DETERMINAZIONE N. 112/2021

Oggetto: Approvazione della Trattazione n. 37/2020, Invito e comunicazione riguardanti la Segnalazione al Difensore civico per il digitale n. 37/2020, prot. n. 5118 del 2020.

IL DIRETTORE GENERALE

VISTI gli articoli 19 (Istituzione dell'Agenzia per l'Italia Digitale), 21 (Organi e statuto), 22 (Soppressione di DigitPA e dell'Agenzia per la diffusione delle tecnologie per l'innovazione; successione dei rapporti e individuazione delle effettive risorse umane e strumentali) del decreto legge n. 83 del 22 giugno 2012, recante "Misure urgenti per la crescita del Paese", convertito, con modificazioni, nella legge n. 134 del 7 agosto 2012 e s.m.i. e l'articolo 14-bis (Agenzia per l'Italia digitale) nonché l'articolo 17, (Responsabile per la transizione digitale e difensore civico digitale) del decreto legislativo n.82 del 7 marzo 2005 (Codice dell'amministrazione digitale) e s.m.i. e, in particolare, il comma 1-quater del suddetto articolo 17 ai sensi del quale è istituito, presso l'AgID, l'ufficio del difensore civico per il digitale;

VISTO il decreto del Presidente del Consiglio dei Ministri dell'8 gennaio 2014 (pubblicato sulla GURI n. 37 del 14 febbraio 2014), che ha approvato lo Statuto dell'Agenzia per l'Italia Digitale (AgID);

VISTO il decreto del Presidente del Consiglio dei Ministri 9 gennaio 2015, pubblicato nella Gazzetta Ufficiale n. 82 del 9 aprile 2015, concernente la "Determinazione delle dotazioni delle risorse umane, finanziarie e strumentali dell'Agenzia per l'Italia digitale", adottato ai sensi dell'articolo 22, comma 6, del decreto-legge n. 83 del 2012;

VISTO il decreto del Presidente del Consiglio dei Ministri in data 27 marzo 2017, recante "Approvazione del regolamento di organizzazione per l'Agenzia per l'Italia Digitale";

VISTO il decreto del Presidente del Consiglio dei Ministri del 16 gennaio 2020, registrato alla Corte dei Conti in data 17 febbraio 2020 al n. 232, con il quale l'ing. Francesco Paorici è stato nominato, per la durata di un triennio, Direttore Generale dell'Agenzia per l'Italia Digitale, con decorrenza 20 gennaio 2020;

VISTA la determinazione n. 15/2018 del 26/1/2018 con la quale si stabilisce che, in attuazione dell'articolo 17 comma 1-quater del decreto legislativo n. 82/2005 e s.m.i., è istituito presso l'AgID l'Ufficio del difensore civico per il digitale, al quale è preposto il dott. Massimo Macchia, che si avvarrà del personale in servizio presso l'ufficio Affari Giuridici e Contratti e che le aree tecniche presteranno

supporto al Difensore civico digitale al fine di fornire al medesimo elementi utili in ordine alle segnalazioni ricadenti nelle aree di propria competenza;

VISTO l'articolo 66 comma 2 del d.lgs. 217/17 ove, tra l'altro, si prevede che, "*al fine di garantire una tempestiva ed efficace attuazione del decreto legislativo n. 82 del 2005, e, in particolare, di svolgere le attività previste dall'articolo 17, comma 1-quater e dall'articolo 71 del predetto decreto legislativo e le altre misure aggiuntive disposte dal presente decreto, l'AgID può avvalersi, in aggiunta alla dotazione organica vigente, di un contingente di 40 unità di personale di altre amministrazioni statali, in posizione di comando o fuori ruolo, ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127*";

VISTA la determinazione n. 37 del 12/02/2018 con la quale è stato approvato il Regolamento concernente le procedure interne all'Agenzia per l'Italia digitale aventi rilevanza esterna, finalizzate allo svolgimento, nella fase di prima applicazione, dei compiti previsti dall'articolo 17, comma 1-quater del Codice dell'Amministrazione digitale, relativi al Difensore civico per il digitale;

VISTA la segnalazione al Difensore civico per il digitale n. 37/2020 del 30/04/2020 acquisita al prot. con n. 5118 in pari data, relativa a due diverse questioni problematiche ossia la asserita mancata pubblicazione del manuale di protocollo informatico dell'amministrazione nonché il lamentato mancato rispetto dei criteri di sicurezza informatica del sito web istituzionale della medesima;

ESAMINATA la Trattazione n. 37/2020, predisposta dall'Ufficio del Difensore civico per il digitale, relativa all'istruttoria del caso sopra segnalato nella quale a seguito di approfondimenti istruttori, è emerso quanto segue.

