

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

SUMÁRIO

1. INTRODUÇÃO	3
2. OBJETIVO	3
3. ESCOPO E APLICAÇÃO	4
4. ALINHAMENTO REGULATÓRIO E DE PADRÕES INTERNACIONAIS	4
5. GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA.....	5
6. GESTÃO DE RISCOS	5
7. GESTÃO DE ATIVOS, ACESSOS E INFORMAÇÕES	5
8. SEGURANÇA DE COLABORADORES E TERCEIROS	5
9. CONTROLES DE SEGURANÇA PROTETIVA	6
10. MONITORAMENTO, DETECÇÃO E GESTÃO DE INCIDENTES	6
11. RECUPERAÇÃO DE DESASTRES.....	6
12. CONSCIENTIZAÇÃO E MELHORIA CONTÍNUA	7

1. INTRODUÇÃO

O Grupo IHS e a I-Systems definiram uma Política de Segurança da Informação abrangente, que serve como base para todas as políticas, procedimentos e controles utilizados pelas Companhias. Ela reflete o compromisso executivo da organização em proteger seus ativos de informação e em operar um Sistema de Gestão de Segurança da Informação (“ISMS”) alinhado com padrões internacionais e expectativas regulatórias.

A presente Política estabelece as diretrizes sobre como a segurança da informação é governada, gerenciada e continuamente aprimorada. Todas as subpolíticas sob os domínios ‘Governar’, ‘Identificar’, ‘Proteger’, ‘Detectar’, ‘Responder’ e ‘Recuperar’ são extensões desta Política principal e definem requisitos operacionais específicos em apoio a esses princípios.

Esta Política se aplica a todos os usuários dos sistemas utilizados pelo Grupo IHS, e a todos os processos, tecnologias e serviços envolvidos na coleta, processamento, armazenamento ou transmissão de informações.

O propósito da Política de Segurança da Informação e Cibersegurança é:

- Apoiar os objetivos estratégicos de negócio, posicionando a segurança como habilitadora e não apenas um mecanismo de proteção.
- Garantir uma abordagem consistente e estruturada para segurança da informação.
- Alinhar-se às normas, padrões e requisitos regulatórios reconhecidos internacionalmente.
- Proteger os ativos de informação contra ameaças cibernéticas.
- Garantir conformidade legal e regulatória com as leis aplicáveis.
- Apoiar melhorias contínuas voltadas à manutenção e promoção da segurança.

O Grupo IHS e a I-Systems estão comprometidos em proteger seus ativos de informação, sistemas e serviços contra ameaças cibernéticas e acessos não autorizados. Segurança da informação e cibersegurança são elementos fundamentais para garantir continuidade de negócios, resiliência operacional, conformidade com regulamentações aplicáveis e confiança de clientes, parceiros e reguladores.

A proteção de informações — incluindo dados pessoais, confidenciais e críticos para o negócio — é essencial para gerir riscos de segurança, proteger infraestruturas críticas e apoiar a capacidade da organização de prevenir, resistir e responder a eventos cibernéticos adversos.

2. OBJETIVO

O objetivo deste documento é apresentar, de forma resumida e transparente, os principais princípios, controles e práticas adotados pelo Grupo IHS e I-Systems para garantir segurança da informação e cibersegurança, alinhadas a padrões internacionais e estruturas regulatórias aplicáveis.

3. ESCOPO E APLICAÇÃO

Esta Política se aplica a todos os colaboradores, contratados, prestadores de serviços e terceiros que acessem, gerenciem, processem, armazenem ou transmitam informações do Grupo IHS e da I-Systems ou utilizem seus sistemas de informação.

Este extrato é destinado a clientes e partes externas, demonstrando as medidas de segurança implementadas para garantir continuidade dos serviços e proteção de dados.

4. ALINHAMENTO REGULATÓRIO E DE PADRÕES INTERNACIONAIS

O Sistema de Gestão de Segurança da Informação (“ISMS”) do Grupo IHS e I-Systems está alinhado com os padrões e boas práticas reconhecidas internacionalmente, os quais são utilizados de acordo com a sua relevância para os serviços de telecomunicações e de infraestrutura em geral, tais como:

- **ISO/IEC 27001**
- **ISO/IEC 27002**
- **NIST Cybersecurity Framework and Principles**
- **Applicable legal, regulatory, and contractual requirements**

Sendo assim, é adotada uma abordagem baseada em riscos para segurança da informação e cibersegurança, consistente com princípios regulatórios aplicáveis a ambientes de telecomunicações, incluindo proteção de infraestruturas críticas, continuidade de serviços e resiliência frente a incidentes cibernéticos.

