**Exercício**

**1.** Qual a importância da informação para a sociedade?

Atualmente, a informação é um ativo importantíssimo, que requer cuidados dos especiais e restrições de acessos, por ser um ativo intangível e abstrato, podendo facilmente sair da empresa em uma lata de lixo, na memória de alguém, em meio magnético, impressa em papel, enfim, é um ativo muito vulnerável, logo, demanda cuidados.

**2.** Conceitue Informação.

São ativos que, como qualquer outro ativo importante para os negócios, possuem valor para uma organização e consequentemente precisam ser protegidos adequadamente.

**3.** Elabore um conceito de Segurança da Informação.

É a proteção das informações contra uma ampla gama de ameaças para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidade comerciais.

**4.** Identifique os objetivos do Departamento de Segurança da Informação em uma empresa.

Basicamente, as atividades pertinentes a esse setor envolvem a criação, implementação, controle e monitoramento de políticas que almejam assegurar os ativos de informação de uma empresa ou pessoa.

**5.** Quais os princípios da segurança da informação? Defina-os. Cite alguns riscos aos quais as pessoas estão sujeitas ao utilizar a Internet.

**• Confidencialidade**

Garante que somente pessoas autorizadas poderão acessar as informações. Trata-se da não permissão da divulgação de uma informação sem prévia autorização.

**• Disponibilidade**

Garante acesso a uma informação no momento desejado. Isso implica no perfeito funcionamento da rede e do sistema. Imagine você necessitando de umas informações para concluir um relatório e o sistema não está funcionando!

**• Integridade**

Garante que a exatidão e completeza das informações não sejam alteradas ou violadas. Um exemplo, vamos supor que um gerente de uma empresa determina aumento de salário de 2% aos funcionários, para isso, utilizou

seu e-mail para o departamento financeiro. Alguém interceptou e alterou de 2% para 20% o aumento!!!

Ao acessar a Internet, sua máquina já está exposta na rede, você poderá ter seus dados pessoais expostos, e caso sejam acessados por alguém mal intencionado, isso poderá lhe proporcionar grandes transtornos.

Uma pessoa, uma vez com seus dados, poderá querer se passar por você na rede e usar sua identidade até mesmo para lhe expor, colocando em risco a sua reputação, ou cometer crimes como, estelionato, sequestro, pedofilia.

**6.** Leia as afirmações e assinale a alternativa correta.

**a)** Quando os princípios da segurança da informação são violados e há interrupção dos processos normais de negócio, denomina-se Incidente. <- alternativa correta

**b)** Ativo é conhecido como tudo que tem valor para a organização e, uma vez violados, não trarão impactos relevantes para a empresa.

**c)** As falhas podem ser apenas humanas e causadas de forma intencional.

**d)** Quando as atividades são interrompidas na empresa em decorrência de um furacão, essa interrupção é entendida como risco.

**7.** Explique a importância de um Plano de Recuperação de Desastre para as empresas.

Um Plano de Recuperação de Desastre (PRD) é um conjunto de procedimentos e estratégias que uma empresa desenvolve para lidar com possíveis desastres que possam afetar suas operações, como incêndios, inundações, terremotos, ataques cibernéticos, entre outros. A importância de um PRD para as empresas pode ser vista em diversos aspectos:

1. Minimizar os impactos do desastre: com um PRD, a empresa estará preparada para agir rapidamente e minimizar os impactos do desastre em suas operações, reduzindo o tempo de inatividade e evitando perdas financeiras.
2. Proteger os dados e informações da empresa: muitas empresas dependem de dados e informações críticas para suas operações, e um desastre pode colocar em risco a integridade desses dados. Com um PRD, a empresa pode estabelecer medidas de segurança e backup para garantir a proteção dessas informações.
3. Manter a reputação da empresa: um desastre pode afetar negativamente a reputação de uma empresa, especialmente se não houver um plano adequado de resposta. Com um PRD, a empresa pode mostrar que está preparada para lidar com situações difíceis e minimizar os impactos sobre seus clientes e parceiros.
4. Atender aos requisitos regulatórios: em muitos setores, as empresas são obrigadas por lei a ter um PRD em vigor. Não ter um PRD pode resultar em multas e sanções, além de colocar em risco a licença da empresa para operar.
5. Promover a segurança dos funcionários: um PRD também deve incluir medidas para garantir a segurança dos funcionários da empresa em caso de desastre. Isso inclui evacuação, primeiros socorros e outras medidas de segurança.

