



Autorità per l'Informatica nella Pubblica Amministrazione

RACCOMANDAZIONE n. 1/2000

Norme provvisorie in materia di sicurezza
dei siti Internet delle Amministrazioni Centrali e degli Enti Pubblici

Capo I

PROCEDURA ORGANIZZATIVA ED AMMINISTRATIVA

Articolo 1

1. I siti delle Amministrazioni Centrali e degli Enti Pubblici con connessione telematica TCP/IP (Internet), prevedendone la naturale evoluzione verso livelli di sempre maggiore interattività, sono funzionalmente classificati in due tipologie:
 - a) siti di informazione non connessi con sistemi informativi delle Amministrazioni Centrali e degli Enti Pubblici:
 - I) destinati al dialogo con i cittadini mediante dati, notizie, informazioni la cui conoscenza può avere interesse o utilità per chi vi accede;
 - II) caratterizzati da un flusso informativo monodirezionale dall'amministrazione verso l'utente;
 - b) siti di servizio connessi con sistemi informativi delle Amministrazioni Centrali e degli Enti Pubblici che permettono al cittadino di:
 - I) intrattenere rapporti ufficiali con l'amministrazione, mediante l'inoltro telematico di denunce, dichiarazioni annuali ed altri atti previsti per legge;
 - II) ottemperare ad altri adempimenti normativi.
2. Per quanto concerne i siti indicati al punto b del comma 1, oltre a quanto previsto nella presente raccomandazione, considerata l'avvenuta attivazione della rete unitaria, saranno oggetto di specifico provvedimento atto a disciplinare il loro funzionamento e garantire le funzionalità di sicurezza e riservatezza.

Articolo 2

1. Le raccomandazioni descritte negli articoli seguenti devono essere rispettate dalle Amministrazioni Centrali ed Enti Pubblici, a prescindere dal fatto che la gestione e la manutenzione del sito Internet venga effettuata in proprio o venga affidata – anche solo in parte – a fornitore esterno; in questo ultimo caso specifiche caratteristiche di sicurezza, descritti negli articoli seguenti della presente raccomandazione, dovranno essere parte ineludibile degli accordi contrattuali tra committente e fornitore in ragione dell'architettura hardware e software del sito.
2. La mancata assicurazione di prescrizioni di sicurezza da parte del fornitore terzo:
 - a) dovrà dar luogo alla rivisitazione degli accordi in essere,
 - b) potrà determinare la revisione delle condizioni stabilite negli accordi vigenti in ordine alle prestazioni già pattuite o già in fase di somministrazione.
3. La mancata adesione alle indicazioni di cui al comma 2 del presente articolo può determinare la corresponsabilità dell'Amministrazione o Ente nelle conseguenze di un eventuale incidente.

Articolo 3

1. Le Amministrazioni Centrali e gli Enti interessati devono provvedere ad individuare i soggetti preposti al presidio del sito Internet, assicurandone la reperibilità per ogni eventuale esigenza di tempestivo intervento.
2. L'elenco delle utenze telefoniche, fisse e radiomobili, corrispondenti agli uffici o strutture preposte al presidio del sito, dovrà essere comunicato, completo delle modalità di rintraccio, all'Autorità per l'Informatica nella P.A., così da permettere eventuali comunicazioni in caso di emergenza.

Articolo 4

1. In attesa della diramazione del regolamento definitivo concernente gli aspetti di sicurezza, affidabilità, integrità e continuità di esercizio dei siti «web» pubblici e delle altre realtà di connessione telematica TCP-IP aperte al pubblico, le Amministrazioni Centrali dovranno provvedere
 - a) alla verifica delle misure di protezione adottate, in accordo con le indicazioni riportate nelle «Linee guida per la definizione di un piano per la sicurezza» pubblicate nel n° 2 ottobre 1999 de «I Quaderni» A.I.P.A.;
 - b) alla compilazione del questionario (che costituisce l'allegato 1 alla presente raccomandazione) predisposto per:
 - 1) agevolare la ricognizione dello stato di fatto,

- II) costituire la base di lavoro per le necessarie iniziative di manutenzione e miglioramento della sicurezza.
2. Il questionario sarà inoltrato a:
- Al Responsabile del Progetto intersettoriale Sicurezza Informatica
Autorità per l'Informatica nella Pubblica Amministrazione
Via Isonzo 21b, 00198 Roma
- Oppure inviato per e-mail all'indirizzo: sicurezza@aipa.it
- Il Responsabile del Progetto intersettoriale Sicurezza Informatica:
- a) provvederà a valutare le garanzie prospettate;
 - b) sottoporrà all'Adunanza dell'Autorità:
 - I) l'esito delle attività svolte,
 - II) le eventuali proposte di intervento,
 - III) ogni altra iniziativa che riterrà necessaria per la salvaguardia del sito considerato e delle relative informazioni.

