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: 6931819223957c934587816b8d19c656
Identificativo del documento digitale originale: 599709
Protocollo: AOM-0002772-2025 27-01-2025 12:46:19

Documento generato dal sistema DgsWebOS in data: 24-02-2025 11:24:35

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

SEDE

Oggetto: **sicurezza informatica – gestione avanzata dei log e degli eventi all'interno della rete aziendale**

Nell'ambito delle finalità di cui alla procedura *"PR25 – security event and incident management"* definita nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni dei Sistemi Informativi Aziendali certificato ISO27001:2022, come da deliberazione n.59/2025, lo scrivente (anche nella qualità di Responsabile Aziendale per la Transizione Digitale giusta deliberazione n.1239/2019) ha individuato (richiamata la deliberazione n.62/2025) un sistema di gestione avanzata dei log e degli eventi all'interno della rete aziendale, integrato nei sistemi firewall aziendali, in alta affidabilità, estensivo delle funzionalità dei sistemi firewall in esercizio in azienda, in tecnologia Fortigate.

Si richiede, pertanto, l'acquisto del sistema *"Fortigate Analyzer 50 GB/day VM + care 2 yr"*, in regime di licenza d'uso triennale, per l'importo presunto di € 30.000,00 oltre IVA, come di seguito specificato:

codice	descrizione	q.tà
FAZ-VM-GB25	FortiAnalyzer-VM Upgrade license for adding 25 GB/Day of Logs	2
FC5-10-LV0VM-661-02-12	FortlAnalyzer-VM IOC and Outbreak Detection Service 1 Year FortiGuard IOC and Outbreak Detection Service for FAZVM Perpetual (1-101 GB/Day of Logs)	2
FC5-10-LV0VM-248-02-12	FortiAnalyzer-VM FortiCare Premium Support 1 Year FortiCare Premium Support (for 1- 101 GB/Day of Logs)	2

Il sistema innanzi emarginato ha lo scopo di migliorare la visibilità e il controllo della rete aziendale, offrendo una panoramica dettagliata delle attività sospette e degli incidenti di sicurezza, tramite servizi di:

- raccolta e analisi dei log dei dati registrati dai dispositivi di sicurezza
- monitoraggio delle minacce: individuazione dei comportamenti anomali e delle minacce in tempo reale, attraverso la correlazione degli eventi
- reportistica dettagliata per conformità normativa, auditing e valutazioni delle performance di sicurezza
- incident response

Il sistema permette una visione centralizzata degli eventi di rete, facilitando l'identificazione di potenziali minacce, ottimizza le operazioni di sicurezza grazie alla correlazione

automatizzata degli eventi, concorre a ridurre il carico di lavoro manuale e a rispondere più rapidamente agli incidenti.

La presente richiesta riveste carattere di urgenza, atteso che la mancanza andrebbe a detrimento della postura di sicurezza informatica aziendale rispetto alla necessità di prevenzione, rilevamento e rapida risposta alle potenziali minacce.

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