**MODULO DI ESEMPIO DEL QUESTIONARIO DI VALUTAZIONE DEL RISCHIO DEL FORNITORE**

|  |  |
| --- | --- |
| NOME FORNITORE | INDIRIZZO DEL FORNITORE |
|   |   |
| PUNTO DI CONTATTO | INFORMAZIONI DI CONTATTO |
|   |   |

ISTRUZIONI: Si prega di compilare questo questionario nella sua interezza, lasciando note e allegando documentazione di supporto ove necessario.

**Natura dei dati il fornitore avrà accesso per verificare** *tutto ciò che si applica*

|  |  |  |
| --- | --- | --- |
| **X** | **TIPO DI DATI** | **NOTE** |
|  | Nessuno scambio di dati |  |
|  | Dati demografici |  |
|  | Dati finanziari |  |
|  | Dati personali (ad es. nome, indirizzo, numero di telefono) |  |
|  | Dati personali non pubblici (ad es. SSN, medici, proprietari) |  |
|  | Altro:  |  |  |

**POLITICHE E PROCESSI**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sì** | **No** | **N/D** | **DOMANDA** | **NOTE** |
|  |  |  | L'organizzazione documenta, pubblica e applica i criteri di sicurezza? |  |
|  |  |  | La tua organizzazione documenta e applica le politiche delle risorse umane? |  |
|  |  |  | L'organizzazione documenta e applica criteri per l'uso autorizzato dei servizi di rete? |  |

**POLITICHE E PROCESSI** *continuati*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sì** | **No** | **N/D** | **DOMANDA** | **NOTE** |
|  |  |  | L'organizzazione documenta e applica criteri per l'uso autorizzato della posta elettronica, di Internet e della rete Intranet aziendali? |  |
|  |  |  | L'organizzazione documenta e applica criteri e standard di crittografia? |  |
|  |  |  | L'organizzazione documenta e applica criteri relativi all'archiviazione, all'utilizzo e allo smaltimento dei dati sensibili? |  |
|  |  |  | La tua organizzazione documenta e applica le politiche relative all'archiviazione, all'utilizzo e allo smaltimento di dati sensibili da parte di terzi? |  |
|  |  |  | La tua organizzazione esternalizza le funzionalità relative alla gestione della sicurezza? |  |
|  |  |  | Le politiche e le procedure aderiscono e rispettano le leggi e i regolamenti sulla privacy relativi alla sicurezza, all'occultamento e alla salvaguardia dei dati dei clienti? |  |
|  |  |  | Le sanzioni associate alla non conformità ai criteri dell'organizzazione sono ben documentate? |  |
|  |  |  | [Inserisci qui la domanda su politiche e processi] |  |
|  |  |  | [Inserisci qui la domanda su politiche e processi] |  |
|  |  |  | [Inserisci qui la domanda su politiche e processi] |  |

**MISURE DI SICUREZZA FISICHE E DEI DATA CENTER**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sì** | **No** | **N/D** | **DOMANDA** | **NOTE** |
|  |  |  | La tua organizzazione rivede e valuta regolarmente i rischi fisici e ambientali? |  |
|  |  |  | I controlli perimetrali dei data center prevedono l'uso di carte di accesso? |  |
|  |  |  | I controlli perimetrali del data center prevedono l'uso di controlli a tastiera? |  |
|  |  |  | I controlli perimetrali dei data center prevedono l'uso di guardie di sicurezza? |  |
|  |  |  | I controlli perimetrali del data center prevedono l'uso di \_\_[add measure here]\_\_? |  |
|  |  |  | Disponete di procedure di continuità operativa se l'ufficio è inaccessibile per qualsiasi motivo? |  |
|  |  |  | Tutte le apparecchiature di rete sono fisicamente protette? |  |
|  |  |  | L'organizzazione utilizza provider di data center? |  |
|  |  |  | La tua organizzazione utilizza i registri dei visitatori? In caso affermativo, vengono mantenuti per più di 30 giorni? |  |
|  |  |  | La tua organizzazione mantiene una politica scritta relativa ai requisiti di sicurezza fisica per l'ufficio? |  |
|  |  |  | [Inserisci qui la domanda sulla sicurezza fisica e del data center] |  |
|  |  |  | [Inserisci qui la domanda sulla sicurezza fisica e del data center] |  |