Em resumo, um Plano de Recuperação de Desastre é fundamental para garantir a continuidade dos negócios em caso de imprevistos. Além disso, pode ajudar a proteger a empresa de possíveis perdas financeiras, danos à reputação e impactos negativos sobre os funcionários e clientes.

8.Que cuidados as empresas devem ter ao contratar um novo funcionário?

Conferindo os documentos e referências apresentados, propor treinamento adequado aos funcionários, deixando claras as diretrizes de segurança da empresa.

**9.** O que você entende por problemas de acesso lógico?

Além de acessos indevidos, podem ocorrer falhas em algum programa que a empresa utiliza para realizar suas atividades diárias, podendo ficar indisponível para a realização das operações por algumas horas ou mesmo até dias.

Esses problemas geralmente estão relacionados a erros que o próprio programa contém, não garantindo a integridade da base de dados e podem ocorrer também quando o computador está infectado com algum tipo de vírus de computador ou outra forma de ataque.

Os controles nada mais são que barreiras que tentam restringir ou limitar o acesso de pessoas não autorizadas ao sistema da empresa.

Alguns recursos que devem ser protegidos pelo controle de acesso lógico são: os arquivos-fontes, sistemas operacionais e os aplicativos instalados na máquina, sendo definidos pela ISO/IEC 17799.

**10.** Cite alguns cuidados que o setor de Tecnologia da Informação deve tomar para fazer o reconhecimento e autenticação do usuário no sistema.

Integrar a esse sistema de autenticação, soluções melhor elaboradas, dificultando a quebra.

Nesse sentido, instrumentos físicos – hardware – dão suporte a esse mecanismo de segurança. Como exemplos, temos: os recursos da certificação digital, palavras-chaves, cartões inteligentes e os recursos da biometria.

**11.** Por que fazer o controle dos funcionários que gerenciam os privilégios os usuários? Explique.

Fazer o controle dos funcionários que gerenciam os privilégios dos usuários é importante para garantir a segurança da rede e dos dados da empresa. Os funcionários que gerenciam os privilégios dos usuários têm acesso a informações críticas da empresa e podem conceder ou revogar privilégios para outros usuários. Se esses funcionários não forem monitorados e controlados adequadamente, podem ocorrer situações de abuso de privilégios ou vazamento de informações.

Algumas das principais razões pelas quais é importante fazer o controle dos funcionários que gerenciam os privilégios dos usuários incluem:

1. Prevenção de abuso de privilégios: se um funcionário mal-intencionado ou descuidado tiver acesso aos privilégios dos usuários, poderá conceder privilégios a outros usuários sem a devida autorização, o que pode levar a um acesso não autorizado a informações críticas ou ações prejudiciais ao sistema.
2. Proteção contra ataques internos: funcionários com acesso aos privilégios dos usuários podem se tornar alvos de ataques internos, como ameaças de roubo de dados ou extorsão. Ao monitorar e controlar esses funcionários, a empresa pode reduzir o risco de ataques internos.
3. Conformidade com regulamentações: em muitos setores, as empresas são obrigadas por lei a manter registros de quem tem acesso aos dados da empresa e quem os gerencia. Monitorar e controlar os funcionários que gerenciam os privilégios dos usuários pode ajudar a garantir a conformidade com essas regulamentações.
4. Redução de riscos: controlar e monitorar os funcionários que gerenciam os privilégios dos usuários pode ajudar a identificar e reduzir riscos de segurança cibernética. Ao limitar o acesso aos dados e sistemas críticos apenas aos funcionários autorizados, a empresa pode reduzir o risco de perda de dados e danos à reputação.

Em resumo, o controle dos funcionários que gerenciam os privilégios dos usuários é fundamental para garantir a segurança da rede e dos dados da empresa. Ele ajuda a prevenir abuso de privilégios, proteger contra ataques internos, garantir a conformidade com regulamentações e reduzir riscos de segurança cibernética.

**12.** Cite duas tecnologias de identificação e autenticação de usuários.

Biometria e certificados digitais.