Domande per chi sviluppa il vostro software

Le domande che seguono aiutano a valutare se i sistemi sviluppati e gestiti da un fornitore resterebbero utilizzabili anche in sua assenza. Non richiedono competenze tecniche. Sotto ciascuna è indicato, in breve, che cosa caratterizza una buona risposta; lo spazio a destra serve per annotare la risposta ricevuta. Una risposta incompleta non è un giudizio sul fornitore: indica un punto da chiarire e, se necessario, da scrivere nel contratto.

Azienda

Fornitore

Sistema

Data del colloquio

	DOMANDA	RISPOSTA DEL FORNITORE
1	**Dove si trova la documentazione del sistema, e quando è stata aggiornata l'ultima volta?** **Una buona risposta:** un luogo accessibile anche all'azienda e una data recente; la documentazione indica dove è installata ogni parte del sistema, quali servizi esterni utilizza e come si ripristina.	
2	**Chi custodisce le chiavi di accesso, e dove sono conservate?** **Una buona risposta:** un archivio cifrato (vault), le persone che vi hanno accesso, l'elenco delle chiavi per nome. File sul computer di una sola persona, fogli di calcolo o messaggi di posta non sono una custodia adeguata.	
3	**A chi sono intestati il dominio, i server e gli account dei servizi esterni?** **Una buona risposta:** un elenco, servizio per servizio, con l'intestatario di ciascuno; per i servizi intestati al fornitore, il modo in cui verrebbero trasferiti all'azienda.	
4	**Che cosa accade se il fornitore non è disponibile per qualche settimana, o non lo è più?** **Una buona risposta:** una procedura scritta, con chi contattare e i tempi di riscontro, e un documento con le informazioni essenziali di ogni sistema, consultabile anche quando il fornitore non risponde.	

	DOMANDA	RISPOSTA DEL FORNITORE
5	**Chi subentrerebbe, e l'azienda ha approvato quella persona?** **Una buona risposta:** una persona con nome e recapiti, esterna al fornitore, conosciuta e approvata dall'azienda, che riceve accessi propri e limitati nel tempo, non le password del fornitore.	
6	**L'azienda può ottenere le chiavi d'emergenza, e in quanto tempo?** **Una buona risposta:** sì, secondo una procedura e un tempo stabiliti nel contratto, in modo analogo al trasferimento di un dominio; il fornitore può sospendere la consegna soltanto per un motivo dichiarato.	
7	**Le copie di sicurezza sono realmente ripristinabili, e quando è stato verificato l'ultima volta?** **Una buona risposta:** la data e l'esito dell'ultima prova di ripristino effettivamente eseguita, e la frequenza con cui la prova viene ripetuta. «Facciamo un backup ogni notte», da solo, non risponde.	
8	**Chi ha avuto accesso ai sistemi, e ne resta una registrazione?** **Una buona risposta:** un registro con le persone e le date, non un elenco a memoria; quando un collaboratore lascia il fornitore, gli accessi vengono revocati e le chiavi che conosceva vengono sostituite.	
9	**Che cosa accade al termine del contratto?** **Una buona risposta:** l'elenco di ciò che viene consegnato (documentazione leggibile senza i programmi del fornitore, chiavi, codice, account dei servizi), con i tempi e la forma, scritto nel contratto.	

Direttiva NIS2. Le aziende che rientrano nell'ambito della direttiva (UE) 2022/2555 sono tenute, tra le misure di gestione dei rischi, a curare la sicurezza della catena di approvvigionamento, compresi i rapporti con i fornitori diretti (articolo 21). Le risposte a queste domande possono essere utili a tale scopo, ma non sostituiscono le valutazioni che la normativa richiede e che vanno svolte con i propri consulenti.

Versione commentata. Ogni domanda è spiegata più ampiamente, insieme al modo in cui risponde una software house che utilizza Symbiont, all'indirizzo getsymbiont.com/it/per-le-aziende.html. Questo documento può essere stampato e consegnato liberamente.