Con riferimento al primo profilo problematico segnalato, a seguito dei riscontri alle richieste di acquisizione elementi rivolte all'amministrazione (nota prot. 2993 del 03/07/2020, acquisita agli atti di Agid al prot.n. 7699 del 06/07/2020 e nota prot. 3606 del 06/08/2020, acquisita agli atti dell'Agenzia per l'Italia digitale al prot. n. 9310 in pari data) è stato possibile appurare che l'amministrazione, pur non avendo inserito il manuale di gestione del protocollo informatico nell'ambito della pagina relativa ai propri regolamenti comunali, ha comunque provveduto a collegare il suo nuovo portale dell'amministrazione trasparente (che è sotto il dominio web del fornitore) alla pagina del proprio sito web istituzionale dedicata all'argomento.

Conseguentemente il suddetto manuale, pur trovandosi collocato sul sito del fornitore della soluzione informatica, risulta raggiungibile attraverso il sito dell'amministrazione.

Con riferimento al secondo profilo problematico segnalato, poiché il tentativo, effettuato in data 11/05/2020, di contattare il *Computer Security Incident Response Team* (CSIRT) (struttura istituita

presso il Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri, che, a partire dal 6 maggio, ha assorbito le competenze e le attività svolte dal precedente Cert-PA presso AgID) non ha sortito esito alcuno, in data 13 luglio partendo dall'osservazione che il problema di sicurezza indicato dal segnalante era probabilmente originato dalla mancata implementazione del protocollo HTTPS nel sito web in questione si provvedeva a consultare i colleghi del CERT-Agid al fine di sapere se tra le misure minime di sicurezza ICT incluse nella Circolare Agid 18 aprile 2017, n. 2/2017, ve ne fosse una che preveda esplicitamente ed espressamente l'obbligo per le pubbliche amministrazioni di adottare per i propri siti web il protocollo HTTPS al posto del protocollo HTTP.

Al riguardo è stato indicato che "non vi è nessuna misura minima che preveda espressamente l'utilizzo del protocollo HTTPS sui propri siti web". Contestualmente è stato precisato anche che "Non vi sono indicazioni poiché l'utilizzo del protocollo HTTPS è fortemente consigliato ma non è obbligatorio. Si può dire che è ormai uno standard "*de facto*" ma non "*de jure*"."

Peraltro, poiché l'osservazione di cui sopra era un semplice assunto istruttorio, considerata la perdurante assenza di riscontri da parte dello CSIRT, in data 28/10/2020, si è ritenuto opportuno chiedere ulteriore supporto tecnico ai colleghi del CERT-AgID, al fine di comprendere da cosa dipende la problematica di sicurezza che porta alla generazione del messaggio di allerta al quale il segnalante fa riferimento.

A tal proposito si è ricevuta conferma che "il sito in oggetto non è dotato di certificato SSL, motivo per cui i browser di ultima generazione emettono il messaggio di avvertimento riportato dalla segnalazione.

Per eliminare l'errore, il gestore del sito dovrebbe riconfigurare lo stesso, dotandolo di un certificato SSL in modo tale da poter avere sessioni cifrate con il protocollo HTTPS.

In questo modo, il messaggio di avvertimento viene disabilitato.".

Ne deriva che si è effettivamente in presenza di un problema tecnico di sicurezza informatica, ma, al tempo stesso, il relativo rimedio risultava solo fortemente consigliato ma non obbligatorio in quanto non incluso nelle misure minime di sicurezza informatica previste da AgID.

In materia occorre però tenere presenti anche le previsioni contenute nel Piano triennale per l'informatica nella P.A. 2020-2022; secondo quest'ultimo, infatti: "Le PA devono aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA" (ob. 6.1) e devono altresì, "aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione" (ob.6.2).

Tanto premesso, con riferimento al primo profilo problematico segnalato si propone al Difensore per il digitale di archiviare la questione; al contrario, con riferimento al secondo profilo problematico si propone di formulare un Invito all'Amministrazione a porre rimedio a quanto segnalato;

ESAMINATO l'Invito predisposto dal Difensore civico per il digitale, che approva la richiamata Trattazione n.37/2020 ritenendo fondata la Segnalazione in questione, con comunicazione al Direttore Generale per quanto di competenza e, qualora nulla osti, con invito all'Amministrazione segnalata a porre tempestivamente rimedio a quanto rappresentato, dandone comunicazione al Segnalante

DETERMINA

1) di approvare dette Trattazione n. 37/2020, Invito e comunicazione al segnalante che allegati alla presente ne formano parte integrante;

2) di autorizzare la pubblicazione dello stesso invito nella apposita Area del sito Internet dell'Agenzia.

FRANCESCO PAORICI

Firmato digitalmente da FRANCESCO PAORICI
Data: 2021.02.02 09:28:26 +01'00'

Segnalazione n.37/2020 - Trattazione

Amministrazione segnalata: Comune di Falvaterra - Qualificazione tematica: Altro - prot. n. 5118 del 2020.

