Requisitos de hospedagem de dados externos de terceiros

As seguintes condições devem ser cumpridas quando os dados BT são

- Hospedados num ambiente externo (Centro de Dados não BT)
- Transferidos entre Centros de Dados (CD) (Centros de Dados não BT)
- Transferidos entre Centros de Dados e as instalações de cópia de segurança. (Centro de dados não BT)

Aplica-se a todos os dados «Confidenciais» (IC) da BT, «Muito Confidenciais» (ISC) da BT e dados pessoais da BT. Consulte as Especificação de Manipulação e Classificação de Informações de Terceiros http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm para obter definições. Existem controlos adicionais para Dados Pessoais Sensíveis.

Ref	Controlo	Razão
EDH20	Se a hospedagem externa ficar comprometida e os dados da BT forem roubados ou modificados, deve ser implementado um processo para garantir que a BT seja notificada de acordo com o contrato, com um nível de detalhe suficiente de acordo com os Requisitos Mínimos de Segurança da BT e com a condição de «proteção de Dados Pessoais» quando há processamento de dados pessoais.	Para garantir que a BT seja rapidamente informada dum potencial incidente / roubo de dados.
EDH30	O Centro de Dados deve possuir um certificado ISO 27001 válido para gestão de segurança (ou certificação(s) que demonstrem controlos equivalentes, suportados por relatório de auditores independentes)	A ISO27001 demonstra que um quadro de boas práticas de gestão de risco de informações está em vigor.
EDH60	A gestão de chaves criptográficas deve atender aos requisitos do Padrão de Criptografia na Especificação de Manipulação e Classificação de Informações de Terceiros http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Melhores práticas de criptografia
EDH70	O acesso lógico de utilizadores para fins de administração deve depender da função e usar a autenticação de 2 fatores que seja padrão no sector, por exemplo, tokens de palavra-passe de utilização única ou certificados emitidos por autoridades de certificação raiz confiáveis e reconhecidas. Listas e ficheiros de autoridades de certificação raiz confiáveis podem ser encontrados em - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/	Um controle de acesso fraco pode resultar em acessos não autorizados.
EDH90	A administração de aplicações ou dados hospedados externamente deve ser feita através de uma ligação segura (criptografada) e usar a autenticação de 2 fatores conforme EDH70.	Para garantir que o suporte ao acesso remoto é tão seguro quanto o acesso local.
EDH100	Qualquer acesso direto remoto aos dados em que os dados BT estão em trânsito ou em repouso deve ser feito a partir do mesmo país do Data Center ou num país ou território que garanta um nível adequado de proteção para os dados da BT. Qualquer acesso fora do local deve ser feito a partir do mesmo país do Data Center ou num país ou território que garanta um nível adequado de proteção para os dados da BT	Para minimizar o risco de não cumprir as leis de proteção de dados do país ou de haver processamento de dados Confidenciais em zonas suspeitas para a BT.
EDH110	Qualquer acesso (físico ou lógico) para o controlo de mudanças ou a investigação de falhas / remediação deve ter um pedido de alteração ou um ticket de falha. Esse acesso só deve ser concedido durante a duração da mudança / falha e removido posteriormente.	Para minimizar o risco de mudanças não autorizadas serem feitas.

EDH130	O armazenamento de dados de cópia de segurança deve ser criptografado no nível do meio, por exemplo, fita, discos, etc., de acordo com o padrão de encriptação da Especificação de Manipulação e Classificação de Informações de Terceiros http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	Para proteger os dados da BT e minimizar o risco de não cumprir as leis de proteção de dados do país