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: 3e076f9c5727d9a0915ace1c9963db2a
Identificativo del documento digitale originale: 597892
Protocollo: AOM-0002353-2025 22-01-2025 13:45:22

Documento generato dal sistema DgsWebOS in data: 24-02-2025 11:19:31

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: **Linee Guida AgID per la configurazione per adeguare la sicurezza del software di base – WAF (web application filter)**

Richiamate le vigenti Linee Guida AgID in oggetto emarginate, che, al paragrafo 5.5 in materia di *"sicurezza dei web application server"* prescrivono l'adozione di un Web Application Firewall (WAF) quale contromisura per mitigare i rischi da:

- accesso non autorizzato alle informazioni
- attacchi all'integrità delle informazioni

considerato che, pertanto, i sistemi firewall aziendali di front end, in tecnologia Fortigate, devono essere oggetto di upgrade ed estensione con funzionalità di web application firewalling, in alta affidabiilità, a protezione dei servizi aziendali esposti al pubblico (sito web, cartelle cliniche on-line, referti on-line, etc.) ed ai dipendenti (portale del dipendente), lo scrivente, anche nell'ambito degli obiettivi per la corrente annualità e nella qualità di Responsabile Aziendale per la Transizione Digitale giusta deliberazione n.1239/2019, ha individuato, all'uopo, i seguenti sistemi e servizi, di cui si richiede l'acquisto:

codice	descrizione	q.tà
FWB-VM04	FortiWeb-VM04 Web Application Firewall - virtual appliance for all supported platforms. Supports up to 4 x vCPU core	2
FC-10-VVM04-581-02-36	FortiWeb-VM04 3 Year Advanced Bundle - Standard Bundle plus Credential Stuffing Defense Service and Threat Analytics	2

Con relativi servizi manutentivi per la durata di mesi 36, per l'importo presunto di € 120.000,00 oltre IVA.

La presente richiesta, oltre a ricondursi alle linee guida nazionali innanzi richiamate, riveste carattere di urgenza in relazione alla necessità di riduzione ulteriore della superficie di attacco dei sistemi aziendali rispetto a potenziali minacce informatiche (quali ad esempio, cross-site scripting (XSS), SQL injection, DDoS, dirottamento di sessioni, buffer overflow, etc.), 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