L'Assessore alla Semplificazione Amministrativa e al Turismo

Prot. n. 2677/SP del 7 settembre 2021

Alle Direzioni Generali

Agli Uffici Speciali

e p.c. al Capo di Gabinetto

Oggetto: Processi digitali e utilizzo degli strumenti informatici.

Come è noto, il "Codice dell'amministrazione digitale" (Decreto Legislativo 7 marzo 2005, n. 82), all'articolo 2, comma 1, stabilisce che: "*Lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando, con le modalità più appropriate e nel modo più adeguato al soddisfacimento degli interessi degli utenti, le tecnologie dell'informazione e della comunicazione*" e, all'articolo 3-bis, afferma che "*chiunque ha il diritto di accedere ai servizi on-line … tramite la propria identità digitale*".

Il Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022 promuove la trasformazione digitale del Paese, favorisce l'utilizzo di piattaforme tecnologiche al fine di razionalizzare i servizi per le Pubbliche Amministrazioni ed i cittadini agevolandone una più facile interazione e - per lo sviluppo dell'informatica pubblica - fissa i principi architetturali fondamentali nonché le regole di usabilità e di interoperabilità, nella consapevolezza che, attraverso il digitale, si può favorire di molto la semplificazione reale.

La Strategia per la crescita digitale evidenzia la necessità di un ripensamento del sistema di progettazione, gestione ed erogazione dei servizi pubblici in rete: la trasformazione digitale, infatti, va intesa come cambiamento della cultura del dipendente all'interno dell'organizzazione, e non, dunque, solo come una sequenza di interventi di automazione dei processi e di integrazione dei dati. In quest'ottica si potrà stimolare un approccio proattivo e ridurre i divari informativi, potenziando la fruibilità e la comprensione delle informazioni diffuse, sia internamente che verso l'utenza esterna, al fine di migliorare i servizi resi.

A seguito della conversione del Decreto-legge 16 luglio 2020, n. 76 – ad opera della Legge 11 settembre 2020, n. 120 – sono divenute operative le norme che ridisegnano la *governance* del digitale, accelerano la digitalizzazione dei servizi pubblici e semplificano i rapporti tra cittadini e P.A., diffondendo la cultura dell'innovazione con attenzione anche all'accesso agli strumenti informatici da parte delle persone con disabilità.

Inoltre, nel corso dell'ultimo anno, l'emergenza legata al Covid-19 ha portato all'attenzione dei cittadini, delle imprese e delle PP.AA. l'importanza cruciale della connettività, dei servizi digitali e delle relative competenze.

Nell'ottica della semplificazione amministrativa e del consolidamento dell'innovazione tecnologica regionale occorre realizzare a pieno il processo di digitalizzazione dell'azione amministrativa e di implementazione dell'utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) per assicurare

80143 NAPOLI – Centro Direzionale is. C5 – Tel. 081.7968673 – 8674 – 8676 – Fax 081.7968589
e-mail: assessore.casucci@regione.campania.it

a cittadini e imprese l'effettivo esercizio del diritto all'uso delle tecnologie digitali, rendendo più efficienti i servizi resi. In proposito, giova qui richiamare due principi del suddetto Piano Triennale: "*digital & mobile first*" (per i servizi che devono essere accessibili in via esclusiva con sistemi di identità digitale assicurando almeno l'accesso tramite SPID) e "*cloud first*" (per cui le PP.AA., nella definizione di nuovi progetti e nello sviluppo di nuovi servizi, adottano primariamente il paradigma *cloud*).

Sul tema va considerato, inoltre, che l'efficacia e la diffusione delle minacce informatiche richiedono appropriate contromisure, finalizzate all'aggiornamento e all'introduzione di misure specifiche per la sicurezza informatica e per la protezione della *privacy* degli utenti.

Ciò premesso, di seguito – per ogni opportunità – si riporta una breve ricognizione di alcune semplici indicazioni relative all'uso delle risorse *ICT*: alcune di esse costituiscono, in realtà, prescrizioni enucleabili direttamente dalle vigenti norme, altre, invece, ne risultano sviluppo logico e/o esplicazione applicativa pratica e sono qui riepilogate quale mero supporto conoscitivo utile nell'ottica della realizzazione dei principi di efficacia, efficienza ed economicità dell'azione amministrativa.