Il Segnalante espone la seguente questione:

"Con la presente si segnala che tra i regolamenti pubblicati dal Comune di Falvaterra non vi è traccia del manuale di gestione del protocollo informatico (ex. art. 5 comma 3 DPCM 3 dicembre 2013, d.lgs. n. 82/2005) e navigando sul sito istituzionale del Comune il bronswer Chrome segnala che il sito non è sicuro ed invita a non inserire dati sensibili in quanto potrebbero essere intercettati da utenti malintenzionati.

Premesso quanto sopra si chiede di accertare l'esistenza del manuale di gestione del protocollo informatico comunale ed il rispetto sia della pubblicazione dello stesso che dei criteri di sicurezza del sito istituzionale.

Sicuro di un vostro veloce riscontro vi saluto cordialmente e resto a disposizione per qualsiasi ulteriore chiarimento.".

Dall'esame preliminare, emerge che il segnalante lamenta due distinte problematiche con riferimento al sito web istituzionale dell'amministrazione segnalata (raggiungibile all'indirizzo http://www.falvaterra.workmm.com), ossia la mancata pubblicazione del manuale si gestione documentale dell'amministrazione e, d'altra parte quella che sembrerebbe configurarsi come mancato rispetto della normativa in materia di sicurezza del sito web istituzionale del comune.

Al riguardo, si considera quanto segue.

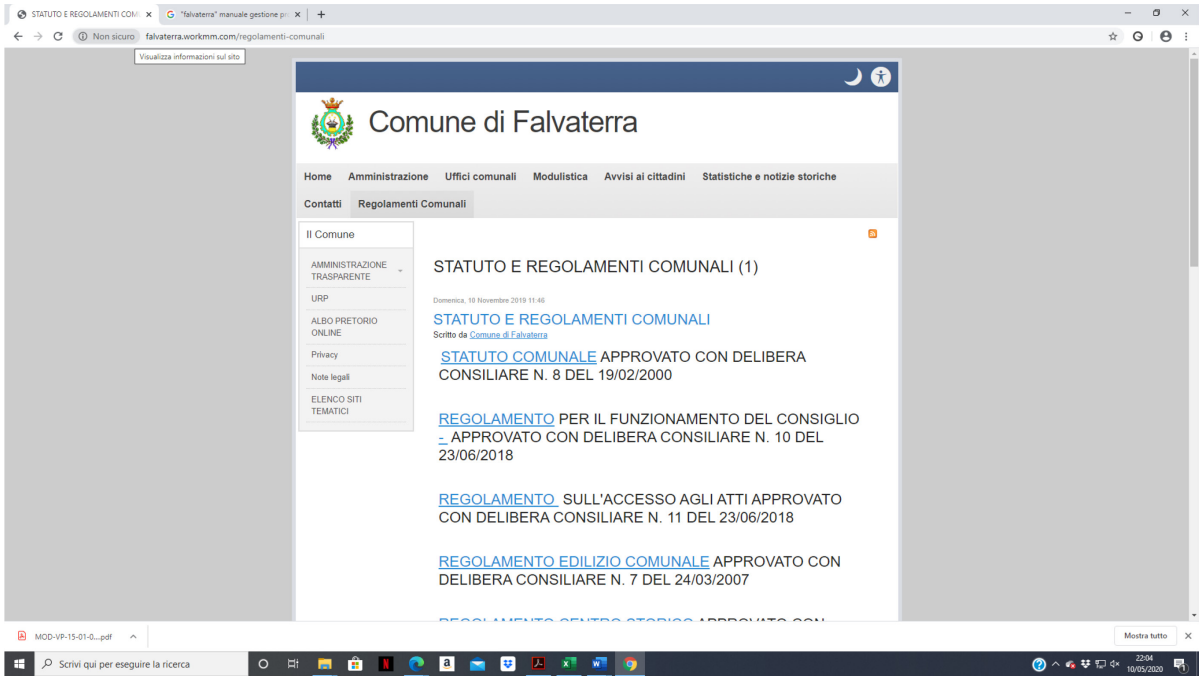
La prima problematica indicata implicherebbe il mancato rispetto del DPCM 3 dicembre 2013 (recante "*Regole tecniche sul protocollo informatico*") e, in particolare dell'articolo 5, ossia della norma che delinea il contenuto del manuale di gestione del protocollo informatico ("*Il manuale di gestione descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.*") e, tra l'altro, stabilisce che il manuale stesso venga pubblicato dalle pubbliche amministrazioni sul proprio sito web istituzionale ("*Il manuale di gestione è reso pubblico dalle pubbliche amministrazioni […] mediante la pubblicazione sul proprio sito istituzionale*.");