Capo II

PROCEDURA DI MONITORAGGIO

Articolo 5

- 1. Il responsabile del sistema informativo dell'Amministrazione o Ente deve concordare con il gestore del sito Internet (o «webmaster»):
 - a) la predisposizione di un «log server», ovvero di un apparato destinato
 - I) a registrare tutti gli eventi telematici che hanno impatto sul sito,
 - II) a permettere la ricostruzione di eventuali comportamenti insidiosi e l'individuazione di possibili responsabilità penali e civili conseguenti condotte illecite in danno al sito;
 - b) le modalità di monitoraggio delle pagine multimediali con particolare riguardo:
 - I) alla corretta funzionalità e aggiornamento continuo dell'hardware e del software del server,
 - II) alla efficienza dei servizi erogati «On line»,
 - III) alla integrità dell'architettura del sito WEB,
 - IV) alla integrità dei contenuti.

Articolo 6

- 1. In caso di incidenti il gestore del sito redige un rapporto scritto in cui analizza e riepiloga gli eventi che hanno causato l'interruzione di servizio.
- 2. Il rapporto, che può essere costituito da un prospetto riepilogativo realizzato con sistemi informatici, deve riportare:
 - a) il numero di accessi indebiti o tentativi di accesso indebito

- b) con evidenza:
 - b.1 del numero IP dell'apparato con cui sono stati effettuati gli accessi o i tentativi,
 - b.2 del numero della porta su cui è stata eseguita l'attività non ammessa,
 - b.3 della tipologia di azione perpetrata,
 - b.4 delle conseguenze tecniche dell'accaduto,
 - b.5 dei tempi di rilevazione dell'incidente,
 - b.6 dei tempi di ripristino,
 - b.7 del numero delle precedenti connessioni effettuate o tentate dal numero IP in questione,
 - b.8 del numero di tentativi analoghi per metodologia,
 - b.9 di altre anomalie riscontrate.
 - 3. Il rapporto deve essere recapitato al Responsabile del Sistema informativo – o alla struttura da questo delegata alla sicurezza – dell'Amministrazione Centrale e dell'Ente Pubblico oggetto dell'incidente o attacco, entro e non oltre le 24 ore successive all'anomalia o incidente.
Copia del rapporto deve essere inviata immediatamente a:
Al Responsabile del Progetto intersettoriale Sicurezza Informatica
A.I.P.A. Autorità per l'Informatica nella Pubblica Amministrazione
Via Isonzo 21b, 00195 Roma
- Oppure inviato per e-mail all'indirizzo:
sicurezza@aipa.it
- 3. Il Responsabile del Progetto Intersettoriale Sicurezza Autorità per l'Informatica nella Pubblica Amministrazione offrirà supporto tecnico per la disamina dell'accaduto.

Articolo 7

- 1. Le Amministrazioni Centrali e gli Enti Pubblici devono concordare con il gestore del sito le modalità di
 - a) intervento immediato,
 - b) ripristino delle funzionalità.
- 2. Le indicazioni di massima in ordine alle relative procedure di emergenza sono descritte nei successivi Capi delle presenti norme.

Capo III

PROCEDURA DI INTERVENTO E RIPRISTINO

Articolo 8

1. In caso di incidente il gestore deve provvedere
 - a) all'immediata sospensione del collegamento del sito web coinvolto nell'incidente.
 - b) alla comunicazione telefonica al responsabile del sistema informativo dell'Amministrazione o Ente, facendo riserva di tempestivo invio del rapporto di cui all'articolo 6,
 - c) alla attivazione delle iniziative per il ripristino delle ordinarie funzionalità.
 - d) ad informare l'Autorità Giudiziaria se si ravvisa condotta dolosa

Articolo 9

1. Le attività innescate in conseguenza dell'incidente devono essere verbalizzate, con la descrizione di
 - a) azioni cui si è dato corso,
 - b) figure professionali coinvolte, con indicazione dei rispettivi compiti svolti nella specifica occasione,
 - c) fasi operative e relativo sviluppo,
 - d) sintesi di ricostruzione della dinamica offensiva con indicazione dei tempi impiegati da chi ha operato l'attacco,
 - e) indicazione degli oneri sostenuti per il ripristino,
 - f) stima degli eventuali danni subiti.
 - g) dandone comunicazione a:

