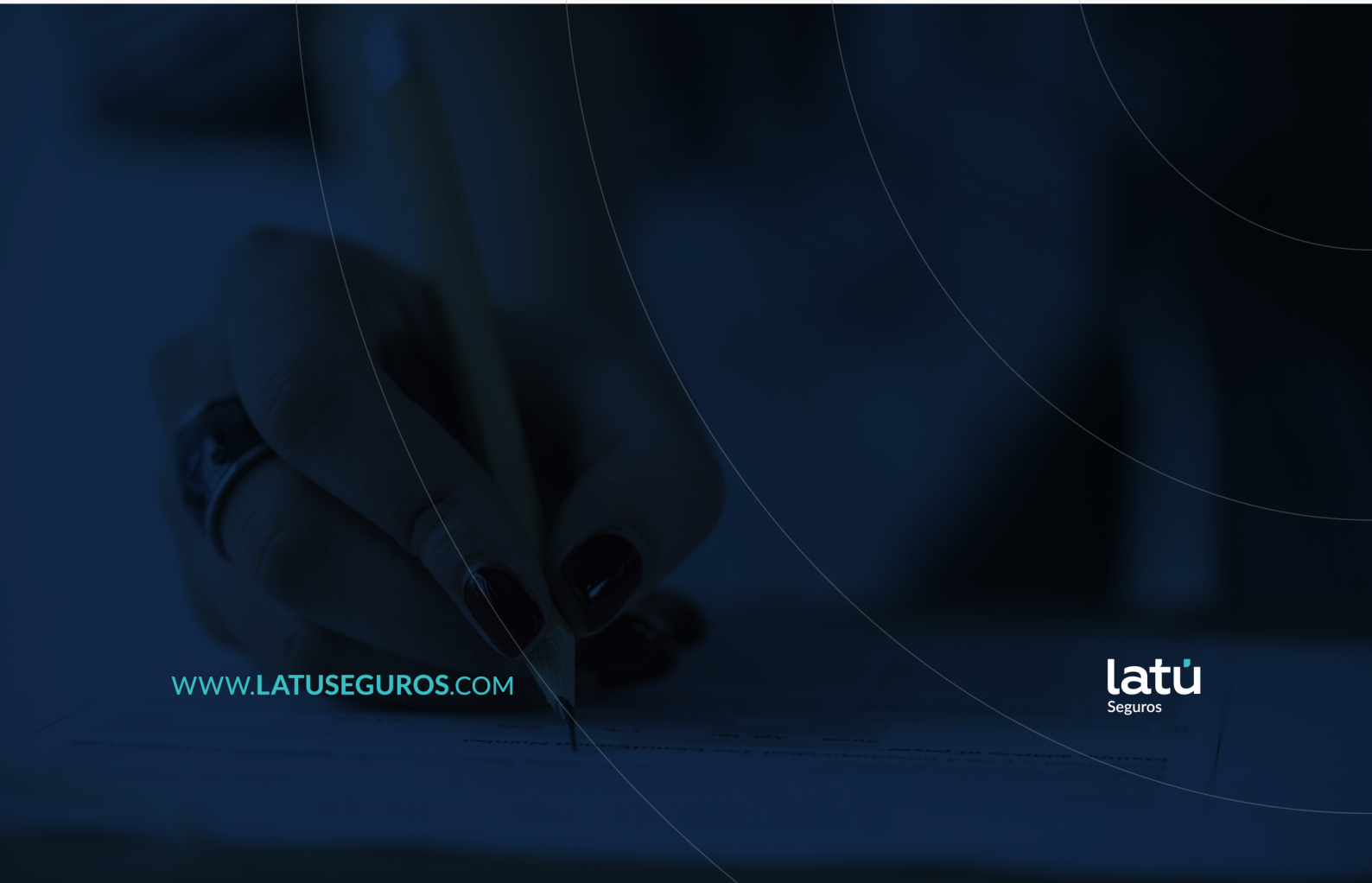
2025

CHECKLISTS ESSENCIAIS DE SEGURANÇA CIBÉRNETICA PARA SUA EMPRESA

Garanta o básico da segurança cibernética
e saiba como agir no caso de um ataque.



WWW.LATUSEGUROS.COM

latú
Seguros

PROTEJA SUA EMPRESA

Comece o ano com **sua empresa à prova de ameaças digitais**, com nossos checklists de segurança cibernética.

Nos dias de hoje, **os ataques cibernéticos estão cada vez mais sofisticados e podem causar danos graves**, desde interrupções nas operações até prejuízos financeiros e danos à reputação da sua empresa. Para evitar que isso aconteça, **é essencial adotar boas práticas de segurança e estar preparado para responder rapidamente em caso de incidentes**.

Pensando nisso, preparamos dois checklists práticos para ajudar sua equipe a garantir o básico da segurança cibernética e saber como agir em caso de um ataque:

01

Medidas preventivas para garantir a segurança da sua empresa.