Em alinhamento com expectativas similares às estabelecidas pela ANATEL para ecossistemas de telecomunicações no âmbito de suas regulamentações específicas, o Grupo IHS e I-Systems:

- Implementa estruturas de governança, gestão de riscos e controles para proteger sistemas que suportam serviços críticos.
- Mantém controles de segurança voltados à preservação da confidencialidade, integridade, disponibilidade, autenticidade e resiliência de informações e serviços.
- Aplica gestão de riscos estruturada para identificar e mitigar ameaças cibernéticas que possam impactar infraestrutura, operações ou clientes.
- Mantém capacidades de backup, recuperação e continuidade para sistemas críticos.
- Promove monitoramento contínuo e detecção de incidentes para possibilitar resposta tempestiva.

Essas medidas contribuem para evitar incidentes que possam comprometer disponibilidade de serviço, estabilidade da infraestrutura ou segurança de dados dos usuários e da rede.

5. GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

O Sistema de Gestão de Segurança da Informação (“ISMS”), sob supervisão executiva e liderança do *Chief Information Security Officer* (CISO), contempla atividades que garantem:

- Papéis e responsabilidades definidos para segurança da informação.
- Estruturação de identificação, avaliação e tratamento de riscos.
- Alinhamento com requisitos legais, regulatórios e do setor.
- Melhoria contínua dos controles e processos de segurança.

O ISMS é revisado, monitorado e auditado periodicamente para garantir eficácia e conformidade.

6. GESTÃO DE RISCOS

Os riscos de segurança da informação são gerenciados via processos formais e documentados que consideram:

- Impacto operacional e sobre o negócio.
- Probabilidade de ameaças e vulnerabilidades.
- Criticidade de ativos e essencialidade de serviços.
- Estratégias de tratamento definidas.

Avaliações de risco são conduzidas recorrentemente ao longo de todo o ciclo de vida de ativos e dos sistemas de informação.

7. GESTÃO DE ATIVOS, ACESSOS E INFORMAÇÕES

O Grupo IHS e I-Systems asseguram que:

- Ativos de informação são devidamente inventariados, classificados e protegidos durante todo seu ciclo de vida.
- Informações são tratadas conforme sua sensibilidade e criticidade.
- Acesso a informações e sistemas é concebido com base nos princípios (i) *security by design* e (ii) *need to know*.
- Controles de acesso físico e lógico são aplicados e revisados periodicamente.

8. SEGURANÇA DE COLABORADORES E TERCEIROS

Requisitos de segurança são aplicados a funcionários e estendidos a terceiros, parceiros e prestadores de serviços, tais quais:

- Papéis e responsabilidades definidos.

- Obrigações de confidencialidade.
- Treinamento e conscientização em segurança da informação e cibersegurança.
- *Due diligence* e avaliação de riscos de terceiros.
- Requisitos de segurança aplicados contratualmente.

9. CONTROLES DE SEGURANÇA PROTETIVA

O Grupo IHS e I-Systems implementam conjuntamente controles administrativos, técnicos e físicos, os quais protegem informações contra acesso, divulgação, alteração ou interrupção não autorizado. Essas medidas podem ser alcançadas como, por exemplo:

- Aquisição e desenvolvimento seguro de sistemas.
- Autenticação e gestão de acessos.
- Proteção criptográfica de dados.
- Segurança de rede, aplicação e nuvem.
- Medidas de privacidade e proteção de dados.
- Programas de treinamento e conscientização em segurança e cibersegurança.

10. MONITORAMENTO, DETECÇÃO E GESTÃO DE INCIDENTES

O Grupo IHS e I-Systems conduzem um monitoramento contínuo e registram eventos para detectar eventuais incidentes de segurança, que inclui:

- Identificação, classificação e avaliação de incidentes.
- Procedimentos definidos de resposta e escalonamento.
- Ações de investigação, contenção e remediação.
- Documentação e reporte, quando necessário.

11. RECUPERAÇÃO DE DESASTRES

Para apoiar resiliência e disponibilidade, o Grupo IHS e I-Systems mantém:

- Planos de Recuperação de Desastres para sistemas críticos.
- Mecanismos de *backup*, retenção e arquivamento.
- Testes periódicos das capacidades de recuperação.

Essas medidas apoiam continuidade operacional em caso de incidentes cibernéticos ou interrupções.

12. CONSCIENTIZAÇÃO E MELHORIA CONTÍNUA

Programas de conscientização e treinamento em segurança são disponibilizados a colaboradores e terceiros relevantes no *onboarding* e periodicamente.

A Política de Segurança da Informação e Cibersegurança, bem como os controles relacionados são revisados ao menos anualmente e são atualizados conforme necessário, para refletir mudanças de negócio, requisitos regulatórios e evolução do cenário e soluções aplicáveis.