Extrato da Política de Segurança da Informação e Segurança Cibernética

Cuidamos com muita responsabilidade e transparência de todos os detalhes para garantir a proteção das informações de nossos clientes, prestadores de serviços e colaboradores.

Trabalhamos para que todas as informações sejam tratadas de maneira ética e sigilosa e que sejam implementados controles para prevenir que ativos de sistemas de informação possam ser acessados ilegalmente, modificados, divulgados sem autorização, falsificados, destruídos ou sofram interferências que afetem a autenticidade, confidencialidade, integridade e disponibilidade das informações.

Respeitamos e promovemos os direitos humanos e as garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação do usuário dos serviços de telecomunicações.

Quer saber mais?

Veja nossa Política de Segurança da Informação e Segurança Cibernética

Política de Segurança da Informação e Segurança Cibernética

1. Objetivos:

Definir os princípios da implantação dos controles de Segurança da Informação, Segurança Cibernética e Privacidade para preservação da finalidade, necessidade, autenticidade, confidencialidade, disponibilidade, diversidade, integridade, interoperabilidade, prioridade, responsabilidade e transparência das informações, protegendo seus clientes, colaboradores, prestadores de serviços, partes interessadas, relacionados aos riscos da Segurança da Informação e Segurança Cibernética para assegurar a continuidade dos negócios da Empresa.

2. Normas, padrões e boas práticas adotadas:

CÓDIGO DE ÉTICA DA AMÉRICA MÓVIL;

RESOLUÇÃO ANATEL Nº 632/2014 - Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações;

RESOLUÇÃO ANATEL Nº 740/2020 - Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações;

LEI Nº 13.709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD);

LEI Nº 13.853/19 – Lei que altera a LGPD e cria a Autoridade Nacional de Proteção de Dados;

ABNT NBR ISO/IEC 27001:2013: Tecnologia da Informação — Técnicas de Segurança — Sistemas de Gestão da Segurança da Informação — Requisitos;

ABNT NBR ISO/IEC 27002:2013: Tecnologia da Informação — Técnicas de Segurança — Código de Prática para Controles de Segurança da Informação;

ABNT NBR ISO/IEC 27032:2015: Tecnologia da Informação — Técnicas de Segurança — Diretrizes para Segurança Cibernética;

ABNT NBR ISO/IEC 27701:2019: Tecnologia da Informação — Técnicas de Segurança — Extensão à ABNT NBR ISO/IEC 27002 para Gestão da Privacidade da Informação – Requisitos e Diretrizes;

ABNT NBR ISO/IEC 27005:2011: Tecnologia da Informação — Técnicas de segurança — Gestão de Riscos de Segurança da Informação;

ABNT NBR ISO 31000:2009 – Gestão de Riscos: Princípios e Diretrizes;

NR-OPS-005 – Plano de Gestão de Riscos para Redes e Serviços de Telecomunicações;

DISASTER RECOVERY INSTITUTE INTERNATIONAL (DRI - https://drii.org/),

BS 25999-1 – BUSINESS CONTINUITY MANAGEMENT Code of Practice (British Standards Institution - https://www.bsigroup.com)

ISO 22.301 - Gestão de Continuidade dos Negócios (https://www.iso.org/standard/50038.html).

3. **Área responsável**: Diretoria de Segurança Corporativa (DSC).

4. **Aprovação:** A Política é aprovada pelo Conselho de Administração da Claro.

5. **Contato para questões relacionadas:**

   A Claro disponibiliza a seus clientes o e-mail duvida.sic@claro.com.br como canal de contato para esclarecimentos de dúvidas ou sugestões.

6. **Ações de conscientização dos usuários:** A Claro disponibiliza através do seu site https://www.claro.com.br/seguranca dicas de Segurança para que os seus clientes tenham o máximo de informações disponíveis, a fim de preveni-los contra Fraudes.