Al Responsabile del Progetto intersettoriale Sicurezza Informatica
Autorità per l'Informatica nella Pubblica Amministrazione
Via Isonzo 21b, 00198 Roma

Oppure inviato per e-mail all'indirizzo:
sicurezza@aipa.it

capo IV
PROCEDURA DI CERTIFICAZIONE

Articolo 10

1. Il gestore del sito deve offrire garanzia scritta dell'impegno espletato a tutela delle relative informazioni, così da autocertificare la rispondenza del sito ai requisiti di sicurezza e delle procedure in osservanza della tempestività e della professionalità.
2. Nel caso il gestore sia esterno all'Amministrazione, tale garanzia dovrà essere prevista contrattualmente.



Autorità per l'Informatica nella Pubblica Amministrazione
PROGETTO INTERSETTORIALE «SICUREZZA INFORMATICA»

questionario

stato dell'arte in materia di sicurezza dei siti Internet
delle Amministrazioni e degli Enti pubblici

Amministrazione

--

Riferimenti dei soggetti preposti al presidio del sito internet

Cognome e nome	Utenze telefoniche di reperibilità	Ufficio di appartenenza

l'Amministrazione/Ente dispone di un sito web o di altri servizi telematici attraverso la rete Internet?

	<i>commenti</i>
sì, ed è attualmente in funzione	<i>fornire indicazioni sulla consistenza del patrimonio informativo «online», sulla frequenza di aggiornamento, sulle autorizzazioni ad agire sulle pagine in linea</i>
sì, ed è in fase di allestimento	
ha acquisito il dominio ma al momento il sito non è attivo	
ha pianificato la realizzazione entro	
altro	

quali tipi di servizio sono stati resi disponibili o sono stati pianificati?

	<i>commenti</i>
web	<i>fornire succinte informazioni</i>
posta elettronica	
DNS	
news	
ftp	
altro	
altro	
altro	
altro	
altro	

da chi sono gestiti i servizi Internet?

	<i>commenti</i>
con risorse proprie centralizzate	
con risorse proprie distribuite e coordinate	
con incarico a struttura esterna che gestisce anche il sistema informativo	
con incarico ad altra struttura esterna	
altro	
altro	
altro	

si dispone, all'interno dell'Amministrazione, di personale con competenze tecniche specializzate per operare in questo ambito?

	<i>commenti</i>
in fase di addestramento	
di elevata preparazione e in condizioni di operatività immediata	
di estrema qualificazione professionale e in servizio attivo in altro settore	
di specifica formazione e in servizio nell'ambito in argomento	
di capacità tecniche e comunicative tali da poter addestrare altro personale	
altro	
altro	
altro	
altro	

come è assicurata la reperibilità del personale (interno ed esterno) in caso di emergenza e quali sono le modalità di attivazione?

	<i>commenti</i>
è previsto un turno di servizio del personale interno a presidio delle risorse «on-line»	<i>indicare la consistenza delle risorse umane disponibili complessivamente e per singolo turno</i>
il contratto stipulato con il terzo gestore del sito prevede il controllo costante delle risorse in Internet e la possibilità di intervento immediato	<i>riportare le clausole contrattuali, specificando i termini di intervento e le eventuali penali in caso di mancato adempimento agli obblighi pattuiti</i>
il contratto stipulato con il terzo gestore del sito prevede il controllo ciclico delle risorse in Internet e il rintraccio degli operatori è assicurato dal fornitore del servizio	<i>riportare le clausole contrattuali, specificando i termini di intervento e le eventuali penali in caso di mancato adempimento agli obblighi pattuiti</i>

come è assicurata la procedura d'emergenza?

<p>il sistema informativo è stato impostato per attivare una procedura di emergenza in caso di attacco e provvede allo «shut down» o spegnimento automatico del server e alla chiusura delle sessioni</p>	<p><i>indicare le modalità di rilevazione dell'attacco o dell'eventuale anomalia e descrivere la procedura di disattivazione del sito</i></p>
<p>il sistema informativo – nell'ipotesi di aggressione telematica – è in grado di segnalare al personale incaricato l'urgenza di intervento</p>	<p><i>specificare le modalità di esecuzione (SMS, chiamata su telefono cellulare, chiamata su telefono abitazione o altra utenza...)</i></p>
<p>altro</p>	
<p>altro</p>	
<p>altro</p>	

Esiste la necessità di fornire servizi al cittadino attingendo i dati dal sistema informativo interno? quale soluzione è stata adottata?

collegamento alla rete interna	
collegamento a basi dati interne o replicate	
altro	
altro	
altro	
altro	
altro	
altro	
altro	

quale architettura tecnologica di sicurezza di supporto è stata adottata?

