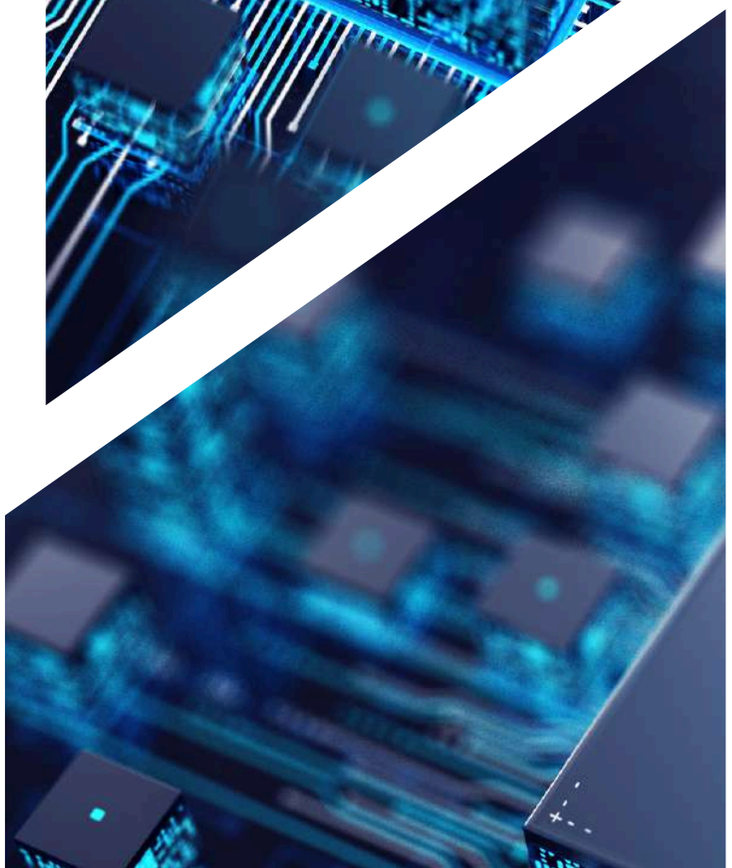
BOAS PRÁTICAS DE CIBERSEGURANÇA E PROTEÇÃO DE DADOS



Introdução

Em um mundo cada vez mais digital, a segurança cibernética e a proteção de dados pessoais se tornaram essenciais para empresas e pessoas. Este eBook aborda os princípios básicos da cibersegurança, as melhores práticas para identificar e reduzir riscos, e como implementar políticas e procedimentos eficazes para proteger informações confidenciais.