**MISURE DI SICUREZZA DEL MALWARE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sì** | **No** | **N/D** | **DOMANDA** | **NOTE** |
|  |  |  | Tutte le e-mail vengono scansionate alla ricerca di virus? |  |
|  |  |  | Il software antivirus è necessario e abilitato su tutti i computer di rete? |  |
|  |  |  | Il software antivirus ha una frequenza di scansione stabilita sui computer di rete? |  |
|  |  |  | L'organizzazione consente l'installazione di software non approvato nei computer di rete? |  |
|  |  |  | [Inserisci qui la domanda sulla sicurezza del malware] |  |
|  |  |  | [Inserisci qui la domanda sulla sicurezza del malware] |  |
|  |  |  | [Inserisci qui la domanda sulla sicurezza del malware] |  |

**MISURE DI SICUREZZA DELLE INFORMAZIONI**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sì** | **No** | **N/D** | **DOMANDA** | **NOTE** |
|  |  |  | L'organizzazione dispone di un programma di sicurezza delle informazioni? (Nella colonna delle note, si prega di fornire un link a tutte le politiche di sicurezza e privacy pertinenti rivolte al pubblico.) |  |
|  |  |  | Se l'organizzazione dispone di un programma di sicurezza delle informazioni, si applica a tutte le operazioni e i sistemi che elaborano dati sensibili? |  |
|  |  |  | Il personale e i manager interessati sono professionalmente certificati in materia di sicurezza delle informazioni? |  |
|  |  |  | L'accesso a livello di amministratore è limitato all'infrastruttura di rete? |  |
|  |  |  | Sono in atto controlli rigorosi per accedere ai registri di sicurezza? |  |
|  |  |  | [Inserisci qui la domanda sulla sicurezza delle informazioni] |  |
|  |  |  | [Inserisci qui la domanda sulla sicurezza delle informazioni] |  |
|  |  |  | [Inserisci qui la domanda sulla sicurezza delle informazioni] |  |

**MISURE DI SICUREZZA DELL'INFRASTRUTTURA DI RETE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sì** | **No** | **N/D** | **DOMANDA** | **NOTE** |
|  |  |  | L'organizzazione mantiene un criterio di sicurezza di rete? |  |
|  |  |  | Tutti i router sono sistematizzati con elenchi di controllo degli accessi per soffocare il traffico non autorizzato? |  |
|  |  |  | I sistemi operativi server sono dotati di patch al livello più recente? |  |
|  |  |  | L'organizzazione dispone di un processo per tenere traccia e comunicare le patch di vulnerabilità? |  |
|  |  |  | L'organizzazione esegue il backup dei dati? |  |
|  |  |  | I backup vengono archiviati e testati? |  |
|  |  |  | I dispositivi dei dipendenti sono crittografati? |  |
|  |  |  | Viene utilizzata una terza parte per testare la sicurezza dell'infrastruttura di rete? |  |
|  |  |  | Utilizzate sistemi di rilevamento delle intrusioni? |  |
|  |  |  | [Inserire qui la domanda sulla sicurezza dell'infrastruttura di rete] |  |
|  |  |  | [Inserire qui la domanda sulla sicurezza dell'infrastruttura di rete] |  |
|  |  |  | [Inserire qui la domanda sulla sicurezza dell'infrastruttura di rete] |  |

|  |
| --- |
| **INFORMAZIONI AGGIUNTIVE** |
|  |

|  |  |  |
| --- | --- | --- |
| NOME E TITOLO DEL VALUTATORE DEL RISCHIO | FIRMA | DATTERO |
|  |  |  |

|  |
| --- |
| **DISCONOSCIMENTO**Tutti gli articoli, i modelli o le informazioni fornite da Smartsheet sul sito Web sono solo di riferimento. Mentre ci sforziamo di mantenere le informazioni aggiornate e corrette, non rilasciamo dichiarazioni o garanzie di alcun tipo, esplicite o implicite, circa la completezza, l'accuratezza, l'affidabilità, l'idoneità o la disponibilità in relazione al sito Web o alle informazioni, agli articoli, ai modelli o alla grafica correlata contenuti nel sito Web. Qualsiasi affidamento che fai su tali informazioni è quindi strettamente a tuo rischio. |