1. Le credenziali di autenticazione, codice per l'identificazione dell'utente (user id) associato a una parola chiave (password) sono riservate, devono essere conosciute solamente dall'utente che non deve, in alcun caso, comunicarle a terzi.
2. La Posta Elettronica Certificata (PEC) va utilizzata soltanto nei rapporti con soggetti esterni all'Ente, privilegiandosi, invece, nelle comunicazioni c.d. "interne", l'e-mail istituzionale, strumento idoneo e sufficiente a garantire la provenienza delle comunicazioni e l'attribuibilità dei contenuti al responsabile presidio dell'intestatario della casella elettronica.
3. La comunicazione esterna, in uscita verso altre pubbliche amministrazioni, imprese, liberi professionisti e cittadini, che hanno dichiarato il proprio domicilio digitale, quando non tramite altri canali telematici, avviene esclusivamente attraverso le caselle di posta elettronica certificata istituzionali associate al sistema di protocollo.
4. Nell'ottica della compiuta realizzazione del principio "once only" e del rafforzamento dell'interoperabilità, non vanno richieste ai cittadini e alle imprese informazioni dai medesimi già fornite alla P.A.
5. Occorre evitare la pubblicazione e/o l'invio a mezzo mail di documenti-immagine (i.e. scansioni), preferendo, invece, modalità che consentano l'estrapolazione dei dati dai documenti pubblicati (fatto salvo il caso di impedimenti che possono sussistere nelle ipotesi, ad esempio, di mappe, planimetrie, etc.).
6. È superfluo stampare le PEC e le corrispondenti ricevute di accettazione e consegna, né vanno protocollate le relative copie cartacee, la validità del documento è garantita dalla sua versione digitale che è l'unica originale, quelle prodotte in versione cartacea non hanno nessun valore.
7. Allo scopo di garantire sicurezza alla rete dell'Ente, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi

80143 NAPOLI – Centro Direzionale is. C5 – Tel. 081.7968673 – 8674 – 8676 – Fax 081.7968589
e-mail: assessore.casucci@regione.campania.it

informatiche. In qualunque situazione di incertezza contattare l'Amministratore di sistema per una valutazione dei singoli casi.

8. Per la firma dei documenti va utilizzata esclusivamente la firma digitale, recando, la stessa, la validazione temporale.
9. I documenti digitali devono essere predisposti in formato accessibile di modo che siano fruibili con modalità assistive, indipendentemente da eventuali condizioni di disabilità (rif. Decreto del Ministro per l'Innovazione e le Tecnologie 8 luglio 2005 e art. 23, co. 5-bis, del CAD).
10. Per motivi di sicurezza, comprensivi tra gli altri dell'intangibilità, dell'immodificabilità e dell'accessibilità nel tempo del documento, non sono accettati documenti consultabili tramite indirizzo (link) a siti e/o domini esterni e interni. Non sono altresì accettati documenti dinamici se contenenti rinvii, in forma di indirizzi (link), a siti che rendono disponibili informazioni e/o dati che integrano o esplicano i contenuti dei documenti stessi.
11. I documenti informatici prodotti su formati diversi (ad esempio, in estensione ".doc" di Microsoft Word, ".xls" di Microsoft Excel) prima della loro sottoscrizione con firma digitale o, comunque, nel momento che si considerano perfezionati, sono convertiti nel formato PDF/A - o nei formati sopraindicati se maggiormente confacenti al tipo di documento considerato - al fine di garantirne la leggibilità, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.
12. Si raccomanda l'impiego della massima prudenza nell'uso delle attrezzature informatiche fornite dall'Amministrazione, in particolare nella navigazione in rete e nell'utilizzo della posta elettronica che deve avvenire in maniera sicura e in conformità alla c.d. "politica aziendale".
13. Ogni utente deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio responsabile e al personale addetto ai sistemi informatici verbalmente e tramite posta interna.
14. Durante le sessioni di lavoro gli strumenti elettronici non possono essere lasciati incustoditi e accessibili a terzi. Pertanto, ogni qualvolta l'utente si allontani o si assenti dalla postazione di lavoro usata per il trattamento dei dati, è tenuto a chiudere la sessione, oppure a rendere inaccessibile a terzi (ad esempio mediante l'utilizzo del salvaschermo dotato di password) la propria postazione di lavoro.
15. Al fine di proteggere i dati dal rischio di accesso abusivo e dall'azione dannosa di programmi (ad esempio virus), l'ente predispone a livello centralizzato, adeguati strumenti elettronici nonché il loro aggiornamento secondo le modalità previste dalla legge. Il personale è tenuto a segnalare ogni malfunzionamento degli strumenti antivirus ed affini e, per nessun motivo, è autorizzato a disattivarli.

Il Responsabile dell'Ufficio Speciale
Per la Crescita e la Transizione Digitale
Massimo Bisogno

Assessore
Felice Casucci

Documento firmato da:
MASSIMO BISOGNO
07.09.2021 14:16:07 UTC