Avaliação de controles

Ativos correntes

Os ativos geridos pelo Departamento de TI incluem:

- Equipamento local para necessidades de negócios no escritório
- Equipamentos de funcionários: dispositivos de usuário final (desktops/laptops, smartphones), estações de trabalho remotas, fones de ouvido, cabos, teclados, mouses, docking station, câmeras de vigilância, etc.
- Gestão de sistemas, software e serviços: contabilidade, telecomunicações, banco de dados, segurança, comércio eletrônico e gestão de estoque
- Acesso à internet
- Rede interna
- Gerenciamento de acesso do fornecedor
- Serviços de hospedagem de data center
- Retenção e armazenamento de dados
- Leitores de crachás
- Manutenção do sistema legado: sistemas em fim de vida que requerem monitoramento humano

Controles Administrativos			
Nome do controle	**Tipo de controle e explicação**	**Precisa ser implementado (X)**	**Prioridade**
Ultimo privilégio	Preventiva; reduz o risco, garantindo que fornecedores e funcionários não autorizados tenham acesso apenas aos ativos/dados de que precisam para realizar seus trabalhos	X	Alta
Planos de recuperação de desastres	Corretivo; continuidade de negócios para garantir que os sistemas sejam capazes de funcionar em caso de	X	Alta

Controles Administrativos			
	incidente/não haja perda de produtividade, tempo de inatividade/impacto nos componentes do sistema, incluindo: ambiente da sala de informática (ar condicionado, fonte de alimentação, etc.); hardware (servidores, equipamentos de funcionários); conectividade (rede interna, sem fio); aplicativos (e-mail, dados eletrônicos); dados e restauração		
Políticas de senha	Preventiva; estabelecer regras de força de senha para melhorar a segurança/reduzir a probabilidade de comprometimento da conta por meio de força bruta ou técnicas de ataque de dicionário	X	Alta
Políticas de controle de acesso	Preventiva; aumentar a confidencialidade e a integridade dos dados	X	High
Políticas de gerenciamento de contas	Preventiva; reduzir a superfície de ataque e limitar o impacto geral de funcionários insatisfeitos/ex-funcionários	X	Alta/Média
Separação de deveres	Preventiva; garantir que ninguém tenha tanto acesso que possa abusar do sistema para ganho pessoal	X	Alta

Controles técnicos			
Nome do controle	**Tipo de controle e explicação**	**Precisa ser implementado (X)**	**Prioridade**
Firewall	Preventiva; já existem firewalls para filtrar o tráfego indesejado/malicioso de entrar na rede interna	X	Alta
Sistema de Detecção de Intrusão (IDS)	Detetive; permite que a equipe de TI identifique possíveis invasões (por exemplo, tráfego anômalo) rapidamente	X	Alta
Criptografia	Dissuasor; torna as informações/dados confidenciais mais seguros (por exemplo, transações de pagamento no site)	X	Alta
Backups	Corretivo; apoia a produtividade contínua no caso de um evento; se alinha ao plano de recuperação de desastres	X	Alta/Média
Sistema de gerenciamento de senhas	Corretivo; recuperação de senha, redefinir, bloquear notificações	X	Alta
Software antivírus (AV)	Corretivo; detectar e colocar em quarentena ameaças conhecidas	X	Média/Baixa
Monitoramento manual, manutenção e intervenção	Preventiva/corretiva; necessário para que os sistemas legados identifiquem e mitiguem ameaças, riscos e vulnerabilidades potenciais	X	Média/Baixa

Controles Físicos			
Nome do controle	**Tipo de controle e explicação**	**Precisa ser implementado (X)**	**Prioridade**
Cofre controlado por tempo	Dissuasor; reduzir a superfície de ataque/impacto de ameaças físicas	X	Alta/Média
Iluminação adequada	Dissuasor; limitar os “esconderijos” para impedir ameaças	X	Baixa
Vigilância por circuito fechado de televisão (CCTV)	Preventivo/detetive; pode reduzir o risco de certos eventos; pode ser usado após o evento para investigação	X	Média/Baixa
Armários de travamento (para equipamentos de rede)	Preventiva; aumentar a integridade impedindo que pessoas/indivíduos não autorizados acessem/modifiquem fisicamente equipamentos de infraestrutura de rede	X	Média
Sinalização indicando prestador de serviço de alarme	Dissuasor; faz com que a probabilidade de um ataque bem-sucedido pareça baixa	X	Baixa
Armários	Preventiva; ativos físicos e digitais são mais seguros	X	Média/Baixa
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detecção e prevenção de incêndios (alarme de incêndio, sistema de sprinklers, etc.)	X	Baixa

Lista de verificação de conformidade

☐ **A Comissão Reguladora Federal de Energia - North American Electric Reliability Corporation (FERC-NERC)**

O regulamento FERC-NERC se aplica a organizações que trabalham com eletricidade ou que estão envolvidas com a rede elétrica dos EUA e da América do Norte. As organizações têm a obrigação de se preparar, mitigar e relatar qualquer possível incidente de segurança que possa afetar negativamente a rede elétrica. As organizações são legalmente obrigadas a aderir aos Padrões de Confiabilidade de Proteção de Infraestrutura Crítica (CIP) definidos pelo FERC.

Explicação: S/N

☑ **Regulamento Geral de Proteção de Dados (GDPR)**

GDPR é um regulamento geral de dados da União Europeia (E.U.) que protege o processamento de dados da E.U. dados dos cidadãos e seu direito à privacidade dentro e fora da UE território. Além disso, se ocorrer uma violação e um E.U. os dados do cidadão forem comprometidos, eles devem ser informados em até 72 horas após o ocorrido.

Explicação: A Botium Toys precisa aderir ao GDPR porque conduz negócios e coleta informações pessoais de pessoas em todo o mundo, incluindo a UE.

☑ **Padrão de segurança de dados do setor de cartões de pagamento (PCI DSS)**

O PCI DSS é um padrão de segurança internacional destinado a garantir que as organizações que armazenam, aceitam, processam e transmitem informações de cartão de crédito o façam em um ambiente seguro.

Explicação: A Botium Toys precisa aderir ao PCI DSS porque armazena, aceita, processa e transmite informações de cartão de crédito pessoalmente e online.

☐ **A Lei de Portabilidade e Responsabilidade de Seguro Saúde (HIPAA)**

HIPAA é uma lei federal estabelecida em 1996 para proteger as informações de saúde dos pacientes dos EUA. Esta lei proíbe que as informações do paciente sejam compartilhadas sem o seu consentimento. As organizações têm a obrigação legal de informar os pacientes sobre uma violação.

Explicação: NA

☑ **Controles de Sistema e Organizações (SOC tipo 1, SOC tipo 2)**

O SOC1 e o SOC2 são uma série de relatórios que se concentram nas políticas de acesso do usuário de uma organização em diferentes níveis organizacionais. Eles são usados para avaliar a conformidade financeira e os níveis de risco de uma organização. Eles também cobrem confidencialidade, privacidade, integridade, disponibilidade, segurança e segurança geral dos dados. Falhas de controle nessas áreas podem levar a fraudes.

Explicação: A Botium Toys precisa estabelecer e aplicar o acesso de usuário apropriado para pessoal interno e externo (fornecedor terceirizado) para mitigar riscos e garantir a segurança dos dados.