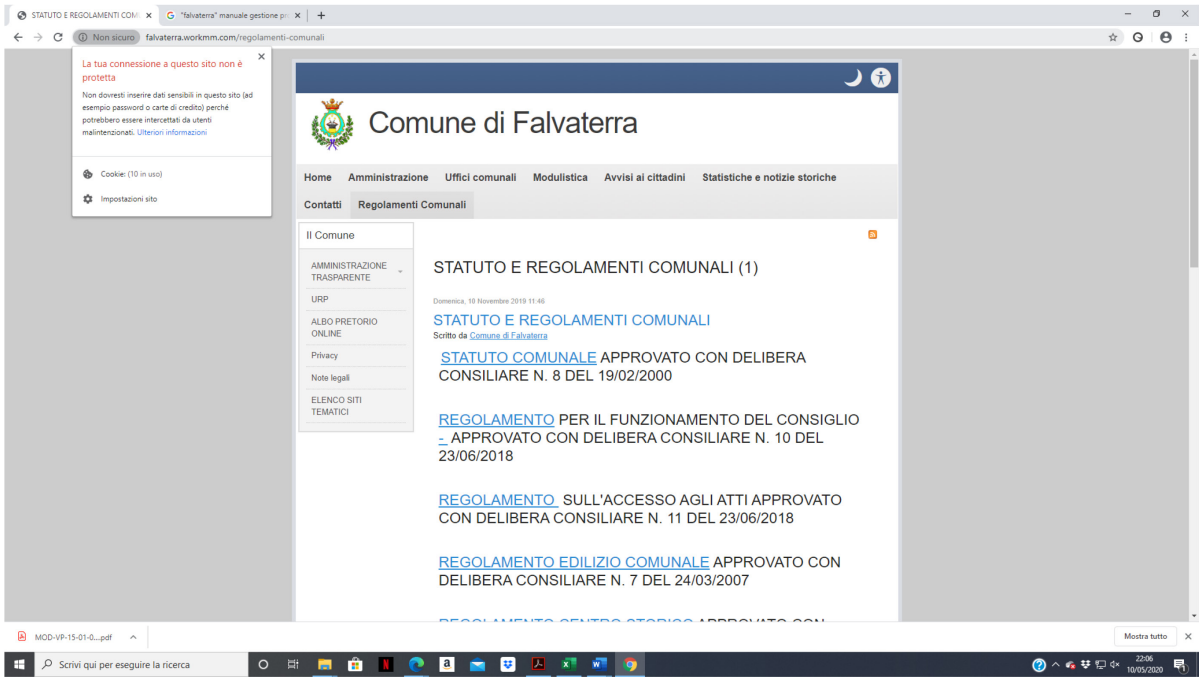
La seconda problematica indicata potrebbe configurarsi come possibile violazione della disposizione di cui all'articolo 51, comma 2 del decreto legislativo 7 marzo 2005, n.82 e s.m.i. "Codice dell'Amministrazione digitale", (di seguito CAD). Secondo tale norma

"I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.".

Si ritiene quindi che la segnalazione sia astrattamente ricevibile.

Viste le sopra richiamate norme, in avvio di istruttoria si è effettuata una ricognizione del sito web istituzionale del Comune di Falvaterra.





Poiché effettivamente nel sito indicato non è stata trovata traccia del manuale di gestione documentale ed effettivamente il sito web risulta presentare problemi di sicurezza, si propone all'ufficio del difensore civico per il digitale di procedere come segue.

Previa richiesta di supporto tecnico al *Computer security incident response team* - CSIRT italiano (di cui al decreto del presidente del consiglio dei Ministri 8 agosto 2019) per un approfondimento e una verifica circa la questione della sicurezza informatica del sito web istituzionale, predisporre, con riferimento ad entrambe le problematiche segnalate, una nota per acquisire maggiori elementi presso l'amministrazione segnalata.

Così, in data 11/05/2020, ore 11:10, si è inviata ai colleghi dell'ex Cert-PA, una richiesta di supporto di questo tenore:

"Gentili colleghi buongiorno,

so che le competenze in materia di sicurezza informatica sono passate allo CSIRT; con riferimento alla segnalazione di cui in oggetto giunta al difensore civico per il digitale e qui acclusa, vi chiedo supporto tecnico.

Qualora non possiate approfondire la questione e darmi un vostro feedback diretto al riguardo, vi chiedo la cortesia di indicarmi a chi posso rivolgermi presso lo CSIRT.".

Poco dopo i colleghi dell'ex CERT-PA fornivano la risposta interlocutoria che si riporta di seguito.

"*inoltriamo allo CSIRT la parte della segnalazione riguardante il certificato del sito in questione.*"

Da cui si desumeva la competenza della nuova struttura CSIRT al riguardo.

