Anexo 5 - Requisitos de segurança de hospedagem de dados

Estes requisitos se aplicam à hospedagem de todos os aplicativos e dados **Confidenciais (IC)** ou **Estritamente confidenciais (ISC)** da BT que estejam localizados em qualquer local que não seja de propriedade da BT ou por ela gerenciado. Isto inclui, mas não está limitado a, serviços em nuvem onde a) os dados em trânsito normalmente sejam seguros e protegidos contra interceptação através de um protocolo criptografado; e b) os dados da BT sejam criptografados em repouso dentro do serviço em nuvem.

As condições a seguir se aplicam a aplicativos Confidenciais e a dados hospedados fora da BT:

- A Central de Dados deve ter uma certificação ISO 27001 válida (ou certificações que demonstrem controles equivalentes) de gestão de segurança ou deve estar em conformidade com as Exigências de Segurança da certificação ISO 27001 ou com as políticas de segurança alinhadas à ISO 27001 e/ou esteja trabalhando para adquirir a certificação ISO 27001 dentro de um prazo acordado junto à BT;
- Dados “em trânsito” devem ser rigorosamente criptografados para proteger os dados da BT entre o ponto de saída da BT e o limite da central de dados (normalmente o balanceamento de carga e o dispositivo de descriptografia localizados atrás do firewall de limite da central de dados);
- Os engenheiros da central de dados com acesso físico aos servidores não podem ter acesso lógico ao ambiente de produção e os administradores com acesso lógico aos sistemas não devem ter acesso físico à central de dados;
- Todo o acesso lógico deve ser controlado por um sistema de segurança de conta que garanta que a gestão de senhas seja controlada e que o processo de autorização apropriado seja implementado de forma a garantir a identidade do solicitante, ex: CyberArk;
- Para acesso privilegiado (inclusive, mas não restrito a DBA), a gestão de senhas deve ter tempo limite e, sempre que possível, restrições adicionais devem ser implementadas no endereço IP de origem;
- Todo acesso privilegiado, ex: DBA, ASG, etc. aos sistemas que processam informações da BT deve estar em conformidade com as exigências do Anexo 1 - classificação de informações;
- Para acesso remoto, uma Rede Privada Virtual deve ser usada junto a uma autenticação de função baseada em dois fatores; além disso, todo acesso privilegiado remoto de terceiros deve acessar apenas os sistemas em que os dados da BT estejam em trânsito ou em repouso dentro do mesmo país da central de dados, ou um país ou território que garanta um nível adequado de proteção para os dados da BT;
- Implemente processos de gestão de chaves criptográficas para a vida toda comensuráveis com as melhores práticas da indústria;
- Todo acesso físico às áreas ou aos equipamentos em que as informações da BT estão armazenada ou são processadas devem ter um processo auditável, ex. solicitação de alteração, para garantir que o acesso só seja concedido pela duração mínima necessária, ex: acesso não permanente;
- O armazenamento de dados de backup fora do local deve ser criptografado de acordo com as exigências do Anexo 1;

- Os controles devem estar em vigor para mitigar, detectar e evitar o acesso não autorizado. Os controles devem criar uma trilha de auditoria usando o princípio “Quem, o que, onde e quando”.
- Quem era o usuário, ex: Identificação da conta do usuário;
- Qual ativo estavam acessando, ex: dados;
- De onde estavam acessando o ativo, ex: endereço IP; e
- Quando, ex. carimbo de hora.
- Todo acesso físico e lógico deve ser registrado e os arquivos de registro devem ficar retidos por 1 ano (mínimo);
- Em caso de violação em que os dados da BT sejam comprometidos, roubados ou alterados, deve ser realizado um processo para garantir que a BT seja informada dentro de um prazo razoável e com um nível suficiente de detalhes;

Quando houver informações ISC, o que segue também se aplica -

- A Central de dados deve passar por uma inspeção de segurança no local;
- Os servidores de aplicativos, de base de dados e etc. devem ficar em uma infraestrutura dedicada e não alugada por diversas empresas e devem ficar hospedados em um rack dedicado dentro de uma gaiola de segurança. Quando esta exigência não puder ser atendida, deve ser realizada uma avaliação de risco da BT demonstrando a separação adequada dos dados da BT dos dados de outros clientes que compartilham o mesmo ambiente, garantindo que as DBAs não tenham login de acesso às instâncias dos clientes e não vejam os dados dos clientes de forma conjunta. As tabelas e as linhas da base de dados não devem refletir a visualização da instância de um único cliente;
- Devem ser implementados processos que garantam que os dados ISC sejam excluídos de forma segura ao final de seu ciclo de vida na nuvem; Todos os dispositivos de armazenamento que contenham dados ISC devem ser removidos/excluídos conforme especificado no Anexo 1.