Política de Segurança da Informação e Segurança Cibernética

Milhares de consumidores, empresas, colaboradores e prestadores de serviço dependem da segurança dos dados da Claro. Para manter suas informações seguras e os serviços sempre funcionando, a Claro conta com uma infraestrutura sólida e uma política de segurança bem definida. Aqui você vai descobrir um pouco de como ela funciona.

A Claro sempre respeita e promove os direitos humanos e 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.

Além das normas legais, a Claro adota normas, padrões e práticas de segurança internacionais.

Processos de segurança da informação.
Confira alguns dos controles que a Claro adota para assegurar que as informações que usamos estejam devidamente protegidas.

Gestão
Os dados dos clientes são acessados apenas para finalidades específicas, por pessoas e em situações autorizadas. Todo o acesso às salas e edifícios é limitado por mecanismos de autenticação e autorização de acesso.

Autenticação

A Claro conta com diversos mecanismos para garantir que o acesso às informações e ambientes tecnológicos só sejam acessados por indivíduos autorizados. Toda informação é classificada e as funções de cada colaborador são separadas para que cada um tenha acesso ao que é permitido.

Segmentação de Rede

Todos os computadores conectados à rede corporativa da Claro não estão acessíveis diretamente pela Internet. Esse e outros mecanismos internos segmentam a rede para proteger os dados de ataques cibernéticos.

Classificação da Informação

Toda e qualquer informação da Empresa é classificada de acordo com a confidencialidade e as proteções necessárias. 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.

Controle de Acesso

Todos os ambientes físicos e os sistemas internos da Claro possuem controles de acesso para autenticar e rastrear quem tem ou teve acesso a quais ambientes e informações. Assim, evitamos que pessoas não autorizadas tenham acesso aos seus dados.

Gestão de Riscos

Uma das formas de se prevenir e saber como lidar com emergências quando elas aparecem é gestão de riscos.

A Claro identifica potenciais ameaças, avalia as consequências destes possíveis impactos, com uma lista de prioridade de riscos e formas de como

lidar com cada um deles. As ameaças são constantemente monitoradas, assim como os planos de ações para lidar com eles.

Gestão de Fornecedores

Os parceiros da Claro são chave fundamental para garantir a segurança. Por isso, todos os fornecedores que processam e/ou armazenam dados da empresa são avaliados previamente para identificar se eles atendem ao padrão de segurança da Claro.

Notificação de incidentes

No caso de um eventual problema de segurança, a Claro tem uma política de notificação para a ANATEL, para as prestadoras de serviços e para os nossos usuários.

- Incidentes relevantes são comunicados à ANATEL e compartilhados com outras prestadoras em uma plataforma específica, tudo acompanhado das informações técnicas necessárias.
- Se o incidente tiver envolvido dados pessoais, a ANPD - Autoridade Nacional de Proteção de Dados e os usuários afetados serão também comunicados, seguindo a LGPD - Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018.

Você também pode aprender dicas para prevenir fraudes e saber mais sobre segurança na página https://www.claro.com.br/seguranca

Dúvidas ou sugestões sobre nossa Política de Segurança da Informação e Segurança Cibernética: duvida.sic@claro.com.br

Diretoria de Segurança da Informação Corporativa