Peraltro, in data 29/05/2020 In assenza di riscontro dallo CSIRT per la parte di competenza, si è provveduto a trasmettere, con nota Agid prot.n. 6194, una specifica richiesta di acquisizione elementi all'amministrazione circa il manuale di gestione documentale. In proposito si precisa che la richiesta di elementi appena citata è stata reiterata (con nota Agid prot.n.7578 del 01/07/2020).

L'amministrazione segnalata ha riscontrato la richiesta (con propria nota prot. 2993 del 03/07/2020, acquisita agli atti di Agid al prot.n. 7699 del 06/07/2020), rappresentando quanto segue.

"Questa Amministrazione sta provvedendo al graduale rinnovo di tutte le procedure informatiche, affidandone la fornitura e manutenzione alla HALLEY INFORMATICA, società di indubbia notorietà ed affidabilità.
Tra le procedure si annovera anche il protocollo informatico, il cui manuale, e successivo aggiornamento, è in dotazione degli operatori ed è stato pubblicato sul sito comunale nella Sezione Trasparenza, raggiungibile al seguente link:
http://www.halleyweb.com/c060032/zf/index.php/trasparenza/index/index
Si assicura inoltre che si procederà alla puntuale pubblicazione anche dei futuri aggiornamenti del manuale. Con Osservanza.".

Dalla verifica effettuata emerge che effettivamente all'indirizzo web indicato è presente un manuale di gestione documentale (che risulta essere stato caricato on line in data 02/07/2020).

In base alle evidenze ottenute non è tuttavia chiaro quale sia stato l'iter amministrativo di adozione formale del manuale di gestione documentale in questione. E, soprattutto, si è rilevato che il link sopra riportato non risulta reperibile nel lato front-office del sito web dell'amministrazione.

A quest'ultimo riguardo in data 03/08/2020 si è pertanto inviata all'amministrazione segnalata un'ulteriore richiesta di chiarimenti (nota Agid prot. 9091). Con nota prot. 3606 del 06/08/2020 (acquisita agli atti dell'Agenzia per l'Italia digitale al prot. n. 9310 in pari data l'amministrazione ha fornito risposta rappresentando quanto segue

"A riscontro della nota di codesto Ufficio […] si precisa che, cliccando sul seguente link: http://www.halleyweb.com/c060032/zf/index.php/trasparenza/index/index si apre la schermata della sezione AMMINISTRAZIONE TRASPARENTE. Sotto tale titolo è pubblicato il MANUALE PROTOCOLLO INFORMATICO. Lo stesso manuale è consultabile altresì nella predetta AMMINISTRAZIONE TRASPARENTE alla sezione ATTI GENERALI – MANUALE PROTOCOLLO INFORMATICO, come meglio illustrato nell'allegata schermata."

A tal proposito si osserva che la schermata appena riportata pur richiamandosi esplicitamente al Comune di Falvaterra, fa tuttavia capo al dominio web della società Halley invece che al dominio web istituzionale del comune di Falvaterra.

Al riguardo si è ritenuto opportuno cercare di verificare se, ed in quali termini, la suddetta fattispecie possa configurarsi tuttora come una violazione delle indicazioni contenute nella Direttiva n.8/2009 del Ministro per la Pubblica Amministrazione e l'Innovazione "*per la riduzione dei siti web delle pubbliche amministrazioni e per il miglioramento della qualità dei servizi e delle informazioni on line al cittadino*" e dalla successiva regolamentazione attuativa; si è rilevato, infatti, che come evidenziato dalle relative linee guida sui siti web della P.A del 2011, la Direttiva "*impone agli enti pubblici di elevare lo standard qualitativo dei siti web sotto molteplici aspetti: l'aggiornamento dei contenuti, l'usabilità dei servizi, l'accessibilità del codice html, la riconoscibilità e riconducibilità del sito all'amministrazione responsabile dei contenuti pubblicati on line.".*

Nel caso di specie, infatti, proprio sotto il profilo della riconoscibilità e riconducibilità del sito all'amministrazione responsabile dei contenuti pubblicati on line, risulta essersi creato una sorta di disallineamento: emerge infatti che il manuale di protocollo è sì pubblicato in una pagina web che si riferisce all'amministrazione segnalata, ma al tempo stesso l'indirizzo web non è riconducibile ad essa, bensì al fornitore.

Al fine di determinare se i suddetti principi di riconoscibilità e riconducibilità del sito all'amministrazione responsabile dei contenuti pubblicati on line trovino tuttora riscontro in regolamentazione vigente (come ad esempio le Linee guida di design per i servizi digitali della PA) e, più in generale, al fine di ricevere un chiarimento sulla situazione tecnica della segnalazione in relazione ai riscontri ottenuti dalla P.A., in data 28/08/2020, ore 18:09, si è rivolta, tramite mail, una richiesta di

supporto al responsabile del "Servizio sviluppo web e communities"; il riscontro a tale richiesta è stato sollecitato per le vie brevi nel corso di contatti con componenti del servizio. Data l'assenza di riscontri la richiesta di supporto è stata ribadita, sempre tramite mail al responsabile del Servizio, in data 23/09/2020 ore 11:59 e poi ulteriormente reiterata in data 28/09/2020 ore 17:45, purtroppo sempre senza esito.

