Gabriel Barbosa

Cursando Analise e Desenvolvimento de Sistemas, e certificação Google Cybersecurity.
Exemplo de auditoria a uma empresa fictícia a "Botium Toys". Utilizando a estrutura de segurança cibernética do NIST CSF.

AUDITORIA "**BOTIUM TOYS**"

Objetivo: Encontrar a existência de vulnerabilidades e verificar se os processos internos estão de acordo com as leis.

Recursos a serem avaliados: SPII, PII, recursos físicos, procedimentos organizacionais.

Realizar auditorias colabora para encontrar vulnerabilidades e mitigar riscos que possam comprometer a segurança da empresa, evitando assim receber processos e multas prejudicando a boa imagem da empresa no mercado.

Recomenda -se realizar auditoria de segurança a cada três meses.

Lista de verificação de controles e conformidades.

A Botium Toys possui atualmente esses controles?

Lista de veri cação e avaliação de controles

Sim	*Não*	*Controle*
☐	☑	Menor Privilegio.
☐	☑	Planos de recuperação de desastres.
☐	☑	Politica de Senhas.
☐	☑	Separação de funções.
☐	☑	Firewall.
☑	☐	Sistema de detecção de intrusão (IDS).
☑	☐	Backups
☑	☐	So ware de antivirus.
☐	☑	Monitoramento, manutenção e intervenção manual para sistemas legados.
☐	☑	Criptogra a.
☑	☐	Sistema de gerenciamento de senhas.
☑	☐	Fechaduras (escritórios, armazém)
☐	☑	Vigilância em circuito fechados de vídeo monitoramento.
☑	☐	Detecção / prevenção de incêndio, alarmes de incêndios.

A Botium Toys, atualmente adere a essas práticas de conformidades?

Lista de veri cação de conformidade.

Padrão de segurança de dados da indústria de cartões de pagamentos (PCI, DSS)

Sim	*Não*	*MelhoresPráticas*
☐	☑	Somente usuários autorizados têm acesso às informações do cartão de crédito dos clientes.
☐	☑	As informações do cartão de crédito são armazenadas, aceitas, processadas e transmitidas internamente em um ambiente seguro.
☑	☐	Implementar procedimentos de criptogra a de dados, para proteger melhor os dados e pontos de contato de transações de cartão de crédito.
☐	☑	Adota políticas seguras de gerenciamento de senhas.

Regulamento Geral de proteção de dados (RGPD)

Sim	*Não*	*MelhoresPráticas*
☑	☐	E.U. Os dados dos clientes são mantidos privados / protegidos.
☐	☑	Existe um plano em vigor para comunicar a E.U / clientes dentro de 72 horas se seus dados forem violados ou comprometidos.
☐	☑	Certi que -se que os dados sejam devidamente classi cados e inventariados
☑	☐	Aplica políticas, procedimentos e processos de privacidade para documentar e manter os dados adequadamente.

Controles de sistemas e organizações (SOC type 1, SOC type 2)

Sim	*Não*	*MelhoresPráticas*
☑	☐	Políticas de acesso de usuários são estabelecidas.
☑	☐	Dados con denciais (PII/SPII) são con denciais e privados.
☑	☐	A integridade dos dados garante que os dados sejam consistentes, completos, precisos e validados.
☑	☐	Os dados estão disponíveis para indivíduos autorizados acessá-los.

Relatório de Auditoria:

Constatado sérios riscos à integridade, confiabilidade e disponibilidade a segurança de informações da “Botium Toys”. Vulnerabilidades tanto nos controles técnicos, físicos e administrativos.

Recomenda - se uma forte conscientização e treinamento aos funcionários para ajudar na mitigação de riscos. Analisar, revisar e implementar políticas sólidas ao lidar com recursos valiosos como as PII, SPII, para evitar multas, e preservar a imagem da instituição.