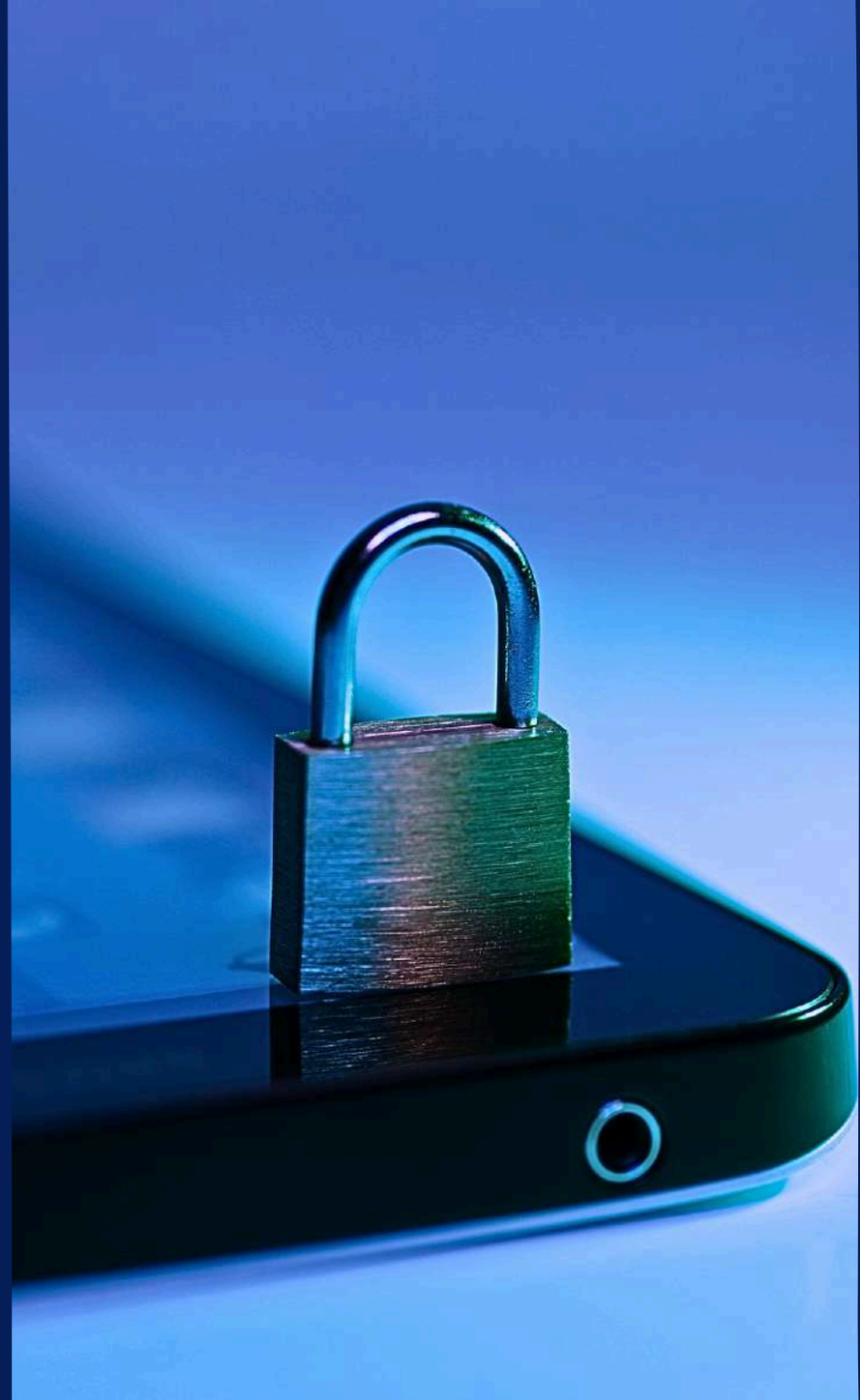
Princípios Básicos de Cibersegurança

1. **Confidencialidade**
Garantir que apenas indivíduos autorizados tenham acesso a informações sensíveis.

2. **Integridade**
Assegurar que os dados não sejam alterados ou corrompidos de forma não autorizada.

3. **Disponibilidade**
Certificar-se de que as informações e sistemas estejam acessíveis aos usuários autorizados quando necessário.

4. **Responsabilidade**
Garantir que todas as atividades em sistemas e redes possam ser rastreadas e atribuídas a indivíduos específicos.



Identificação de Situações de Riscos

Engenharia Social

É uma técnica utilizada para uma vasta gama de atividades maliciosas realizadas através da interação humana. Utiliza a manipulação psicológica para enganar a vítima, levando-a a cometer erros de segurança ou a partilhar informação sensível.

Phishing

É um tipo de ataque cibernético que usa e-mails, mensagens de texto, telefonemas ou sites fraudulentos para enganar as pessoas a compartilhar dados confidenciais, baixar malware ou se expor a crimes cibernéticos de outras formas.

Perigos na Utilização de Redes Wifi Desconhecidas / Públicas

Wifi desconhecidos ou públicos normalmente disponíveis em locais como aeroportos, centros comerciais, restaurantes e etc, costumam ser desprovidos de segurança.

Boas Práticas em Cibersegurança

Não responda e-mails e/ou mensagens de contatos desconhecidos.

Encare como suspeitas mensagens contendo: "Parabéns, você ganhou", "A sua encomenda encontra-se retida" e "Responda agora".

Evite ligar armazenamentos desconhecidos ao seu computador.

Altere periodicamente suas senhas de e-mail, redes sociais e celular.

Evite deixar suas senhas escrita em locais expostos ou a tela do seu computador desbloqueada.

Utilizar, sempre que possível, autenticações de dois fatores - por e-mail, SMS, token, etc. -, uma vez que estas aumentam consideravelmente a segurança da conta.

Em Casos de Incidentes de Segurança

1

Detecção

Identifique rapidamente qualquer atividade suspeita ou violação de segurança.

2

Análise e Contenção

Investigue o incidente, determine o escopo e impacto, e implemente medidas imediatas para conter os danos.

3

Contato

Entre em contato imediatamente com as equipes de LGPD e TI.

4

Aprendizado e Melhoria

Identifique oportunidades de melhoria e aplique as estratégias de cibersegurança no seu dia a dia.

Conclusão e Considerações Finais

À medida em que os golpes digitais se tornam mais sofisticados, a necessidade de prevenção e preparação se torna ainda mais real. Sendo assim, devemos agir agora para fortalecer uma
cultura de defesas cibernéticas, garantindo a segurança do ambiente digital das nossas empresas.

A prevenção é a melhor forma de proteção!

Em Caso de Dúvidas:

Tecnologia da Informação
gerti@grupoatlantica.com.br

LGPD
encarregado@grupoatlantica.com.br