Tuttavia si è constatato che l'amministrazione segnalata, nel frattempo, pur non avendo inserito il manuale di gestione del protocollo informatico nell'ambito della pagina relativa ai propri regolamenti comunali ha comunque provveduto a collegare il suo nuovo portale dell'amministrazione trasparente (che è sotto il dominio web del fornitore Halleyweb) alla pagina del proprio sito web istituzionale dedicata all'argomento.

Conseguentemente il suddetto manuale, pur trovandosi collocato sul sito del fornitore della soluzione informatica, risulta ora raggiungibile attraverso il sito dell'amministrazione.

Con riferimento al secondo profilo problematico segnalato, ossia l'aspetto relativo alla sicurezza del sito web dell'amministrazione, si è constatato che il sito web istituzionale dell'amministrazione segnalata (http://www.falvaterra.workmm.com/) e la parte relativa al portale dell'amministrazione trasparente (http://www.halleyweb.com/c060032/zf/index.php/trasparenza/index/index) sono effettivamente accompagnati e caratterizzati dal messaggio di *warning* riportato dal segnalante circa la mancanza di sicurezza del sito web dell'amministrazione.

Al riguardo, vista la perdurante assenza di riscontro tecnico richiesto allo CSIRT, al fine di giungere alla definizione della relativa istruttoria in relazione a questo specifico aspetto di sicurezza, dapprima, con l'ausilio dei colleghi del CERT-AgID, si è cercato di comprendere se la questione tecnica sottesa alla segnalazione ricevuta rientrasse o meno tra le misure minime di sicurezza informatica di cui alla Circolare AgID 18 aprile 2017, n. 2/2017 (si veda mail del 13/07/2020 ore 17:14 di cui si dà conto più oltre); successivamente si è valutata l'ipotesi di provare a ricontattare comunque lo CSIRT, infine tramite mail del 28/10/2020 ore 18:29, si è chiesto un supporto tecnico ai colleghi del CERT-AgID, formulando il quesito che di seguito si riporta:

"Da cosa dipende la problematica di sicurezza che porta alla generazione del messaggio di allerta al quale il segnalante fa riferimento?"

In riscontro, si è ottenuta, tramite mail del 29/10/2020 ore 16:47, la risposta che segue

"*il sito in oggetto non è dotato di certificato SSL, motivo per cui i browser di ultima generazione emettono il messaggio di avvertimento riportato dalla segnalazione.*

Per eliminare l'errore, il gestore del sito dovrebbe riconfigurare lo stesso, dotandolo di un certificato SSL in modo tale da poter avere sessioni cifrate con il protocollo HTTPS.

In questo modo, il messaggio di avvertimento viene disabilitato.

Dovrebbe ormai essere prassi comune di chi gestisce siti web (vista la deprecazione in atto sui siti non conformi) ma, evidentemente, c'è ancora qualcuno che non se ne cura.".

In merito si è osservato che la mancata adozione del protocollo https per i siti delle P.A. non costituisce un'esplicita e chiara violazione dell'articolo 51 del CAD, avente ad oggetto la sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni; ciò in quanto se è vero che il comma 1 del suddetto articolo stabilisce quanto segue

"*Con le Linee guida sono individuate le soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture*.",

si evidenzia che, come indicato dagli stessi colleghi del CERT Agid in una precedente mail sul tema delle linee guida in materia (mail del 13/07/2020 ore 17:14), nella Circolare 18 aprile 2017, n. 2/2017 recante "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «*Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)*» "non vi è nessuna misura minima che preveda espressamente l'utilizzo del protocollo HTTPS sui propri siti web*"."*

D'altra parte, la difficoltà di individuare esattamente la norma violata non faceva venir meno la circostanza che la problematica rilevata costituisce quantomeno una mancanza in materia di sicurezza informatica (oltre che una probabile mancanza in materia di trattamento dei dati personali in base a quanto previsto dall'articolo 32, comma 1, lettera b), del GDPR e quindi eventualmente suscettibile di segnalazione al Garante).

In questo senso, si è considerato che secondo il Piano triennale per l'informatica nella P.A. 2020-2022: "Le PA devono aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA" (ob. 6.1) e devono altresì, "aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione" (ob.6.2).

Del resto la circostanza che il mancato utilizzo del protocollo HTTPS rappresenti un serio problema di sicurezza ha ricevuto conferma più generale dal monitoraggio condotto dallo stesso CERT-AgID su tutti i portali web istituzionali presenti in IPA, in ossequio a quanto previsto dallo stesso Piano triennale per l'informatica pubblica nella P.A. 2020 -2022, (https://cert-agid.gov.it/news/monitoraggio-sul-corretto-utilizzo-del-protocollo-https-e-dei-livelli-di-aggiornamento-delle-versioni-dei-cms-nei-portali-istituzionali-della-pa/).

