Indice dei contenuti

GENERALITÀ

1. ASPETTI DI SICUREZZA INERENTI LA FORMAZIONE DEI DOCUMENTI

2. ASPETTI DI SICUREZZA INERENTI LA GESTIONE DEI DOCUMENTI

3. COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

4. COMPONENTE FISICA, LOGICA ED INFRASTRUTTURALE DELLA SICUREZZA

5. LE REGISTRAZIONI DI SICUREZZA

6. ASPETTI DI SICUREZZA INERENTI LA TRASMISSIONE DEI DOCUMENTI

7. ASPETTI DI SICUREZZA INERENTI L'INTEROPERABILITÀ DEL P.d.P

8. ASPETTI DI SICUREZZA INERENTI LA TRASMISSIONE DEI DOCUMENTI ALL' INTERNO DELLA AOO

9. ACCESSO AI DOCUMENTI INFORMATICI

10. ACCESSO AL REGISTRO DI PROTOCOLLO PER UTENTI INTERNI ALLA AOO

11. UTENTI ESTERNI ALLA AOO - ALTRE AOO/AMMINISTRAZIONI O PRIVATI

Firmato digitalmente da FILISETTI MARCO UGO
ND: c=IT, o=MINISTERO ISTRUZIONE UNIVERSITA' E RICERCA/80185250588, cn=FILISETTI MARCO UGO, serialNumber=IT:FLSMCG56B07A794A, givenName=MARCO UGO, sn=FILISETTI, dnQualifier=3588568
Data: 2015.10.09 16:41:02 +02'00'

GENERALITÀ

Il piano di sicurezza definisce misure che riguardano la/il:

- protezione periferica della Intranet dell'amministrazione/AOO;
- protezione dei sistemi di acceso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno *trimestrale* durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- conservazione, a cura dei gestori del S.I. del M.I.U.R., delle copie di riserva dei dati e dei documenti, in locali diversi e, se possibile, lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad *es. separazione della parte anagrafica da quella "sensibile*") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I dati personali o le user ID di accesso, registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzati saranno consultati solo in caso di necessità dal RSP e dal titolare dei dati e, ove previsto, dalle FF.OO ed Autorità giudiziarie.

1. ASPETTI DI SICUREZZA INERENTI LA FORMAZIONE DEI DOCUMENTI

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

• l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;

• la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;

• l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;

• l'accesso ai documenti informatici tramite sistemi informativi automatizzati;

• la leggibilità dei documenti nel tempo;

• l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti informatici prodotti dall'AOO con l'ausilio di applicativi di videoscrittura o *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e riservatezza, il documento va sottoscritto con firma digitale. Nel caso in cui il documento informatico sia prodotto in modo automatico dai S.I. del MIUR, la sottoscrizione dello stesso avviene "a mezzo stampa" ai sensi dell'art. 3 comma 2 della L. n. 39/1993.

Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).

L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

2. ASPETTI DI SICUREZZA INERENTI LA GESTIONE DEI DOCUMENTI

I sistemi che ospitano i documenti sono configurati in modo tale da consentire:

• l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;

• la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

• garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;

• garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;

•fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;

• consente il reperimento delle informazioni riguardanti i documenti registrati;

• consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;

• garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

3. COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informatico dell'amministrazione.

Il DM 26 settembre 2014 ad oggetto "Individuazione degli uffici di livello dirigenziale non generale dell'Amministrazione Centrale del MIUR", attribuisce sia la pianificazione, gestione e sviluppo del sistema informativo che la gestione della sicurezza, fruibilità e accessibilità delle procedure del sistema informativo, anche in attuazione di quanto alla legge del 9 gennaio 2004, n 4, all'Ufficio III della Direzione Generale per i contratti, gli acquisti per i servizi e la Statistica.

La conduzione e la gestione tecnico-operativa del sistema di sicurezza sono attribuibili a specifiche professionalità appartenenti ai gestori del S.I. del MIUR.

4. COMPONENTE FISICA, LOGICA ED INFRASTRUTTURALE DELLA SICUREZZA

I gestori del S.I. del MIUR possono essere affidatari in particolare delle seguenti componenti ed attività:

- controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico e le misure di sicurezza fisica;
- verifica dei requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni acquisite attraverso gli strumenti di gestione documentale (protocollo informatico, PEC e PEO);
- tenuta delle registrazioni di sicurezza (informazioni di qualsiasi tipo - ad es. dati o transazioni - presenti o transitate sul PdP) che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

5. LE REGISTRAZIONI DI SICUREZZA

Le registrazioni di sicurezza sono costituite:

• dai log di sistema generati dal sistema operativo;

• dai log dei dispositivi di protezione periferica del sistema informatico [Intrusion Detection System (IDS), sensori di rete e firewall];

• dalle registrazioni del PdP.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RSP e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

6. ASPETTI DI SICUREZZA INERENTI LA TRASMISSIONE DEI DOCUMENTI

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo, trattenere per se o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate a essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (*provider*) di cui si avvale l'amministrazione oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

• accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;

• tracciamento delle attività nel file di log tenuti dal provider;

• gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, può essere utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

7. ASPETTI DI SICUREZZA INERENTI L'INTEROPERABILITÀ DEL P.d.P

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del TUDA).

