2. **Gestão de Chaves**: Garantir que as chaves de criptografia sejam gerenciadas de forma segura e que os mecanismos de criptografia estejam sempre atualizados; e

6.1.3.3. **Zero Trust**: Adotar progressivamente uma abordagem de 'Zero Trust', baseada na verificação explícita, concessão de privilégio mínimo e na presunção de violação, para acesso a todos os recursos.

#### 6.1.4. Monitoramento e Detecção de Ameaças

6.1.4.1. **Monitoramento Contínuo**: Monitorar continuamente o ambiente cibernético por meio de sistemas de detecção e resposta a ameaças (EDR) e Sistema de Gerenciamento e Monitoramento de Eventos de Segurança (SIEM) Security Information and Event Management;

6.1.4.2. **Análise de Logs:** Analisar logs de eventos de segurança para identificar atividades suspeitas e anômalas; e

6.1.4.3. **Alertas Automáticos:** Configurar alertas automáticos para responder rapidamente a potenciais incidentes.

#### 6.1.5. Resposta a Incidentes de Segurança Cibernética

6.1.5.1. **Plano de Resposta a Incidentes:** Manter um plano de resposta a incidentes cibernéticos com procedimentos claros para notificação, análise, contenção, erradicação e recuperação; e

6.1.5.2. Plano de Resposta a Incidente (PRI) estabelece as diretrizes e os procedimentos a serem seguidos em caso de incidentes de segurança que possam comprometer a confidencialidade, integridade ou a disponibilidade dos ativos de informação da Open Co, os documento a ser utilizados são:

6.1.5.2.1. Norma de Gestão de Incidentes de Segurança da Informação (NOR-SEG-003);

6.1.5.2.2. Plano de Resposta a Incidente (DOC-SEG-001);

6.1.5.2.3. Plano de Continuidade Operacional de APIs (FOR-SEG-023);

6.1.5.2.4. Plano de Resposta a Incidente em Cenários (FOR-SEG-015);

6.1.5.2.5. Plano de Resposta e Cenários - Tecnológicos e Infraestrutura em Rede (FOR-SEG-013); e

6.1.5.2.6. Plano de Resposta e Cenários - Ambientais e Físicos (FOR-SEG-012 - PRD).

**6.1.6. Relatório Anual de Implementação do Plano de Ação e de Resposta a Incidentes:**

6.1.6.1. Manter atualizado, conforme necessidade, os relatórios abaixo:

6.1.6.1.1. Relatório Anual de Implementação do Plano de Ação e de Resposta a Incidentes;

6.1.6.1.2. Relatório Anual de Implementação do Plano de Ação e de Resposta a Incidentes; e

6.1.6.1.3. Relatório Anual de Implementação do PRI.

**6.1.7. Simulações e Treinamentos**

6.1.7.1. Realizar as simulações e treinamentos periódicos para preparar a equipe para possíveis incidentes;

6.1.7.2. Manter atualizado, conforme necessidade, os relatórios abaixo:

6.1.7.2.1. Relatório do Resultado do teste de Recuperação de Desastre / DR (Disaster Recovery).

**6.1.8. Treinamento e Conscientização**

6.1.8.1. **Capacitação Contínua**: Oferecer treinamentos regulares sobre as práticas de cibersegurança para todos os colaboradores, focando na identificação de phishing a partir de simulações práticas, uso seguro de senhas e boas práticas no ambiente digital entre outras campanhas. Para atender as necessidades de capacitação, seguir e manter atualizados os seguintes controles:

6.1.8.1.1. Calendário de publicação de treinamentos e campanhas de conscientizações (POP-SEG-037); e

6.1.8.1.2. Campanhas de Simulação de Phishing (POP-SEG-038).

6.1.8.2. **Campanhas de Conscientização:** Promover campanhas de conscientização para reforçar a importância da segurança cibernética no dia a dia. Para atender as necessidades de campanhas, seguir e manter atualizados os seguintes controles:

6.1.8.2.1. Programa de Conscientização & Simulação de Phishing (POP-SEG-035); e

6.1.8.2.2. Campanhas de Conscientização (POP-SEG-036).

**6.1.9. Gestão de Terceiros e Computação em Nuvem**

6.1.9.1. **Avaliação de Risco de Terceiros**

6.1.9.1.1. **Identificação dos Terceiros:** Registrar e monitorar todos os terceiros que tenham acesso aos sistemas e dados da Open Co, conforme as diretrizes de segurança da Política:

6.1.9.1.1.1. Política de Compras (POL-GOV-001).

**6.1.9.1.2. Avaliação Inicial de Riscos:** Realizar uma avaliação de segurança antes de contratar serviços de terceiros ou de computação em nuvem, identificando possíveis ameaças e vulnerabilidades associadas e notificar o Banco Central do Brasil sobre contratações em nuvem conforme:

6.1.9.1.2.1. Norma de Segurança para Serviços em Nuvem (NOR-TEC-005); e

6.1.9.1.2.2. Procedimento de Reporte de Contratação de Serviços em Nuvem ao Banco Central do Brasil (POP-JUR-001).

**6.1.9.1.3. Monitoramento Contínuo**: Realizar as avaliações periódicas para assegurar que os riscos continuam sendo gerenciados adequadamente, especialmente quando há mudanças nos serviços prestados ou no ambiente de operacional. Para atender as necessidades de gestão de mudanças seguir e manter atualizado os seguintes controles:

6.1.9.1.3.1. Política de Gestão Integrada de Riscos (POL-SCD-10/22); e

6.1.9.1.3.2. Matriz de Riscos de Segurança da Informação (FOR-SEG-016).

**6.1.9.1.4. Critérios de Seleção:** Estabelecer critérios rigorosos para seleção de fornecedores, assegurando que atenda aos padrões de segurança exigidos. Para atender as necessidades de critérios de seleção seguir e manter atualizado os seguintes controles:

