AF – Gabarito: Norma IEC 27002

1. A lei vigente que exige a notificação de incidentes de segurança é a LGPD.

   O procedimento está baseado na notificação imediata de eventos ou fragilidades de situações que envolvem: falhas em controles de segurança, erros humanos violações de disponibilidade, confidencialidade e integridade, não conformidade com políticas, violações de segurança física, mudanças descontroladas de sistemas, mau funcionamento de *software* e *hardware*, violáceos de acesso e fragilidades de sistemas.

   Caso tenha dificuldade, consulte o material: seção 16.1.2 e 16.1.3 (pag. 84 e 85 da norma IEC 27002).

2. Primeiro é muito importante o princípio do mínimo privilégio para evitar ser vítima fácil de *malwares*, porque o usuário é inexperiente e clica de maneira inadvertida em *links* ou executáveis de origem perigosa/desconhecida.

   Outro aspecto muito importante é evitar a perda de controle com relação ao que pode ser instalado para violar as políticas da própria organização ou violar leis de direitos autorais (pactuando pirataria) e outros riscos que podem levar a incidentes de segurança.

   Caso tenha dificuldade, consulte o material: seção 12.6.2 (pag. 59 da norma IEC 27002).

3. O programa de conscientização e educação em segurança da informação deve ser regular e assumido pela direção da organização.

   O treinamento deve deixar claro as regras e obrigações de segurança, de acordo com as políticas, normas, leis, regulamentações, contratos e acordos.

   Também, é preciso deixar claro a responsabilidade pessoal de cada um por seus atos e missões, e compromissos para com a informação da organização ou externa.

   Evidentemente, procedimentos básicos com notificação de incidentes e controles relacionados a senhas, controles contra *malwares*, devem ser abordados no treinamento.

   Materiais e recursos adicionais que podem utilizados para segurança da informação.

   Caso tenha dificuldade, consulte o material: seção 7.2.2 (pag. 13 da norma IEC 27002).

4. É importante considerar as leis, no caso a LGPD e lei 12.737 porque é feito menção explicita a não divulgação de dados. Outro aspecto importante é que este termo deve ser redigido, assinado, ... porque a tecnologia (controles de segurança não conseguem fazer isto bem por si só).

   O termo deve levar em consideração os seguintes elementos/requisitos: definição da informação a ser protegida, tempo de duração do acordo; ações no encerramento do acordo; responsabilidades; usos permitidos; direito de auditoria das informações confidenciais; processo de notificação de vazamento. É importante notar que é feita menção explicita com relação as responsabilidades dos signatários no termo, assim há conformidade explicita com o que pede a lei LGPD.

Caso tenha dificuldade, consulte o material: seção 13.2.4 (pag. 66 da norma IEC 27002).