7. **Procedimento de notificação de Incidentes à ANATEL, demais prestadoras de serviços e Usuários:**

   a. Incidentes relevantes serão notificados à ANATEL e compartilhado com as demais prestadoras em plataforma específica, acompanhado das informações técnicas previamente estabelecidas.

b. Quando o Incidente relevante afetar os dados pessoais de titulares, a Autoridade Nacional de Proteção de Dados (ANPD) será também notificada, bem como o usuário afetado será devidamente comunicado pela Claro, observando o disposto na Lei Geral de Proteção de Dados - LGPD.

8. Rol dos Procedimentos e controles adotados de segurança:

a. Gestão de Ativos

Os Ativos são inventariados e protegidos de acessos indevidos ou ameaças que possam comprometer o negócio. Para tanto, o acesso às salas e prédios é limitado, por meio de mecanismos de autenticação e autorização de acesso, destinados a impedir o acesso de indivíduos não autorizados.

Os Ativos são utilizados tão somente para a finalidade devidamente autorizada. A empresa assegura a proteção aos Ativos durante todo o seu ciclo de vida, a fim de garantir que os princípios da confidencialidade, integridade e disponibilidade sejam cumpridos integralmente.

b. Autenticação

Adotamos mecanismos internos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados, levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

c. Segmentação de Rede

Adotamos mecanismos internos para a segmentação da rede e proteção dos seus dados de ataques cibernéticos e determinamos que todos os computadores conectados à rede corporativa não estejam acessíveis diretamente pela Internet. O acesso pela Internet somente poderá ocorrer através de VPN ou pelo VDI (Citrix), com duplo fator de autenticação.

d. Classificação da Informação

Toda e qualquer informação da Empresa é classificada de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Confidencial, Confidencial LGPD, Interna e Pública. Para isso, são consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

e. Controle de Acesso

Adotamos controles de acesso em toda infraestrutura para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados e aos sistemas internos. Desta forma, implementamos mecanismos para a autenticação de usuários, manutenção de segregação de funções e rastreabilidade de acesso, de forma a garantir procedimentos internos adequados e consistentes.

f. Funções e Responsabilidades

Adotamos processo para definir as responsabilidades em gerir e definir processos de segurança para proteger as informações e os ativos da Empresa.

g. Gestão de Riscos

O processo de avaliação de riscos identifica e descreve qualitativamente os riscos existentes priorizados em função dos riscos e objetivos de negócio.

Este processo é dividido nas seguintes etapas:

i. **Identificar Riscos** - tem como objetivo identificar os possíveis eventos que possam causar perdas ou oportunidades potenciais; é a etapa mais importante e envolve a Alta Administração e os executivos das áreas;

ii. **Avaliar e mensurar Riscos** – tem como objetivo identificar as consequências (possíveis impactos / severidade) e a probabilidade da ocorrência do evento;

iii. **Priorizar Riscos** – tem como objetivo comparar os resultados gerados pela análise de riscos com os critérios de avaliação de riscos para definir a ordem de prioridade do tratamento dos riscos priorizados pela criticidade e objetivos de negócio;

iv. **Tratar Riscos** – tem como objetivo identificar as possíveis respostas e controles para o risco priorizado na etapa anterior;

v. **Monitorar** – tem como objetivo acompanhar a evolução dos riscos, dos planos de ação e de indicadores chaves de riscos;

vi. **Comunicar –** tem como objetivo comunicar os resultados da gestão de riscos, conforme matriz de comunicação estabelecida.

h. Segurança Física do Ambiente

Implementamos sistemas para controle de acesso dos colaboradores, prestadores de serviços, fornecedores, provedores e parceiros aos locais restritos. Os equipamentos e instalações de processamento de informação crítica ou sensível são mantidos em áreas seguras, com níveis de controle

de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

i. Gestão de Fornecedores

Verificamos o grau de comprometimento em relação a controles de Segurança da Informação e Segurança Cibernética de todos os nossos prestadores de serviços, fornecedores, provedores e parceiros que processam e armazenam dados da empresa, com a finalidade de verificar o nível de maturidade dos controles de Segurança e Privacidade e o plano de tratamento de incidentes adotados.

Disponibilizamos um canal para que nossos prestadores de serviços, fornecedores, provedores e parceiros comuniquem incidentes de Segurança da Informação e Segurança Cibernética que estejam relacionados às informações da empresa.