Appendice 3 - AL CAPITOLATO TECNICO

Piano della sicurezza del Centro Servizi

INDICE

1. Piano della sicurezza del Centro Servizi

Il Fornitore deve disporre di un Centro Servizi tale da garantire tutti i livelli di sicurezza previsti dalle normative vigenti e in particolar modo:

- la presenza di un ambiente sicuro e protetto;
- la privacy delle informazioni raccolte;
- gli strumenti ed i processi organizzativi atti al ripristino di dati e di servizi interrotti.

Il Piano della Sicurezza del Centro Servizi (PSCS) dovrà essere prodotto dal Fornitore nell'ambito del Piano di Migrazione e deve essere validato da Consip. Il PSCS dovrà contenere una descrizione approfondita sulle modalità logistiche ed organizzative, gli strumenti ed i sistemi che il Fornitore intende adottare o di cui è provvisto per rendere sicuro e protetto l'ambiente in cui sono ospitati le infrastrutture, il software e i dati informativi dell'Amministrazione. Di Seguito sono indicati i requisiti minimi che tale Piano dovrà prevedere.

Solo a titolo esemplificativo e non esaustivo, il PSCS dovrà contenere:

- la definizione delle linee guida progettuali per la determinazione delle misure di sicurezza minime e idonee per la protezione dei dati informatici e dei relativi flussi;
- il personale coinvolto nel trattamento dei dati quali:
  - responsabile della sicurezza
  - gli amministratori di sistema;
  - il responsabile del trattamento interno ed esterno;
  - gli Incaricati interni;
  - gli addetti alla gestione e/o alla manutenzione degli strumenti elettronici;
  - i soggetti incaricati della custodia delle credenziali di autenticazione e le relative lettere di nomina;

  per ciascuno di essi dovranno essere descritti compiti e responsabilità di competenza;
- i principali eventi potenzialmente dannosi per la sicurezza dei dati (analisi dei rischi), la valtazione delle possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati (comportamenti anomali da parte degli operatori al servizio, malfunzionamento degli strumenti utilizzati, virus, ecc.);
- i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati, compresa una descrizione sintetica dei criteri e delle procedure adottate per il salvataggio dei dati al fine del loro corretto ripristino;
- il piano degli interventi formativi previsto per le figure professionali precedentemente richiamate;
- la definizione delle attività affidate a terzi con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale attività si

inserisce in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati e dei sistemi.

Tutte le informazioni contenute nel PSCS devono essere desunte dalla documentazione prodotta per la certificazione ISO/IEC 27001:2013 e devono quindi essere parte integrante delle attività regolate dalla stessa.
Eventuali variazioni dovranno essere comunicate dal Responsabile del Servizio tempestivamente. Documenti incompleti o inesatti o non aggiornati dovranno essere immediatamente adeguati ed in ogni caso Consip si riserva di richiedere aggiornamenti o approfondimenti della documentazione stessa.

Il Fornitore dovrà garantire che siano rispettate almeno le seguenti misure generali:

- attuazione delle misure minime organizzative e tecniche previste dal Codice in materia di protezione dei dati personali (D.L. 30 giugno 2003, n. 196 Allegato B – Trattamento con strumenti elettronici) ultima modifica decreto legislativo 14 marzo 2013, n. 33;
- disposizione di un'organizzazione per la gestione della sicurezza dell'infrastruttura, secondo il modello indicato dalla certificazione ISO 27001 in possesso dal fornitore;
- sottoscrizione e applicazione le policy di sicurezza richieste da Consip e produrre le conseguenti istruzioni operative;
- garanzia di tempestivo aggiornamento, con applicazione delle patch, del software/firmware degli apparati (router/switch) che trasportano il traffico secondo le politiche concordate con Consip;
- garanzia di tempestivo aggiornamento dei Sistemi Operativi dei Server per evitare problematiche di sicurezza degli apparati.
- garanzia, sui sistemi server, dell'univoca identificazione ed autenticazione degli utenti; di protezione delle loro informazioni nei confronti di altri utenti; di accesso alle risorse esclusivamente agli utenti abilitati.
- disposizione di sistemi di controllo e filtraggio del traffico e di verifica dell'assenza di codice malevolo nei messaggi di posta elettronica (antispam, antivirus, antiphishing);

implementazione sui dispositivi che realizzano i punti di accesso ai servizi, di tutte le funzionalità volte ad impedire attacchi di tipo IP spoofing provenienti/diretti verso la rete Consip;