*Allegato B*

**SCHEDA FABBISOGNO**

Avviso Pubblico a sportello per l’erogazione di interventi di potenziamento e miglioramento delle capacità cyber degli Organi costituzionali e di rilevanza costituzionale, dei Ministeri, delle Agenzie Fiscali, degli Enti di regolazione dell’attività economica, delle Autorità amministrative indipendenti e degli Enti a struttura associativa

**PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 – Componente 1 – Investimento 1.5 “Cybersecurity”**

**M1C1I1.5**

# **Sezione 1 – ANAGRAFICA DEL SOGGETTO RICHIEDENTE**

|  |  |
| --- | --- |
| **1.A Dati identificativi del Soggetto richiedente** | |
| Denominazione |  |
| Codice IPA |  |
| Posta Elettronica Certificata (PEC) |  |
| Dipartimenti che potranno essere coinvolti nell’intervento |  |
| **1.B Dati identificativi del titolare del potere di impegnare il Soggetto richiedente** *(come riportato nell’Allegato A)* | |
| Nome e Cognome |  |
| Qualifica |  |
| Riferimenti di contatto | Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  N. Telefono: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **1.C Dati identificativi del Referente del Progetto interno all’Amministrazione\*** *(da valorizzare se diverso dal Soggetto di cui al punto 1B)*  \* *righe da duplicare nell’ipotesi in cui siano presenti differenti Referenti per ciascun intervento di cui è richiesta l’erogazione* | |
| Nome e Cognome |  |
| Qualifica |  |
| CF |  |
| Nato a *(indicare il luogo e la data di nascita)* |  |
| Riferimenti di contatto | Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  N. Telefono: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

# **Sezione 2 – CARATTERISTICHE DEL SOGGETTO RICHIEDENTE**

|  |
| --- |
| **2.A Descrizione sintetica dalla struttura organizzativa interna attualmente deputata alla gestione del rischio cyber**  *Max 150 parole* |
|  |

# **Sezione 3 – EROGAZIONE DI INTERVENTI DI POTENZIAMENTO E MIGLIORAMENTO DELLA CAPACITà CYBER**

|  |
| --- |
| **3.A Descrizione sintetica dell’attuale postura di sicurezza cyber del Soggetto richiedente e degli interventi che si intendono attivare**  (*descrivere l’attuale postura di sicurezza cyber e gli interventi che si intendono attivare a valere sul presente Avviso, indicando come gli stessi possano essere funzionali alla risoluzione delle principali criticità riscontrate e/o al raggiungimento degli obiettivi* *di potenziamento e miglioramento delle capacità cyber del Soggetto richiedente)*  *Max 300 parole* |
|  |

|  |
| --- |
| **3.B Interventi richiesti**  *(Selezionare, per la tipologia di interesse, gli interventi di cui è richiesta l’erogazione e il relativo finanziamento. Si specifica che i Soggetti possono indicare al massimo 4 sotto interventi, oltre l’obbligatorio sotto-intervento 1.1 “Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber” tra quelli di seguito proposti. Al fine di consentire la quantificazione del finanziamento, si richiede di indicare per i sotto-interventi selezionati i relativi driver dimensionali)*  *\*Per facilitare la compilazione della sezione, si rimanda al Glossario (allegato B1)* |

**1 - Analisi della postura di sicurezza e piano di potenziamento**

| **Sotto interventi** | | **Driver dimensionali** |
| --- | --- | --- |
| **☒** | 1.1 Analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber\*  \* *Tale sotto-intervento è obbligatorio ai fini di una corretta analisi della maturità cyber* | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Numero di politiche/procedure presenti: oltre 10  Numero di politiche/procedure presenti: da 5 a 10  Numero di politiche/procedure presenti: < 5  Numero di applicazioni gestite: oltre 30  Numero di applicazioni gestite: da 10 a 30  Numero di applicazioni gestite: < 10 |
|  | 1.2 Analisi delle capacità dei sistemi e strumenti di sicurezza in essere | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Numero di soluzioni di sicurezza: oltre 15  Numero di soluzioni di sicurezza: da 5 a 15  Numero di soluzioni di sicurezza: < 5  Numero di asset: oltre 30  Numero di asset: da 20 a 30  Numero di asset: < 20 |
|  | 1.3 Analisi di valutazione del rischio eseguita sui principali asset del Soggetto destinatario | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Numero Applicazioni critiche da analizzare: oltre 10  Numero Applicazioni critiche da analizzare: da 5 a 10  Numero Applicazioni critiche da analizzare: < 5  Numero di responsabili degli applicativi: oltre 3  Numero di responsabili degli applicativi: da 2 a 3  Numero di responsabili degli applicativi: < 2 |