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla normativa di settore vigente.

8. ASPETTI DI SICUREZZA INERENTI LA TRASMISSIONE DEI DOCUMENTI ALL'INTERNO DELLA AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.

9. ACCESSO AI DOCUMENTI INFORMATICI

Il controllo degli accessi è il processo che garantisce agli utenti autorizzati l'impiego del sistema di protocollo informatico secondo le abilitazioni ad essi assegnate.

Le credenziali di accesso al sistema sono del tutto personali e il loro uso ricade sotto la responsabilità di ciascun utente cui sono assegnate. Il personale abilitato è tenuto alla diligente custodia delle credenziali che ai sensi dell'art. 1 co. 1 lett. p del CAD sono assimilabili ad una firma elettronica e quindi incedibili.

Per accedere al sistema ogni utente deve disporre di:

- **PROFILO:** autorizzazioni concesse dal responsabile del servizio;
- **USER_ID:** identifica l'utente mediante i dati personali, (solitamente C.F.);
- **PASSWORD:** stringa segreta e riservata all'utente che, in combinazione con il ruolo, consente di accedere al sistema. Essa è associata allo *user_id.*

Avvalendosi dei privilegi amministrativi, il RDS assegna ad ogni utente un profilo secondo le esigenze eventualmente prospettategli formalmente dal titolare di ciascuna UO/AOO.

Resta inteso che ogni persona fisica può ricoprire più ruoli mantenendo comunque, la stessa *password* di accesso legata, quest'ultima, al proprio *user_id.*

Il controllo degli accessi è pertanto, assicurato utilizzando le credenziali di accesso e un sistema di autorizzazione basato sulla profilatura degli utenti in via preventiva.

Le regole per la composizione delle password delle utenze sono in ***allegato n. 6.***

Non è consentito altresì, cedere a terzi le credenziali personali di accesso alla propria postazione di lavoro, alla posta elettronica ed agli applicativi di gestione dei flussi documentali.

Eventuali eccezioni vanno segnalate ed opportunamente formalizzate, informando sempre gl'interessati.

Il PdP adottato dall'amministrazione:

• consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente;

• assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UO, salvo diversa autorizzazione configurata sull'applicativo di protocollo informatico.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso.

10. ACCESSO AL REGISTRO DI PROTOCOLLO PER UTENTI INTERNI ALLA AOO

L'accesso ai registri di protocollo è consentito al personale specificatamente indicato in un dedicato allegato del manuale di AOO.

La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal sistema attraverso l'uso di profili e password, o altre tecniche e dispositivi di autenticazione sicura. La registrazione di protocollo effettuata da chiunque associa un livello di riservatezza per il documento in esame, applicato automaticamente dal sistema. In modo analogo, l'ufficio che effettua

l'operazione di apertura di un nuovo fascicolo ne determina anche il livello di riservatezza. Per quanto concerne i documenti sottratti all'accesso, si rinvia allo specifico regolamento per l'accesso degli atti.

11. UTENTI ESTERNI ALLA AOO - ALTRE AOO/AMMINISTRAZIONI O PRIVATI

Attualmente, fatta eccezione per la gestione di particolari Registri, non è consentito l'accesso al sistema di gestione del protocollo informatico e documentale da parte di utenti appartenenti ad AOO esterne.

Le AOO che accedono ai sistemi di gestione informatica dei documenti utilizzano funzioni di accesso per ottenere le seguenti informazioni:

• numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;

• identificazione dell'UO.

Se la consultazione del PdP avviene allo sportello o comunque di fronte all'interessato, a tutela della riservatezza delle registrazioni di protocollo, l'addetto posiziona il monitor in modo da evitare ldiffusione di informazioni di carattere personale.

Nei luoghi in cui è previsto l'accesso al pubblico e durante l'orario di ricevimento devono essere resi visibili, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

Non è consentito l'accesso al PdP da parte di utenti esterni alla AOO non espressamente autorizzati.

Non è consentito autorizzare l'accesso al PdP al personale di ditte e società esterne diverse da quelle che gestiscono il S.I. del MIUR.