



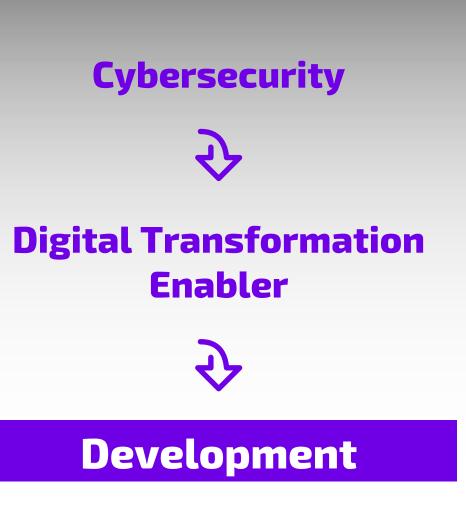
Cybersecurity: The Brazilian Experience in Telecom sector

Humberto Pontes March/2024









Strategic Vision



Strategic Action

Initiative 7: Promotion of a holistic risk management and the protection of the critical infrastrucure

Strategic Action

Initiative 17: Foster the **prevention against fraud and scams** in the digital ecosystem





The promotion of the Security and Resilience of the Telecommunications Networks and Services

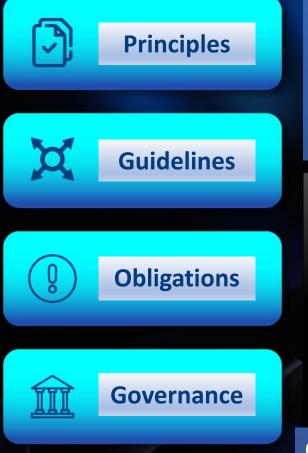




Cybersecurity Regulation



Principles: i.e - Authenticity; Confidentiality; Availability;



Guidelines: i.e - Development of a cybersecurity culture; Safe and sustainable use of networks;Identify, protect, diagnose, respond to and recover from incidents; Security by design and privacy by design.

Mandatory Provisions:

- Cybersecurity Policy;
- Mandatory notification of relevant incidents;
- Information sharing between providers;
- Suppliers cybersecurity policy and audits;
- Vulnerability assessment cycles; and
- Report on critical infrastructure.

Governance

Cybersecurity Technical Group (GT-Ciber)

Conformity and Certification Schemes

Act nº 77/2021

- **Cybersecurity** • **Requirements for Telecommunications Equipment;**
- **Recommendations to** • manufacturers and suppliers; and
- Market Surveillance **Program.**

Act nº 2.436/2023

- Mandatory • requirements for conformity assessment of CPEs;
- Follow discussions within GT-Ciber; and
- In force from March 2024.







XZZ 00000000





The step-by-step process of ANATEL Certification

Selection of a Designated Certification Body (OCD) (Submission of the technical information about the product to OCD)

Laboratory testing of a product in an INMETRO accredited lab (The laboratory testing is carried out as per the product's testing specifications and needs)

Submission of conformity certificate by OCD to ANATEL (ANATEL reviews the application and issues the certificate of homologation)

ANATEL Stamp

(The product receives an ANATEL stamp including a barcode with the product homologation number)

Maintenance of Certification

(OCD reviews the technical documentation intended to maintain the certificate)

Awareness Initiatives

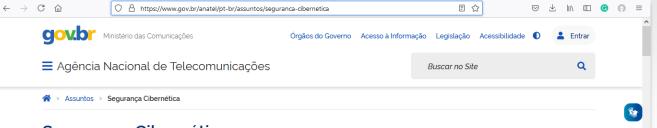


#FiqueEsperto

Dicas de segurança contra diversos tipos de fraudes.

SOMENTE BAIXE APLICATIVOS DE FONTES E





Segurança Cibernética

A segurança cibernética é agenda prioritária da Agência Nacional de Telecomunicações (Anatel) e motivou a edição do Regulamento de Segurança Cibernética aplicada ao Setor de Telecomunicações e do Ato de Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações.

Publicado em 12/05/2021 16h48 Atualizado em 18/05/2021 09h21

Compartilhe: 🫉 🍠 🔗

A segurança cibernética é definida como "ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis", nos termos do Glossário de Segurança da Informação elaborado pelo Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Como se trata de tema transversal, multidisciplinar e multissetorial, a temática da segurança cibernética é abordada em diversos normativos no Brasil, sob

Awareness Initiatives



Playlist Cibersegurança Anatel on Youtube

#Outubrociberseguro



SEGURANÇA DIGITAL

Anatel promove campanha Outubro CiberSeguro

Durante este mês, serão realizadas diversas iniciativas para conscientização da sociedade na proteção e no combate às ameaças on-line

Publicado em 02/10/2023 08h44

Compartilhe: 🛉 X in 🔉 🔗



Simulated cyber defense exercise - EGC 5.0 2023





Completed on October 6 (2023), the Cyber Guardian Exercise (EGC 5.0), organized by the Cyber Defense Command, is considered the largest maneuver to combat digital threats in the Southern Hemisphere. This is a clear demonstration that the country is heavily investing to ensure the security of its networks and systems.