Sulla base di tutto quanto fin qui esposto, con riferimento al profilo relativo alla pubblicazione del manuale di protocollo si propone di archiviare la segnalazione (nella misura in cui il manuale stesso pur trovandosi collocato sul sito web del fornitore della soluzione informatica, risulta ora raggiungibile attraverso il sito web istituzionale dell'amministrazione.

Con riferimento al profilo relativo alla sicurezza del sito web sulla base delle previsioni contenute nel Piano triennale sopra indicate, si propone di ritenere fondata la segnalazione relativamente all'aspetto ora in esame e conseguentemente si propone di invitare l'amministrazione segnalata a riconfigurare il proprio sito web istituzionale, dotandolo di un certificato SSL in modo tale da poter avere sessioni cifrate con il protocollo HTTPS ed inoltre a conformarsi ad ogni altra misura in materia di sicurezza informatica che dovesse essere successivamente indicata da AgID. Nell'ambito della pagina web istituzionale del CERT-AgID (https://cert-agid.gov.it/news/monitoraggio-sul-corretto-utilizzo-del-protocollo-https-e-dei-livelli-di-aggiornamento-delle-versioni-dei-cms-nei-portali-istituzionali-della-pa/) viene infatti indicato che nel corso del 2021 "AgID provvederà a inviare un report informativo alle singole organizzazioni che risulteranno al di sotto del livello atteso indicato negli obiettivi del piano triennale, in modo da intraprendere un percorso utile alla mitigazione dei problemi riscontrati.".

28/12/2020 Raffaele Montanaro

AGID
Agenzia per l'Italia Digitale

Ufficio del difensore civico per il digitale

Oggetto:Invito relativo alla Segnalazione n. 37/2020 - Amministrazione segnalata: Comune di Falvaterra - Qualificazione tematica: Altro - prot. n. 5118 del 2020.

Come è noto l'art.17, comma 1-quater, del decreto legislativo 7 marzo 2005, n.82 (CAD) prevede "È istituito presso l'AgID l'ufficio del difensore civico per il digitale, a cui è preposto un soggetto in possesso di adeguati requisiti di terzietà, autonomia e imparzialità. Chiunque può presentare al difensore civico per il digitale, attraverso apposita area presente sul sito istituzionale dell'AgID, segnalazioni relative a presunte violazioni del presente Codice e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione da parte dei soggetti di cui all'articolo 2, comma 2. Ricevuta la segnalazione, il difensore civico, se la ritiene fondata, invita il soggetto responsabile della violazione a porvi rimedio tempestivamente e comunque non oltre trenta giorni. Le decisioni del difensore civico sono pubblicate in un'apposita area del sito Internet istituzionale. Il difensore segnala le inadempienze all'ufficio competente per i procedimenti disciplinari di ciascuna amministrazione.". La determinazione AgID n.15/2018 del 26/1/2018 ha stabilito che, in attuazione del richiamato art.17, comma 1-quater del CAD, è istituito presso l'Agid l'Ufficio del difensore civico per il digitale.

Con segnalazione pervenuta ad AgID il 30/04/2020, acquisita al protocollo in pari data, con prot. 5118, si lamenta, tra l'altro, il mancato rispetto dei criteri riguardanti la sicurezza informatica del sito web istituzionale . A seguito dell'istruttoria effettuata dagli Uffici dell'Agenzia e delle relative risultanze conclusive, si è effettivamente riscontrato quanto segnalato.

Si ritiene, pertanto, fondata la richiamata Segnalazione e si invita codesta Amministrazione "a porvi rimedio tempestivamente e comunque non oltre trenta giorni", provvedendo a riconfigurare il proprio sito web istituzionale, dotandolo di un certificato SSL in modo tale da poter avere sessioni cifrate con il protocollo HTTPS, dandone conferma alla scrivente Agenzia. Si rappresenta che, in caso di mancato tempestivo riscontro, il presente invito è da considerare anche quale segnalazione dell'inadempienza all'Ufficio competente per i procedimenti disciplinari di codesta Amministrazione, ai sensi dell'art.17, comma 1 quater del C.A.D. Il mancato avvio delle attività necessarie a porre rimedio e il mancato rispetto del termine perentorio per la loro conclusione rileva ai fini della misurazione e della valutazione della performance individuale dei dirigenti

responsabili e comporta responsabilità dirigenziale e disciplinare ai sensi degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165

Cordiali saluti

Massimo Macchia

AGID
Agenzia per l'Italia Digitale

Ufficio del difensore civico per il digitale

Oggetto: Segnalazione n. 37/2020 - Amministrazione segnalata: Comune di Falvaterra - Qualificazione tematica: Altro - prot. n. 5118/2020.