**2 - Miglioramento dei processi e dell’organizzazione di gestione della cybersecurity**

| **Sotto interventi** | | **Driver dimensionali** |
| --- | --- | --- |
|  | 2.1 Definizione e/o potenziamento dei processi di gestione degli incidenti di natura cyber e di backup e restore | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Numero Server: oltre 500  Numero Server: da 100 a 500  Numero Server: < 100  Numero Client: oltre 10.000  Numero Client: da 1.000 a 10.000  Numero Client: < 1.000 |
|  | 2.2 Definizione e/o potenziamento del processo di security by design | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Numero Tecnologie: oltre 20  Numero Tecnologie: da 10 a 20  Numero Tecnologie: < 10 |
|  | 2.3 Definizione e/o potenziamento del processo a supporto della continuità operativa | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Numero di Applicazioni critiche da analizzare: oltre 10  Numero di Applicazioni critiche da analizzare: da 10 a 5  Numero di Applicazioni critiche da analizzare: < 5  Numero di processi/servizi critici: oltre 15  Numero di processi/servizi critici: da 15 a 10  Numero di processi/servizi critici: < 10 |
|  | 2.4 Definizione e/o potenziamento del processo di gestione delle vulnerabilità e di sviluppo sicuro del codice | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Numero di linguaggi di programmazione usati: oltre 5  Numero di linguaggi di programmazione usati: da 3 a 5  Numero di linguaggi di programmazione usati: < 3  Numero di applicazioni gestite: oltre 30  Numero di applicazioni gestite: da 10 a 30  Numero di applicazioni gestite: < 10 |
|  | 2.5 Definizione e/o potenziamento del processo di gestione delle identità digitali e degli accessi ai sistemi informativi | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Numero di Identità gestite: oltre 300  Numero di Identità gestite: da 100 a 300  Numero di Identità gestite: < 100  Numero di policy implementate: oltre 10.000  Numero di policy implementate: da 5.000 a 10.000  Numero di policy implementate: < 5.000 |
|  | 2.6 Supporto in ambito Network Security: analisi della rete e piano di reingegnerizzazione | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Presenza VPN, MPLS, SD-WAN, Dark Fiber  Presenza VPN, MPLS, SD-WAN  Presenze VPN, MPLS  Numero utenti (utilizzatori web proxy): oltre 5.000  Numero utenti (utilizzatori web proxy): da 1.000 a 5.000  Numero utenti (utilizzatori web proxy): < 1.000  Numero di Server: da 501 a 2.000  Numero di Server: da 101 a 500  Numero di Server: < 101 |
|  | 2.7 Revisione e potenziamento del framework documentale (politiche/procedure) di sicurezza sulla base delle esigenze emerse dalle attività di analisi | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Numero di Policy/Procedure in essere: oltre 10  Numero di Policy/Procedure in essere: da 5 a 10  Numero di Policy/Procedure in essere: < 5 |
|  | 2.8 Definizione di un modello di CSIRT/SOC | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Presidio SOC presente: NO  Presidio SOC presente: SI  Presenza SIEM: NO  Presenza SIEM: SI  Applicazioni agganciate SIEM: > 20  Presenza SIEM: SI  Applicazioni agganciate SIEM: da 10 a 20  Presenza SIEM: SI  Applicazioni agganciate SIEM: < 10 |
|  | 2.9 Revisione e potenziamento dell'organizzazione della cybersicurezza e disegno dei relativi processi | Numero di Dipartimenti coinvolti: >= 3  Numero di Dipartimenti coinvolti: 2  Numero di Dipartimenti coinvolti: 1  Numero di processi definiti: oltre 25  Numero di processi definiti: da 15 a 25  Numero di processi definiti: < 15  Numero di applicazioni gestite: oltre 30  Numero di applicazioni gestite: da 10 a 30  Numero di applicazioni gestite: < 10 |

**3 – Miglioramento della consapevolezza delle persone**

|  |  |  |
| --- | --- | --- |
| **Sotto interventi** | | **Driver dimensionali** |
|  | 3.1 Servizi di Cyber Security Awareness (ad es. contrasto mail di phishing) \*  \* *a seconda del numero di dipendenti saranno definite le sessioni utili per l’erogazione dell’attività.* | Numero di Dipendenti: oltre 500  Numero di Dipendenti: da 151 a 500  Numero di Dipendenti: <= 150 |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(*Luogo e data*)

Il/La dichiarante

*(da firmare digitalmente)*

*Allegato B1*

***Glossario***

| **Termini** | **Descrizione esemplificativa** |
| --- | --- |
| ***Applicazione*** | Un software o un insieme di software in esecuzione su un server |
| ***Dipartimento coinvolto nell’intervento*** | Unità organizzativa, composta da uno o più uffici, avente autonomia gestionale in ambito Information Technology (IT), Sistemi Informativi e Sicurezza Informatica, e dunque interessata dagli interventi oggetto dell’Avviso |
| ***Dipendenti a cui è rivolta la formazione*** | Personale dirigenziale e non dirigenziale alle dipendenze delle PA, assunto con contratto a tempo indeterminato, da coinvolgere nell’intervento 3 *“Miglioramento della consapevolezza delle persone”* |
| ***Identità*** | Identità corporate (dipendenti, terze parti, utenze tecniche ecc.) gestite dallo IAM (Identity and Access Management) |
| ***Linguaggio di sviluppo*** | Lingua formale pensata per realizzare set di istruzioni (input) con cui si producono dati in uscita (output). Alcuni esempi sono Java, Python, PHP, ecc. |
| ***Manuale operativo*** | Istruzioni più o meno dettagliate fornite in merito allo svolgimento di specifiche attività relative a un processo di riferimento |
| ***Politica*** | Documento di alto livello, che fornisce linee guida in merito allo svolgimento di uno specifico processo |
| ***Procedura*** | Formalizzazione di un processo in un documento che descrive la sequenza delle azioni eseguite, suddividendo ruoli e responsabilità tra gli attori coinvolti in tale processo |
| ***Processo*** | Sequenza di attività, progettata per produrre uno specifico output |