Guia Orientativo de Segurança Cibernética para prestadoras de serviços de telecomunicações - 2023





GUIA ORIENTATIVO DE SEGURANÇA CIBERNÉTICA PARA PRESTADORAS DE SERVIÇOS DE TELECOMUNICAÇÕES

NÍVEL BÁSICO – Versão 1.0 Outubro/2023





Consulte mais informações no guia completo em www.bit.ly/guiaciber2023

- Inventário de Ativos: Gerenciar constantemente os ativos institucionais e softwares, com o objetivo de identificar precisamente quais necessitam ser monitorados, bloqueados e/ou protegidos dentro da empresa.
- Proteção de Dados: Desenvolva processos e controles técnicos para identificar, classificar, manusear com segurança, reter e descartar dados.
- Configuração Segura de Ativos: Defina e mantenha a configuração segura de recursos empresariais (ex: dispositivos móveis; equipamentos e servidores: e programas (ex:sistemas e aplicações).
- Controle de Acesso e Contas: Use processos e ferramentas para atribuir e gerenciar autorização de credenciais, bem como criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas (ex: usuário e admin.)
 - Monitoramento de Atividades e Gestão de Vulnerabilidades e Registros: Monitore as atividades em sua rede e sistemas para identificar possíveis ameaças e ataques, de forma automatizada, sempre que possível. Mantenha um processo de gestão de vulnerabilidades e de registros de auditoria.
 - Backup e Recuperação de Dados: Faça backups regularmente de seus dados críticos e verifique se eles estão funcionando corretamente. Tenha um plano de recuperação para restaurar a funcionalidade em caso de falha do sistema.
- Conscientização de Segurança Cibernética para os Funcionários: Garanta que seus funcionários estejam cientes dos riscos de segurança cibernética e estejam treinados para reconhecer e evitar ameaças.
- Conscientização de Segurança Cibernética para os Consumidores: Fomente um comportamente mais seguro dos seus consumidores para reconhecer e evitar ameaças cibernéticas.
- Segurança Física: Proteja seus sistemas e dados com medidas físicas de segurança, como controle de acesso físico, monitoramento com câmeras e adote uma política de mesa limpa e tela limpa.
- Plano de Resposta a Incidentes: Tenha um plano de resposta a incidentes em vigor para minimizar danos em caso de violação de segurança
- Política de Segurança da Cibernética: Tenha uma política aprovada pela alta gestão, publicadas e comunicadas aos colaboradores relevantes, para nortear a gestão de segurança cibernética na prestadora.

Lembre-se: as ações para aprimorar a segurança cibernética devem ser contínuas. Atualize e aprimore-as regularmente para garantir a proteção da sua prestadora de telecomunicações!



Guia orientativo DevSecOps - 2023



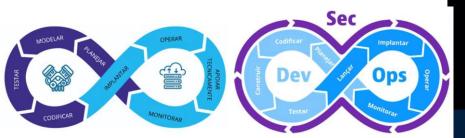
DevSecOps Guia orientativo





Sumário

Lista de Abreviaturas, Acrônimos e Siglas	
Apresentação e Objetivo	3
Introdução	!
Capítulo 1 - Fundamentos de DevSecOps	6
 1.1. Entendendo o conceito de DevOps 1.2. Visão geral do DevSecOps Capítulo 2 - Preparação para a Implementação do DevSecOps 	
 2.1. Avaliação de segurança e conformidade inicial 2.2. Papéis e responsabilidades no DevSecOps. Capítulo 3 - Desenvolvimento Seguro 	9
 3.1. Princípios de segurança e desenvolvimento seguro	1 1
 4.1. Ferramentas de Segurança em uma esteira CI/CD 4.2. Esteira de Desenvolvimento Sugerida 4.3. Gerenciamento de vulnerabilidades e patches Capítulo 5 - Monitoramento e Resposta a Incidentes 	16 18
 5.1. Monitoramento contínuo de segurança 5.2. Detecção e resposta a incidentes Capítulo 6 - Governança e Conformidade	20
 6.1. Políticas de segurança da informação e gerenciamento de acesso 6.2. Auditorias de segurança e conformidade com regulamentações e normas Capítulo 7 - Treinamento e Conscientização 	22
Capítulo 8 - Conclusões	2
8.1. Necessidades Identificadas: Melhoria Contínua e Superação de Obstáculos 8.2. Considerações Finais Referências	26



5G Cybersecurity – Research Cooperation Agreement



- Research and Innovation Project on cybersecurity of telecommunications networks, especially in (5G), also covering legacy networks;
- 20 months;
- Federal University of Campina Grande (UFCG);
- Celebrated in December 2021;
- 3 Perspectives:
 - Basic perspective: identify the main characteristics and dimensions of security in telecommunications networks;
 - Technological perspective; and
 - Economic, Standardization, and Regulatory Perspective.

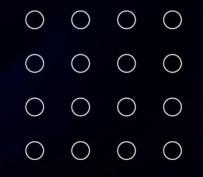


Humberto Pontes

ANATEL

Regulation Specialist GT-Ciber Member

gtciber@anatel.gov.br





www.anatel.gov.br

GT-Ciber



