**Atividade: Realize uma auditoria de segurança**

Na primeira parte desta atividade, você realizará uma auditoria de segurança interna, que poderá incluir em seu portfólio de segurança cibernética. Recorde-se que as auditorias ajudam a garantir que são feitas verificações de segurança, para monitorizar ameaças, riscos ou vulnerabilidades que podem afetar a continuidade dos negócios e os ativos críticos de uma organização.

**Cenário**

A Botium Toys é uma pequena empresa norte-americana que desenvolve e vende brinquedos. A empresa possui um único local físico, que funciona como sede, loja e depósito para seus produtos. No entanto, a presença online da Botium Toy cresceu, atraindo clientes nos EUA e no exterior. Como resultado, o seu departamento de tecnologia da informação (TI) está sob pressão crescente para apoiar o seu mercado online em todo o mundo.

O gerente do departamento de TI decidiu que uma auditoria interna de TI precisa ser realizada. Ela expressa preocupação por não ter um plano de ação solidificado para garantir a continuidade e conformidade dos negócios, à medida que o negócio cresce. Ela acredita que uma auditoria interna pode ajudar a proteger melhor a infraestrutura da empresa e ajudá-la a identificar e mitigar potenciais riscos, ameaças ou vulnerabilidades a ativos críticos. O gestor também está interessado em garantir que cumprem os regulamentos relacionados com o processamento interno e a aceitação de pagamentos online e a realização de negócios na União Europeia (UE).

O gerente de TI começa implementando a Estrutura de Segurança Cibernética do Instituto Nacional de Padrões e Tecnologia (NIST CSF), estabelecendo um escopo e metas de auditoria, listando os ativos atualmente gerenciados pelo departamento de TI e concluindo uma avaliação de risco. O objetivo da auditoria é fornecer uma visão geral dos riscos e/ou multas que a empresa pode enfrentar devido ao estado atual de sua postura de segurança.

Sua tarefa é revisar o escopo, as metas e o relatório de avaliação de riscos do gerente de TI. Em seguida, realize uma auditoria interna preenchendo uma lista de verificação de controles e conformidade.

**Passo 1: Acessar o material de suporte**

Arquivo “*Botium Toys Escopo, metas, e avaliação de riscos*”

**Passo 2: Realizar auditoria: controles e lista de verificação de conformidade**

Conduza a próxima etapa da auditoria de segurança preenchendo os controles e a lista de verificação de conformidade.

Para completar a lista de verificação, abra os materiais de apoio fornecidos na Etapa 1. Em seguida:

1. Revise o escopo, as metas e os detalhes do relatório de avaliação de risco, com foco em:
   1. Os ativos atualmente gerenciados pelo departamento de TI
   2. Os marcadores em “Comentários adicionais” na seção Avaliação de risco
2. Considere as informações fornecidas no cenário, o escopo, as metas e o relatório de avaliação de riscos, bem como os detalhes fornecidos em outros documentos vinculados à lista de verificação.
3. Em seguida, revise a pergunta nas seções de controles e conformidade da lista de verificação e selecione “sim” ou “não” para responder à pergunta em cada seção (observação: a seção de recomendações é opcional).

Arquivo “*Controles e lista de verificação de conformidade”*

**O que incluir em sua resposta**

Certifique-se de abordar os seguintes elementos em sua atividade concluída:

Lista de verificação de controles e conformidade

* “Sim” ou “não” é selecionado para responder à pergunta relacionada a cada controle listado
* “Sim” ou “não” é selecionado para responder à pergunta relacionada a cada melhor prática de conformidade

Uma recomendação é fornecida ao gerente de TI (opcional)

**Exemplo Concluído**

Arquivo “*Controles e lista de verificação de conformidade (Exemplar)*”

**Avaliação do Exemplo**

Compare o exemplar com sua atividade concluída. Revise seu trabalho usando cada um dos critérios do exemplar. O que você fez bem? Onde você pode melhorar? Use suas respostas para revisar seu projeto conforme necessário e orientá-lo à medida que avança no programa de certificação.

**Nota**: O exemplar representa uma forma possível de realizar a atividade. O seu provavelmente será diferente em alguns aspectos. O importante é que sua atividade demonstre sua capacidade de selecionar controles que a Botium Toys precisa ou não implementar e cumprir as melhores práticas que a empresa precisa aderir para mitigar riscos e evitar multas.