Uma lista detalhada de medidas preventivas para proteger seus sistemas e dados.

02

O que fazer no caso de um incidente cibernético.

Um guia claro para investigar, conter e remediar qualquer ataque que sua empresa enfrente.

Com estas orientações, sua empresa estará mais **preparada para enfrentar os desafios do mundo digital**.

Dica: Compartilhe esses checklists com sua equipe de TI ou segurança da informação para garantir que todas as etapas sejam cumpridas!

CHECKLISTS ESSENCIAIS DE SEGURANÇA CIBERNÉTICA

Medidas preventivas para garantir a segurança da sua empresa.

Fortaleça a segurança:

- [ ] **Revise e documente as melhorias** implementadas nos últimos 12 meses.
- [ ] **Configure e revise os firewalls** para prevenir acessos não autorizados.
- [ ] Ofereça **treinamento em cibersegurança** para toda a equipe.
- [ ] **Instale antivírus** de nível corporativo em todos os dispositivos.
- [ ] **Ative a verificação multifatorial** (MFA) em todos os acessos aos sistemas.
- [ ] Elabore e teste um **plano de continuidade de negócios** e recuperação de desastres.

Faça **escaneamentos e backups** regulares:

- [ ] **Defina a frequência** dos escaneamentos internos e externos.
- [ ] **Escaneie todos os backups contra malwares** antes de armazená-los.
- [ ] Mapeie e documente os **tipos de dados que sua empresa utiliza** (PII, HIPAA, PCI, etc.).
- [ ] **Realize backups** dos dados da empresa e garanta que provedores em nuvem também o façam, ao menos semanalmente.

Atualize seus sistemas:

- [ ] Estabeleça um **cronograma para instalar patches** críticos.
- [ ] Faça um **inventário detalhado dos dispositivos conectados à rede** (desktops, laptops, dispositivos móveis e servidores).

Atenção a **sistemas legados e acessos remotos**:

- [ ] Identifique sistemas legados ou em fim de vida e **mantenha-os segmentados**.
- [ ] **Garanta que acessos remotos expostos à internet estejam protegidos** com controles, como listas de IP permitidos.

Se alguma dessas ações não estiver implementada, revise com urgência!
Sua empresa pode estar vulnerável.

O que fazer em caso de um incidente cibernético?

Se sua empresa já **tem Seguro Cyber**:

- [ ] Assim que detectar um incidente, **comunique-o imediatamente à seguradora**.

Investigue o incidente:

- [ ] **Documente** o vetor inicial do ataque.
- [ ] Em casos de phishing, **analise o perfil da vítima e seus privilégios** de acesso.
- [ ] Identifique a **plataforma vulnerável explorada**, se aplicável.
- [ ] Determine **quanto tempo o invasor esteve presente** antes de um ataque como ransomware.

Avalie a segmentação e os impactos.

- [ ] Verifique se **sistemas críticos estão devidamente segmentados**.
- [ ] Estime a **quantidade de dispositivos afetados** (desktops, laptops, dispositivos móveis e servidores).

Lide com o **Ransomware**:

- [ ] Determine a **extensão do ataque** (ativos e dados comprometidos).
- [ ] Verifique se os **backups foram afetados** e identifique como.
- [ ] Liste os **tipos de dados exfiltrados** (PII, HIPAA, PCI, etc.).
- [ ] Documente **como os sistemas foram restaurados** após o ataque.

Resposta e contenção:

- [ ] Registre **como o ataque foi contido e o momento da interrupção do acesso**.
- [ ] Indique a **data em que os sistemas voltaram a funcionar**.
- [ ] Anote o **tempo total de interrupção** nos processos críticos.

Prevenção futura:

- [ ] **Detalhe as ações tomadas** para corrigir a vulnerabilidade inicial.
- [ ] Liste **controles adicionais** implementados para evitar reincidências.

Conclusão

Manter sua empresa protegida contra ameaças cibernéticas não é apenas uma questão de tecnologia, mas também de estratégia, prevenção e preparo. Os checklists apresentados neste material são um ponto de partida essencial para **fortalecer suas defesas e garantir que sua equipe saiba como agir em qualquer cenário**.

Lembre-se: a segurança cibernética é um processo contínuo. Revisite essas práticas regularmente, atualize seus protocolos e invista em treinamento para sua equipe. Além disso, considere contratar uma solução de Seguro Cyber para proteger não apenas seus dados, mas também o futuro do seu negócio.

Na Latú, estamos aqui para ajudá-lo a enfrentar os desafios da era digital com confiança e segurança.

Precisa de mais informações ou **deseja saber como o Seguro Cyber pode ser a proteção ideal** para sua empresa? Entre em contato com seu corretor especializado e solicite uma cotação!

Juntos, podemos construir um ambiente mais seguro para sua operação crescer e prosperar.

Conte conosco!