AO Moscati

L' art. 23 del Codice dell'Amministrazione Digitale (Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i.), riconosce alle copie analogiche di documenti informatici (es. la stampa di un certificato, un contratto, ecc.) la stessa efficacia probatoria dell'originale informatico da cui sono tratti se la loro conformit non viene espressamente disconosciuta (in giudizio). Diverso il caso in cui la conformit all'originare informatico, in tutte le sue componenti, sia attestata da un pubblico ufficiale autorizzato. In questo caso, infatti, per negare alla copia analogica di documento informatico la stessa efficacia probatoria del documento sorgente si rende necessaria la querela di falso.

Questo regime, di carattere generale, incontra alcune deroghe rispetto alle copie analogiche di documenti amministrativi informatici.

L'art. 23-ter del CAD prevede che sulle copie analogiche di documenti amministrativi informatici possa essere apposto un contrassegno a stampa (detto anche timbro digitale o glifo) che consente di accertare la corrispondenza tra le copie analogiche stesse e l'originale informatico (in esso deve essere codificato, infatti, il documento informatico o le informazioni necessarie a verificarne la corrispondenza all'originale in formato digitale). La verifica avviene grazie ad appositi software che leggono le informazioni contenute nel timbro digitale. I software necessari per l'attivit di verifica devono essere gratuiti e messi liberamente a disposizione da parte delle amministrazioni.

Copia conforme di un documento amministrativo informatico formata ai sensi dell'articolo 23-ter, comma 5 del CAD.
Il presente contrassegno digitale Datamatrix contiene informazioni utili alla verifica della corrispondenza del documento all'originale digitale conservato dall'amministrazione proprietaria dello stesso.
Il contrassegno pu essere letto con qualsiasi applicazione in grado di decodificare il formato Datamatrix e con gli smartphone dei principali costruttori.
In alternativa possibile collegarsi al sistema DgsWebOS dell'amministrazione e ricercare dopo l'autenticazione il documento

Impronta del documento digitale originale: 04e5642cff5b6acee8837e9f09a062ab
Identificativo del documento digitale originale: 599216
Protocollo: AOM-0002665-2025 24-01-2025 15:31:58

Documento generato dal sistema DgsWebOS in data: 24-02-2025 11:20:57

A.O.R.N. E DI ALTA SPECIALITÀ
San Giuseppe Moscati

AZIENDA OSPEDALIERA
DI RILIEVO NAZIONALE
E DI ALTA SPECIALITÀ

aornmoscati.it

U.O.C. SISTEMI INFORMATIVI

An ISO 27001:2022 Certified
n. 241217053901

A Direttore U.O.C. A.B.S.

e, p.c. Direttore Amministrativo

Direttore U.O.C. Tecnico-Patrimonio-Ing.Clinica

SEDE

Oggetto: sicurezza informatica dei dispositivi medici in rete

L'infrastruttura TLC aziendale è utilizzata, oltre che dagli host a dominio aziendale *"aornmoscati"* (pc, tablet, palmari, stampanti, multifunzione, server, etc.), anche dai sistemi appartenenti agli ambiti *IoMT/IoT* (*"Internet of Medical Things" / Internet of Things"*), quali dispositivi medici come tac, rm, strumentazioni di laboratorio, sistemi robotizzati per allestimento di antiblastici, etc., e, a breve, anche sistemi robotizzati per la gestione della logistica del farmaco.

Tali sistemi appartengono, nel loro complesso, al mondo dell'OT ("operational technology", tecnologia operativa), come insieme delle risorse hardware e software per il monitoraggio ed il controllo di processi fisici, dispositivi e infrastrutture: sommariamente, mentre la tecnologia dell'informazione (IT) controlla i dati, la tecnologia operativa (OT) controlla le apparecchiature.

L'innovazione digitale in corso in Azienda, che richiede che i sistemi OT interagiscano con i sistemi IT (i dati raccolti dalle apparecchiature fisiche e dai dispositivi IoMT/IoT in ambito sanitario possono confluire nel sistema informativo sanitario aziendale), è supportata, a livello infrastrutturale, dalla condivisione dell'infrastruttura ICT/TLC tra gli ambiti IT/OT, di cui è innanzi detto.

Considerato che la tecnologia operativa gestisce processi che, se violati, potrebbero comportare la sospensione di servizi critici con conseguenze disastrose, rileva la necessità ed urgenza di adottare misure di mitigazione del rischio per la sicurezza informatica dei sistemi OT aziendali che, nel contempo, non richiedano alcun intervento sui sistemi stessi e, quindi, non impattino in alcun modo sulla continuità operativa.

Pertanto lo scrivente, nella qualità di Responsabile Aziendale per la Transizione Digitale giusta deliberazione n.1239/2019, richiamate anche le deliberazioni nn. 59/2025 e 62/2025, ha individuato, all'uopo, un sistema di OT security, integrato nei sistemi firewall aziendali, con funzionalità IPS / Application Control / Virtual Patching per il mondo OT, in alta affidabilità, estensivo delle funzionalità dei sistemi firewall in esercizio in azienda, in tecnologia Fortigate.

Si richiede, pertanto, l'acquisto servizi, in regime di licenza d'uso triennale, per l'importo presunto di € 65.000,00 oltre IVA:

codice	descrizione	q.tà
FC-10-F26HF-159-02-12	IOT FG2600 3YR FortiGate-2600F 1 Year FortiGuard OT Security Service (OT dashboards and compliance reports, OT application and service detection, OT vulnerability correlation, OT virtual patching, OT signatures - Application Control and IPS rules)	6

La presente richiesta riveste carattere di urgenza in relazione alla necessità di riduzione della superficie di attacco dei sistemi aziendali rispetto a **potenziali minacce informatiche con obiettivo i dispositivi medici in rete, rispetto alle quali, in mancanza, l'Azienda risulterebbe maggiormente esposta**.

Ferma la possibilità di rivolgersi alla platea di operatori economici autorizzati alla vendita o distribuzione dei sistemi e servizi innanzi emarginati, si precisa che l'utilizzo di piattaforme di diverso produttore non consentirebbe l'integrazione nativa tra sistemi di sicurezza garantita dall'upgrade della piattaforma esistente oltre a generare oneri economici aggiuntivi e difficoltà tecniche non proporzionate.

Si inoltra alla Direzione Amministrativa anche ai fini autorizzativi, ove il caso occorra.

Distinti saluti.

Il Direttore
Dott. Giuseppe Versace