Autorità per la Vigilanza sui Contratti Pubblici di Lavori, Servizi e Forniture

Determinazione n. 5 del 06/06/2014

Oggetto: Attrezzatura informatica delle SOA per la comunicazione delle informazioni all'Osservatorio.

L'articolo 67 comma 5 del D.P.R. 207/2010 e successive modificazioni ed integrazioni, prevede che le SOA (Società Organismi di Attestazione) debbano disporre di attrezzatura informatica conforme al tipo definito dall'Autorità per la comunicazione delle informazioni all'Osservatorio.

Le caratteristiche dell'attrezzatura, così come di seguito definita, e la struttura informatica delle SOA dovranno essere aggiornate in relazione all'aggiornamento della struttura informatica dell'Autorità. Analogamente, le policy di sicurezza delle SOA dovranno essere, di volta in volta, adeguate ad eventuali mutamenti delle policy di sicurezza dell'Autorità.

La comunicazione delle informazioni "da" e "verso" l'Autorità avviene nel rispetto del **Codice dell'Amministrazione Digitale (CAD)** di cui al Decreto Legislativo 7 marzo 2005 n. 82 e successive modifiche ed integrazioni.

Le tecnologie informatiche a supporto della trasmissione informatica dei documenti, in piena conformità con le **Regole tecniche e di sicurezza** per il funzionamento del Sistema pubblico di connettività previste dall'articolo 71 comma 1bis del CAD, sono principalmente:

- la **cooperazione applicativa**, secondo il modello costituito dall'insieme delle regole e delle specifiche funzionali del sottosistema logico *SPCoop*. Nel caso in cui la SOA debba scambiare informazioni con l'Autorità attraverso l'utilizzo di servizi (ovvero non tramite le applicazioni rese disponibili sul portale web dell'Autorità), dovranno essere adottati i sistemi previsti da *SPCoop*, in conformità alle direttive tecniche emanate da DigitPA (oggi AgID – Agenzia per l'Italia Digitale) in relazione alla *Porta di Dominio* ed alla *busta di eGov*;
- la **posta elettronica certificata (PEC)**, così come previsto dal D.P.R. 11 febbraio 2005 n. 68 pubblicato sulla G.U. 28 aprile 2005 n. 97 e dal Decreto Ministeriale pubblicato sulla G.U. del 15 novembre 2005, n. 266 contenente le "*Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata*";
- la **firma digitale** o altro tipo di firma elettronica qualificata per i legali rappresentanti e i direttori tecnici delle SOA.

La SOA dovrà effettuare la riproduzione su supporti informatici e la conservazione nel tempo dei documenti e delle informazioni di cui è prescritta la conservazione per legge o regolamento in conformità al CAD (Capo III - Formazione, gestione e conservazione dei documenti informatici) e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 del medesimo CAD.

La SOA dovrà operare nel rispetto della regolamentazione in materia di privacy e delle misure minime di sicurezza, così come definito dal **Decreto legislativo 30 giugno 2003, n. 196** "*Codice in materia di protezione*

dei dati personali" (c.d. *Codice della Privacy*), in vigore dal 1 gennaio 2004. In relazione agli aspetti di privacy la SOA dovrà inoltre adottare le prescrizioni introdotte dai seguenti provvedimenti normativi:

- **Legge 6 agosto 2008 n. 133**, di conversione, con modificazioni, del Decreto legge 25 giugno 2008 n. 112 "*Conversione in legge, con modificazioni, del Decreto legge 25 giugno 2008, n. 112, recante disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione tributaria*";
- **Decreto legislativo 30 maggio 2008, n. 109**, "*Attuazione della Direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*".

Dovranno, altresì, essere rispettati i pronunciamenti del Garante della Privacy, ivi compresi gli adempimenti per gli *amministratori di sistema* contenuti in "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" pubblicato sulla Gazzetta Ufficiale del 24/12/08, n. 300 - Serie generale e successive modificazioni ed integrazioni.

ATTREZZATURA INFORMATICA DELLE SOA

Requisiti di sicurezza delle infrastrutture presso le SOA

La SOA dovrà, in sintonia con le politiche di sicurezza dell'Autorità, definire ed applicare idonee misure di sicurezza fisica, logica ed organizzativa sulla base di requisiti di sicurezza, riservatezza, integrità e disponibilità di dati, documenti ed informazioni, oltre alle misure derivanti da una propria analisi dei rischi informatici.

L'infrastruttura di base, nella quale verranno realizzati i database, dovrà essere in grado di garantire il funzionamento continuo delle apparecchiature per quanto riguarda la logica elaborativa necessaria alla visibilità dei dati. Dovranno essere utilizzati, ove necessario, sistemi ridondati in grado di garantire l'alta affidabilità e la continuità nell'utilizzo dei database anche a fronte dell'indisponibilità di alcune componenti dell'infrastruttura di base. Dovranno, inoltre, essere previste procedure di carattere tecnico e organizzativo in materia di conservazione e ripristino delle informazioni (*backup&restore*). In tale ambito la SOA dovrà disporre, tra l'altro, di un gruppo di continuità in grado di alimentare tutte le apparecchiature che si riterrà opportuno collegare per un tempo sufficiente a terminare le operazioni di salvataggio e chiusura ordinata del sistema al fine di evitare la perdita di informazioni.

