SCHEDA PROGETTO :

Progetto: GESTIONE DELLA SICUREZZA DELL'INFRASTRUTTURA INFORMATICA (RETI, TELEFONIA E SISTEMI INFORMATIVI) PERCHÉ SIA AFFIDABILE E SICURA RISPETTO AL LIVELLO DI SERVIZIO, ALLA CONTINUITÀ OPERATIVA E ALLA PROTEZIONE DEI DATI.

Premessa

Il progetto si inserisce nelle attività proprie del U.O. Sistemi Informativi ed attiene ad un tema diventato sempre più centrale e strategico per garantire il corretto ed efficiente funzionamento dell'Ente, come evidenziato anche nel report di gennaio 2022 del World Economic Forum *"l'aumento vertiginoso dello smart working durante la pandemia di COVID-19 accoppiato con l'incremento degli attacchi informatici e del loro livello di complessità, rendono necessario considerare il tema della sicurezza informatica come elemento chiave della strategia delle organizzazioni e delle nazioni"* ed infatti gran parte degli obiettivi del Piano Triennale della Pubblica Amministrazione sono dedicati alle attività da attuare in tale direzione.

Si tratta di attività strategiche ed indispensabili, la cui complessità si sta incrementando anno dopo anno, da gestire e realizzare, che risultano fortemente condizionate dalla disponibilità finanziaria e dalla contrazione di risorse umane.

L'attività, dando seguito alle linee dettate dal Piano Triennale della Pubblica Amministrazione e più in generale alla normativa nazionale relativa alla sicurezza dei sistemi informativi e alla protezione dei dati, riguarda i seguenti principali temi:

- aumentare la consapevolezza del rischio cyber *(Cyber Security Awareness)* all'interno dell'Ente;
- adottare strumenti e modalità operative che riducano il rischio di attacchi informatici e il potenziale impatto, garantendo al contempo la massima disponibilità dei servizi, anche da remoto;
- garantire il costante aggiornamento dell'infrastruttura e delle modalità di gestione secondo le Misure minime di sicurezza ICT per le pubbliche amministrazioni emanate da AgID;
- preparare l'infrastruttura per consentire la migrazione verso data center certificati ed infrastrutture e servizi cloud qualificati, riducendo al minimo i disservizi e la continuità dei servizi.

Finalità:

Il progetto ha l'obiettivo di incentivare la realizzazione delle attività sopra esposte garantendo la massima disponibilità dei servizi, così da non incidere negativamente nell'attività dell'Ente.

E' quindi prevista la possibilità di incentivare la disponibilità ad effettuare attività specialistiche, di maggiore complessità rispetto all'attività ordinaria, e/o al di fuori del normale orario di lavoro da parte del personale, in particolare in relazione a:

- partecipare a corsi di formazione emanati da AgID e seguire incontri specialistici sul tema della cyber security anche al di fuori dell'orario di lavoro, con la finalità di formare e diffondere la consapevolezza del rischio all'interno dell'Ente, oltre che di individuare strumenti, preferibilmente economicamente vantaggiosi, che possano essere acquisiti per la protezione dell'infrastruttura;
- aggiornare l'infrastruttura virtuale, i sistemi operativi dei server, il firewall e le applicazioni;
- adeguare l'infrastruttura virtuale, lo storage, le procedure di backup perché possano essere agevolmente migrate in data center certificati;
- gestire situazioni di particolare emergenza e criticità (attacchi informatici, errori bloccanti sull'infrastruttura, disservizi elettrici, eventi sismici, etc);
- effettuare controllo, supporto e/o esecuzione diretta degli interventi di manutenzione ai sistemi nei momenti di minore impatto sugli utenti.

Personale potenzialmente coinvolto (personale tecnico ed amministrativo): n. 9, suddiviso in 1 unità di livello B, 6 unità di livello C, 2 unità di livello D

Eventuale incentivo: potrà essere definito un incentivo a carico del salario accessorio per riconoscere una premialità aggiuntiva al personale partecipante al progetto

Criteri di ripartizione: considerando che il progetto richiede competenze altamente specialistiche e che il personale coinvolto ha differenti profili e competenze da poter spendere nelle attività del progetto,

l'assegnazione dell'eventuale incentivo sarà differenziato secondo il differente contributo al raggiungimento degli obiettivi del progetto. In particolare verranno misurati e valutati:

- la partecipazione ad attività emergenziali di ripristino in sicurezza dei sistemi, dovute ad incidenti e/o particolari minacce alla sicurezza dell'infrastruttura;
- la partecipazione ad attività di aggiornamento dei sistemi, atti a garantire un innalzamento del livello di sicurezza, anche al di fuori dell'ordinario orario di lavoro (cambiando ad esempio i pomeriggi di lavoro e/o variando gli orari) così da non generare lunghi periodi di disservizio dei sistemi e garantendo l'ordinario funzionamento dell'Ente;
- la partecipazione ad attività di aggiornamento, configurazione e gestione dell'infrastruttura virtuale per garantire la continuità operativa dei server;
- la partecipazione ad attività di supporto e formazione agli utenti dell'Ente, nell'ambito dell'ordinario supporto tramite Help Desk, telefono e richieste di assistenza oppure con l'erogazione di specifici momenti formativi.