Gent.mo segnalante, si riporta quanto da Lei segnalato:

"Con la presente si segnala che tra i regolamenti pubblicati dal Comune di Falvaterra non vi è traccia del manuale di gestione del protocollo informatico (ex. art. 5 comma 3 DPCM 3 dicembre 2013, d.lgs. n. 82/2005) e navigando sul sito istituzionale del Comune il bronswer Chrome segnala che il sito non è sicuro ed invita a non inserire dati sensibili in quanto potrebbero essere intercettati da utenti malintenzionati. Premesso quanto sopra si chiede di accertare l'esistenza del manuale di gestione del protocollo informatico comunale ed il rispetto sia della pubblicazione dello stesso che dei criteri di sicurezza del sito istituzionale. Sicuro di un vostro veloce riscontro vi saluto cordialmente e resto a disposizione per qualsiasi ulteriore chiarimento.".

Si premette che il Difensore civico per il digitale ha il compito di raccogliere tutte le segnalazioni relative alle presunte violazioni del Codice dell'Amministrazione Digitale, o di ogni altra norma in materia di digitalizzazione ed innovazione, a garanzia dei diritti digitali dei cittadini e delle imprese. L'Ufficio del difensore civico per il digitale è stato istituito presso AgID con l'articolo 17, comma 1-quater del Codice dell'Amministrazione Digitale. I principali ambiti di tutela per il cittadino e le imprese riguardano l'uso delle tecnologie, l'identità digitale, il domicilio digitale, i pagamenti con le modalità informatiche e la comunicazione mediante le tecnologie dell'informazione. Si specifica che il Difensore non risolve o media eventuali controversie tra il cittadino e la pubblica amministrazione; non può sostituirsi alla pubblica amministrazione nell'espletamento dell'attività richiesta dal cittadino; non svolge attività di supporto riguardo il malfunzionamento di soluzioni applicative utilizzate dalle pubbliche amministrazioni per l'erogazione di servizi on line (non è un servizio di help desk); non sostituisce l'Ufficio per i rapporti con il pubblico presente in ciascuna amministrazione.

Per quanto riguarda la Sua Segnalazione, scusandoci sentitamente per il ritardo nella risposta conseguente a disguidi interni, con riferimento alla prima problematica segnalata, La informiamo che a seguito di richiesta chiarimenti inviata dallo scrivente Ufficio, l'Amministrazione segnalata,

con nota 3606/2020 (acquisita agli atti dell'Agenzia per l'Italia digitale al prot. n. 9310 in pari data l'amministrazione ha fornito risposta rappresentando quanto segue

"*A riscontro della nota di codesto Ufficio […] si precisa che, cliccando sul seguente link: http://www.halleyweb.com/c060032/zf/index.php/trasparenza/index/index si apre la schermata della sezione AMMINISTRAZIONE TRASPARENTE. Sotto tale titolo è pubblicato il MANUALE PROTOCOLLO INFORMATICO. Lo stesso manuale è consultabile altresì nella predetta AMMINISTRAZIONE TRASPARENTE alla sezione ATTI GENERALI – MANUALE PROTOCOLLO INFORMATICO, come meglio illustrato nell'allegata schermata.*"

Inoltre, si precisa che si è constatato che l'amministrazione segnalata, ha successivamente provveduto a collegare il suo nuovo portale dell'amministrazione trasparente alla pagina del proprio sito web istituzionale dedicata all'argomento.

Conseguentemente il suddetto manuale risulta raggiungibile attraverso il sito dell'amministrazione.Pertanto, questo specifico aspetto è stato ritenuto risolto.

Con riferimento al secondo aspetto segnalato sostanzialmente riconducibile al mancato rispetto della disciplina in materia di sicurezza informatica del sito web istituzionale si informa che questo Ufficio, a seguito dell'istruttoria effettuata, ha ritenuto fondata la sua segnalazione ed ha pertanto proceduto all'invio ddell'Invito n. all'Amministrazione segnalata al fine di invitare la stessa a porre rimedio tempestivamente a quanto riscontrato. Nell'invito richiamato si rappresenta che, in caso di mancato tempestivo riscontro, lo stesso invito è da considerare anche quale segnalazione dell'inadempienza all'Ufficio competente per i procedimenti disciplinari dell'Amministrazione, ai sensi dell'art.17, comma 1 quater del C.A.D. Il mancato avvio delle attività necessarie a porre rimedio e il mancato rispetto del termine perentorio per la loro conclusione rileva ai fini della misurazione e della valutazione della performance individuale dei dirigenti responsabili e comporta responsabilità dirigenziale e disciplinare ai sensi degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165.

Cordiali saluti

Massimo Macchia