	<i>commenti</i>
firewall	indicare l'architettura, il software in uso e le patches installate
antivirus	indicare il tipo di prodotto, l'architettura funzionale, il livello di aggiornamento (modalità di esecuzione e frequenza)
IDS (intrusion detection system)	indicare il tipo di prodotto, l'architettura funzionale, il livello di aggiornamento (modalità di esecuzione e frequenza)
procedure organizzative	
regolamenti e altre disposizioni	
altro	
altro	

quali sono i sistemi operativi, interni e/o esterni, impiegati nei servizi su Internet?

compilare una scheda per ciascun tipo di servizio/apparato

Servizio/apparato	
	<i>commenti</i>
sistema operativo /sistemi operativi	
versione	
patches installate (versione e numero)	
vincoli all'eventuale utilizzo di versioni più recenti	
previsione di sostituzione a breve termine	
altro	
altro	
altro	

qual è la piattaforma software impiegata per l'ambiente Web?

	<i>commenti</i>
software di gestione	
versione del software	
patches installate (versione e numero)	
vincoli all'eventuale utilizzo di versioni più recenti	
previsione di sostituzione a breve termine	
altro	
altro	
altro	

qual è la piattaforma software impiegata per l'ambiente DNS?

	<i>commenti</i>
software di gestione	
versione del software	
patches installate (versione e numero)	
vincoli all'eventuale utilizzo di versioni più recenti	
previsione di sostituzione a breve termine	
altro	
altro	

qual è la piattaforma software impiegata per il servizio di posta elettronica?
(protocollo SMTP)

	<i>commenti</i>
software di gestione	
versione del software	
patches installate (versione e numero)	
vincoli all'eventuale utilizzo di versioni più recenti	
previsione di sostituzione a breve termine	
altro	
altro	

qual è la piattaforma software impiegata per il servizio di News? (protocollo NNTP)

	<i>commenti</i>
software di gestione	
versione del software	
patches installate (versione e numero)	
vincoli all'eventuale utilizzo di versioni più recenti	
previsione di sostituzione a breve termine	
altro	
altro	

qual è la piattaforma software impiegata per il servizio di File transfert? (protocollo FTP)

	<i>commenti</i>
software di gestione	
versione del software	
patches installate (versione e numero)	
vincoli all'eventuale utilizzo di versioni più recenti	
previsione di sostituzione a breve termine	
altro	
altro	

qual è la piattaforma software impiegata per il servizio di WEB (Hypertext)?
(protocollo HTTP)

	<i>commenti</i>
software di gestione	
versione del software	
patches installate (versione e numero)	
vincoli all'eventuale utilizzo di versioni più recenti	
previsione di sostituzione a breve termine	
altro	
altro	

Utilizzo dei «log» di sistema?

	<i>commenti</i>
registrazione delle attività svolte sul sistema informativo	
analisi periodica del log a scopo preventivo	
protezione dei log dal rischio di indebito accesso e modifica del contenuto anche da parte dell'amministratore di sistema	
altro	
altro	
altro	

Predisposizione e caratteristiche dei meccanismi di salvataggio e/o «back-up»?

	<i>commenti</i>
le procedure di back-up riguardano i dati	
le procedure di back-up interessano le procedure	
sono state previste risorse per assicurare la continuità costante (back-up «a caldo»)	
sono stati installati gli impianti di sicurezza a prevenzione dei rischi fisici	<i>specificare quali tipi di impianto sono disponibili (condizionamento, antincendio, antiallagamento...)</i>
Modalità di conservazione delle copie di back-up	
È prevista la procedura di rotazione temporale delle copie di back-up?	
altro	

considerato il rischio di intrusione nelle procedure e nelle basi di dati nel corso delle attività tecniche di manutenzione e revisione, quali iniziative mirate a prevenire l'indebita diffusione di tecnologia intangibile sono state attivate in occasione delle attività di adeguamento dei sistemi informativi per il Millennium Bug?

	<i>commenti</i>
nessuna	
le attività tecniche hw e sw sono state svolte da personale certificato	
le attività tecniche hw e sw si sono svolte sotto il controllo dell'amministrazione o ente	
le attività tecniche hw e sw sono state oggetto di controllo sistematico	
le attività tecniche hw e sw sono state oggetto di controllo a campione	
è stata pianificata la revisione dei sistemi a missione critica	
è previsto il monitoraggio degli accessi da remoto	
altro	

--