L'infrastruttura di rete utilizzata dalla SOA dovrà avvalersi di dispositivi tecnologici (apparecchiature per l'instradamento quali *switch, router, etc.*) idonei a garantire le opportune misure di sicurezza informatica e l'adeguato svolgimento delle attività di pertinenza. In particolare, l'infrastruttura di base e le apparecchiature che ospitano i database dovranno essere protetti da opportuni sistemi *firewall*, in grado di impedire accessi non autorizzati e di concedere l'utilizzo dei database e delle risorse in modo controllato. I sistemi della SOA dovranno prevedere misure idonee a proteggere le informazioni da codice malevolo, *virus informatici* o altri software dannosi, come ad esempio *malware*, *worm* e *trojan*.

Ove applicabile e come prescritto dal già richiamato Codice in materia di protezione dei dati personali con particolare riferimento al Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Codice della Privacy), il trattamento di dati personali con strumenti elettronici deve essere consentito ai soli incaricati dotati di credenziali che consentano il superamento di una procedura di autenticazione specifica.

Per gli incaricati potranno essere individuati "*profili di autorizzazione*" di ambito diverso. Detti profili di autorizzazione, relativi a ciascun incaricato o a classi omogenee di incaricati, dovranno essere individuati e configurati anteriormente all'inizio del trattamento e comunque in modo tale da limitare l'accesso ai soli dati necessari all'effettuazione delle operazioni previste per lo specifico trattamento.

La SOA dovrà disporre di un collegamento alla rete Internet al fine di comunicare e/o reperire le informazioni di propria pertinenza attraverso le funzionalità rese disponibili sul portale dell'Autorità. Tale collegamento dovrà consentire una velocità di navigazione di almeno 7 **Mbps** in *download* e di almeno **384 Kbps** in *upload*.

Caratteristiche hardware minime dei sistemi server

Le SOA dovranno disporre di adeguati *server*, fisici o virtuali, allo stato dell'arte della tecnologia, secondo l'architettura autonomamente scelta per realizzare il sistema.

I sistemi *server* dovranno ricomprendere un sottosistema di memorizzazione con spazio disco adeguato a mantenere in linea le informazioni di competenza acquisite nel corso del tempo e con caratteristiche di alta affidabilità ed efficienza (es. modalità *RAID*).

Per la gestione dei documenti e delle informazioni il cui trattamento è effettuato nell'ambito di un processo di dematerializzazione, ovvero esclusivamente in formato elettronico, le SOA si dovranno dotare di dispositivi per la conservazione dei documenti informatici in accordo con le normative vigenti(CAD - Capo III - Formazione, gestione e conservazione dei documenti informatici e regole tecniche stabilite ai sensi dell'articolo 71 dello stesso Codice).

Caratteristiche software minime

Le SOA dovranno disporre di un database per la gestione di tutte le informazioni di cui all'art. 8 comma 2 del D.P.R. 207/2010.
Il database dovrà, inoltre, gestire le informazioni relative alle istruttorie sulla qualificazione per consentire l'acquisizione di quanto necessario allo svolgimento dell'attività di vigilanza in capo all'Autorità (art.71 del D.P.R. 207/2010).

Il software utilizzato dalle SOA per alimentare il database dovrà essere realizzato in conformità alle regole in materia di tutela della privacy e consentire l'accesso agli utenti in relazione al ruolo svolto nell'ambito del processo di attestazione. Lo stesso dovrà disporre di funzionalità per la gestione dei dati del contratto di attestazione tra la SOA e l'operatore economico, per la gestione del ciclo di vita della richiesta di attestazione e dell'attestato rilasciato ed, in definitiva, per la gestione delle informazioni di cui all'art. 8 comma 2 del D.P.R. 207/2010.

Le SOA dovranno comunicare ad AVCP i dati relativi alle imprese attestande e/o attestate utilizzando una delle seguenti modalità :

- attraverso l'interazione con l'applicazione ***"Attestazioni",*** accessibile dalla sezione dei *"Servizi ad accesso riservato"* del portale AVCP;
- attraverso l'uso di *servizi di cooperazione applicativa* secondo le specifiche pubblicate sul medesimo portale AVCP.

Quanto sopra premesso e considerato si invitano tutte le SOA autorizzate all'adozione e/o all'aggiornamento nei sensi suesposti degli standard infrastrutturali e di sicurezza dei propri sistemi informatici, nell'ottica del perseguimento del migliore efficientamento del sistema, assegnando per l'aggiornamento il termine di 60 giorni dalla pubblicazione della presente determinazione, fermi restando gli obblighi delle SOA di assicurare la trasmissione dei dati/informazioni di cui all'art. 8, comma 2 e seguenti, del D.P.R. n. 207/2010, disciplinata dall'Autorità con il distinto Comunicato afferente il rilascio in esercizio della procedura "attestazioni".

Il riscontro da parte dell'Autorità della mancata tempestiva attuazione di quanto previsto nella presente determinazione comporterà i necessari e conseguenti provvedimenti a carico delle SOA inadempienti.

Il Presidente: Sergio Santoro

Depositato presso la Segreteria del Consiglio in data: 9 giugno 2014

Il Segretario: Maria Esposito