6.1.9.1.4.1. Processo de Due Diligence de Segurança e Privacidade (POP-SEG-064).

**6.1.9.1.5. Padrões de Segurança de Fornecedores**

6.1.9.1.5.1. **Acordos Contratuais**: Incorporar cláusulas contratuais específicas que exijam que os fornecedores sigam os padrões de segurança da Open Co;

6.1.9.1.5.2. **Auditorias de Segurança**: Exigir que os fornecedores realizem auditorias de segurança regulares e forneçam os relatórios dessas auditorias;

6.1.9.1.5.3. **Conformidade com Políticas e Normas**: Assegurar que os fornecedores implementem e mantenham políticas de segurança cibernética alinhadas às exigências da Open Co; e

6.1.9.1.5.4. **Relatórios de Conformidade**: Solicitar que os fornecedores apresentem relatórios de

conformidade que comprovem a aderência aos padrões de segurança.

**6.1.10. Auditorias e Revisões**

6.1.10.1. **Plano de Auditoria:** Desenvolver e manter um plano de auditoria cibernética que detalhe a frequência e o escopo das auditorias a serem realizadas;

6.1.10.2. **Equipe de Auditoria**: Designar uma equipe de auditores internos ou contratar uma externa para conduzir as auditorias de segurança cibernética, assegurando que possuem habilidades e conhecimentos necessários;

6.1.10.3. **Processo de Auditoria:** Realizar auditorias abrangentes que incluem a revisão de controles técnicos, operacionais e administrativos de segurança cibernética; e

6.1.10.4. **Correção de Deficiências:** Documentar as deficiências de segurança identificadas durante a auditoria e implementar um plano de ações corretivas.

## 7. REVISÕES

**7.1.** Esta política é revisada com periodicidade anual, ou quando ocorre uma mudança no seu escopo, regulamentações setoriais, leis vigentes ou conforme o entendimento do Comitê no processo de melhoria contínua.

## 8. CONTROLE DE VERSÃO

**8.1.** Esta Política possui um controle de versão que identifica o número da sua versão, a data que entrou em vigor e os responsáveis pela revisão e aprovação; e

**8.2.** Esta Política é aprovada pela Alta Direção da Open Co, e entra em vigor imediatamente após sua aprovação formal, assinada em formato eletrônico, usando sistemas como ClickSign ou DocuSign.

| Versão | Data | Descrição | Elaboração | Revisão | Aprovação |
|---|---|---|---|---|---|
| 1.0 | 21/01/22 | Criação do Documento | Analista de Segurança da Informação | Diretora - Jurídico | CEO |
| 2.0 | 12/11/24 | Atualização do Documento - POL-SCD-14 | Analista de Segurança da Informação Alan Cardoso | Head of Engineering Daniel Frank<br><br>Coordenadora de Compliance Cecilia Santana | CEO - Chief Executive Officer Sandro Reiss<br><br>CTO - Chief Technology Officer Francisco Ferreira |

# POL-SEG-002 - Política Cibernética..pdf

Documento número #ccf8dbe3-7597-4614-a208-2bd0b2264c94

**Hash do documento original (SHA256):** 1c583bebaaf746d5f6889208aa84e964f1c594f6deb859754fbe5556d2d808b0

## Assinaturas

**Sandro Weinfeld Reiss**
Assinou para aprovar em 23 mai 2025 às 10:28:51

**Francisco Ferreira**
Assinou em 22 mai 2025 às 15:16:02

## Log

| | |
|---|---|
| 22 mai 2025, 15:07:14 | Operador com email cecilia.souza@open-co.com na Conta ca522fc5-ccd7-4c9b-8de6-35d4730b760d criou este documento número ccf8dbe3-7597-4614-a208-2bd0b2264c94. Data limite para assinatura do documento: 21 de junho de 2025 (15:07). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro. |
| 22 mai 2025, 15:08:41 | Operador com email cecilia.souza@open-co.com na Conta ca522fc5-ccd7-4c9b-8de6-35d4730b760d alterou o processo de assinatura. Data limite para assinatura do documento: 21 de junho de 2025 (16:55). |
| 22 mai 2025, 15:08:41 | Operador com email cecilia.souza@open-co.com na Conta ca522fc5-ccd7-4c9b-8de6-35d4730b760d adicionou à Lista de Assinatura: francisco.ferreira@open-co.com para assinar, via E-mail.<br><br>Pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Francisco Ferreira. |
| 22 mai 2025, 15:08:41 | Operador com email cecilia.souza@open-co.com na Conta ca522fc5-ccd7-4c9b-8de6-35d4730b760d adicionou à Lista de Assinatura: sandro@open-co.com para assinar para aprovar, via E-mail.<br><br>Pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Sandro Weinfeld Reiss. |
| 22 mai 2025, 15:16:02 | Francisco Ferreira assinou. Pontos de autenticação: Token via E-mail francisco.ferreira@open-co.com. IP: 201.76.168.178. Componente de assinatura versão 1.1215.0 disponibilizado em https://app.clicksign.com. |
| 23 mai 2025, 10:28:51 | Sandro Weinfeld Reiss assinou para aprovar. Pontos de autenticação: Token via E-mail sandro@open-co.com. IP: 189.110.23.150. Localização compartilhada pelo dispositivo eletrônico: latitude -23.55159030448064 e longitude -46.68656259462919. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1215.0 disponibilizado em https://app.clicksign.com. |

| | |
|---|---|
| 23 mai 2025, 10:28:53 | Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número ccf8dbe3-7597-4614-a208-2bd0b2264c94. |