Checklists para verificação de política e plano de *backup*

A norma ABNT NBR ISO/IEC 27002:2013 fornece diretrizes para gestão de segurança da informação, levando em consideração os ambientes de risco das organizações. A norma foi projetada para ser usada como referência na seleção e implementação de controles de segurança da informação comumente aceitos.

De acordo com o item 12.3.1 da norma, cópias de segurança (*backups*) de dados e de sistemas devem ser efetuadas e testadas regularmente conforme uma política previamente definida. Este *checklist* de política e de plano de *backup* foi definido conforme as diretrizes para implementação relacionadas nesse mesmo item da ABNT NBR ISO/IEC 27002:2013.

--> *Checklist* para verificação de política de *backup*

#	Verificar se	S/N	Observações/ evidências
1	Existe uma política de *backup* (ou instrumento normativo equivalente) formalmente estabelecida		
2	A política foi publicada/comunicada para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)		
3	A política estabelece que planos/procedimentos/roteiros de *backup* de dados e de sistemas específicos devem ser definidos para atender as necessidades de negócio e/ou requisitos da organização		
4	A política estabelece que as cópias de segurança devem ser testadas regularmente por meio de testes de recuperação/restauração (*restore*), a fim de detectar eventuais falhas lógicas e físicas (nas mídias de armazenamento)		
5	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir requisitos específicos de segurança da informação* paras as cópias de segurança realizadas (ex.: controles de acesso lógico, uso de criptografia, armazenamento em local seguro, armazenamento em local remoto seguro diferente do local original etc.) ** Requisitos de segurança da informação referem-se, em especial, à confidencialidade, à integridade e à disponibilidade das informações. Porém, como esses termos podem não ser citados na política, é preciso focar nos exemplos citados acima ou, então, checar se a política registra a necessidade de os controles serem compatíveis com a segurança das informações ou com a classificação das informações.*		
6	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir a abrangência/escopo das cópias de segurança de dados e de sistemas (ou seja, aquilo que deve ser copiado, incluindo indicações de datas/períodos) Ex.: quais arquivos de dados ou de sistema, quais bases de dados, quais tabelas, quais pastas/*folders* etc.		
7	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir a frequência de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.)		
8	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir os tipos de cópias a serem realizadas (completa/*full*, incremental ou diferencial)		
9	A política estabelece que os planos/procedimentos/roteiros de *backup* devem definir o tempo de retenção das cópias de segurança, inclusive com base em requisitos legais		

--> *Checklist* para verificação de plano (ou procedimento/roteiro) de *backup* específico

{especificar o nome da base de dados, arquivo de dados, sistema, aplicativo, servidor etc.}

#	Verificar se	S/N	Observações/ evidências
1	O plano foi publicado/comunicado para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)		
2	O plano foi aprovado pelas partes interessadas		
3	O plano registra/define de modo completo e exato a abrangência/escopo das cópias de segurança (ou seja, aquilo que deve ser copiado, incluindo indicações de datas/períodos) [diretrizes para implementação, alínea "a"] Ex.: quais arquivos de dados ou de sistema, quais bases de dados, quais tabelas, quais pastas/*folders* etc.		
4	O plano estabelece que seja monitorada e documentada a execução do procedimento de geração das cópias de segurança, por meio de registros (*logs*) relativos a todos os itens copiados, a fim de detectar eventuais falhas e assegurar que houve a realização integral das cópias de segurança		
5	O plano documenta os procedimentos para realizar a recuperação/restauração (*restore*) das cópias de segurança quando necessário (ou seja, o "como" recuperar os *backups*) [diretrizes para implementação, alínea "a"]		
6	O plano define a frequência de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.) [diretrizes para implementação, alínea "b"]		
7	O plano define os tipos de cópias a serem realizadas (completa/*full*, incremental ou diferencial) [diretrizes para implementação, alínea "b"]		
8	O plano define o tempo de retenção das cópias de segurança		
9	O plano define requisitos específicos de segurança da informação* (ex.: controles de acesso lógico, uso de criptografia etc.) [diretrizes para implementação, alíneas "b" e "f"] ** Requisitos relativos à confidencialidade, à integridade e à disponibilidade das informações*		
10	O plano define a necessidade de armazenamento das cópias de segurança em local seguro e em local remoto seguro diferente do local original [diretrizes para implementação, alíneas "c" e "d"]		
11	O plano define procedimentos regulares de teste de recuperação/restauração (*restore*) das cópias de segurança, a fim de detectar tempestivamente eventuais falhas lógicas e físicas (nas mídias de armazenamento) [diretrizes para implementação, alínea "e"]		
12	O plano estabelece que a execução dos procedimentos de teste de recuperação/restauração (*restore*) das cópias de segurança seja documentada por meio de registros (*logs*) relativos a todos os itens restaurados, a fim de detectar eventuais falhas e assegurar que houve a recuperação integral das informações		