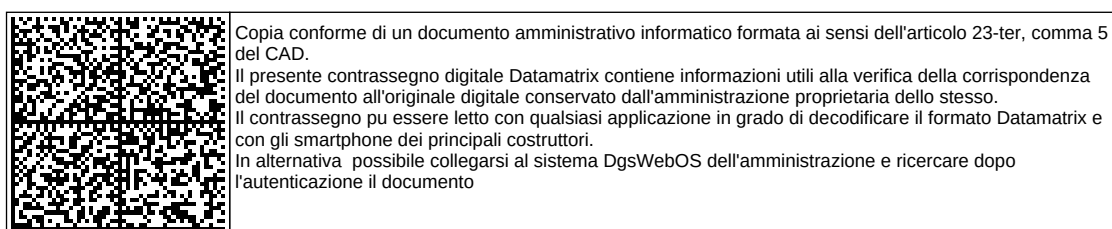


AO Moscati

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 conformità non viene espressamente disconosciuta (in giudizio). Diverso il caso in cui la conformità all'originale 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'attività di verifica devono essere gratuiti e messi liberamente a disposizione da parte delle amministrazioni.



Impronta del documento digitale originale: 6b997b47a1855728028972c75e378233

Identificativo del documento digitale originale: 597108

Protocollo: AOM-0002158-2025 21-01-2025 12:35:44



U.O.C. SISTEMI INFORMATIVI



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

e, p.c. Direttore Amministrativo

SEDE

Oggetto: adempimenti ex D.Lgs.n.138 del 4/9/2024 di recepimento della Direttiva UE 2022/2555 del 14/12/2022 recante disposizioni in materia di sicurezza delle reti e delle informazioni (NIS 2) – crittografia

Richiamata la normativa in oggetto emarginata, che all'art.21 della Direttiva, rubricato *"misure di gestione dei rischi di cibersicurezza"* prescrive che *"le misure [...] comprendono almeno [...] politiche e procedure relative all'uso della crittografia"*, considerato che, per l'effetto, la piattaforma di end point XDR Sophos attiva in azienda deve essere oggetto di upgrade ed estensione con sistemi di crittografia dei files (residenti sugli end-point, trasmessi a mezzo mail, copiati su supporto rimovibile, etc.) da attivare per tutti gli host (pc, server, tablet, etc.) a dominio aziendale *"aornmoscati"*, 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
MDRCEU15AHNGAA	Central Managed Detection and Response Complete 1000-1999 users - 15 MOS - GOV	1500
MDRCSS15BDNGAA	Central Managed Detection and Response Complete Server 50-99 servers - 15 MOS - GOV	70
PRPH4500ZZPCAA	Professional Services - MDR Guided Onboarding Upgrade	1
CDEAAU15AHNGAA	Central Device Encryption - 1000-1999 clients - 15 MOS - GOV	1500

per la durata di mesi 15, fino al termine di scadenza delle licenze d'uso dell'attuale sistema XDR, per l'importo presunto di € 130.000,00 oltre IVA.

La presente richiesta, oltre a ricondursi alla normativa innanzi richiamata, riveste carattere di urgenza in relazione alla necessità di riduzione della superficie di attacco dei sistemi aziendali rispetto a potenziali minacce informatiche.

In mancanza, l'Azienda risulterebbe esposta alle minacce di utilizzo illecito di dati critici e/o sensibili in caso di evento avverso di esfiltrazione di dati residenti dagli end-point (files memorizzati localmente sui dispositivi aziendali: pc, tablet, etc.) o da questi inviati o scaricati.

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 crittografia 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

