ASL Foggia
PugliaSalute

PROCEDURA INTERNA PER LA GESTIONE DEI LOG

Versione	Data	Modifiche
1.0	01/02/2023	Prima stesura

SOMMARIO

1. Premessa

Un log è la registrazione di ogni attività eseguita su un dispositivo elettronico. Esso normalmente riporta indicazioni temporali, riferimenti all'attività effettuata ed ovviamente riferimenti a chi l'ha eseguita; gli eventi vengono quindi registrati e memorizzati, dando origine a quelli che vengono definiti come file di log. Tutti i sistemi digitali generano log. Ogni nostro dispositivo tiene traccia delle nostre attività, anche senza che noi lo sappiamo o lo approviamo, sotto forma per l'appunto di log.

L'utilità di questi ultimi, che tracciano tutte le attività di sistema, è indubbia: ad esempio, quando occorra effettuare una valutazione oggettiva di particolari situazioni, dovendo ricostruire un certo evento e/o la causa di un errore. Anche in termini giuridici, i log sono spesso utilizzati come evidenza probatoria (in informatica forense), dovendo dare evidenza di eventuali comportamenti illeciti. La quantità dei log generata dai sistemi oltretutto è imponente e per gestirli si ricorre sempre più a sistemi per la gestione dei Big Data (Data Base specifici, sistemi di reportistica adeguati, ecc.). Attraverso piattaforme di analisi e di "intelligenza artificiale" (SIEM – Security Information and Event Management) i log consentono peraltro di identificare comportamenti anomali nei sistemi, tentativi di attacco e vulnerabilità più in generale.

Essi costituiscono quindi, con tutta evidenza, un elemento essenziale anche per la sicurezza. Pertanto, la gestione e la conservazione dei log sono attività fondamentali per il corretto svolgimento delle attività di gestione dei sistemi informatici e per la continuità operativa dei servizi erogati.

A tali considerazioni devono essere inoltre aggiunti gli obblighi di adempimento alle normative, alle diverse prescrizioni del Garante in materia, tra cui quelle delle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (G.U. 24 dicembre 2008, n° 300), nonché alle diverse norme ISO in materia di sicurezza informatica ed alle linee di indirizzo interne dell'azienda, ivi incluse le presenti linee guida, che si collocano nell'insieme delle misure di carattere organizzativo e procedurale concorrenti alla tutela dei diritti dell'interessato ed alla sicurezza dei dati personali, in ottemperanza al principio di responsabilizzazione, formulato nel Regolamento UE 2016/679.

2. Finalità

Le presenti linee guida indirizzano l'insieme dei requisiti volti a regolamentare il processo di gestione e conservazione dei log dei sistemi ICT presso l'ASL di Foggia, con particolare riguardo a quelli preposti al trattamento di dati personali.

3. Ambito di applicazione

Le indicazioni definite nel presente documento si applicano a tutti i sistemi informatici riconducibili alla titolarità dell'ASL di Foggia, le cui funzionalità determinano la generazione di informazioni relative ad eventi avvenuti sull'infrastruttura ICT.

4. Normativa di riferimento

- Regolamento (UE) 2016 del Parlamento Europeo e del Consiglio, del 27 Aprile 2016, relativo alla protezione delle persone con riguardo al trattamento dei dati personali – Regolamento Generale sulla Protezione dei Dati (GDPR) e s.m.i.;
- D.lgs 10 agosto 2018, n. 101. "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- D.Lgs. 30 Giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e s.m.i.;
- Legge 20 maggio 1970, n.300 (Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento) e s.m.i.;
- Provvedimento del Garante per la protezione dei dati personali n. 13 del 1° marzo 2007 (G.U. n. 58 del 10 marzo 2007) "Linee guida del Garante per posta elettronica e internet" e s.m.i.;
- Provvedimento del Garante per la protezione dei dati personali del 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i.;

- Legge 18 marzo 2008, n. 48 “Ratifica ed esecuzione della Convenzione del Consiglio d’Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell’ordinamento interno”;
- Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 “Smaltimento e cancellazione sicura dei dati” e s.m.i.;
- “Linee guida in materia di Dossier sanitario” del Garante per la protezione dei dati personali del 4 giugno 2015 (G.U. n. 164 del 17 luglio 2015);
- ISO/IEC 27001:2022 “Information Security Management Systems”;
- ISO/IEC 27002:2022 “Code of practice for information security controls";
- ISO/IEC 29151:2017 “Information technology - Security techniques – Code of practice for personally identifiable information protection”, First edition 2017-08;
- ISO 8601:2004 “Data elements and interchange formats - Information interchange - Representation of dates and times”;
- “Guide to Computer Security Log Management” – NIST SP 800-92 9/2006.

5. Definizioni

Amministratore di Sistema	Figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.
Categorie particolari di dati personali	Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
DBMS	Database Management System.

Dossier sanitario	Il dossier sanitario è lo strumento costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es. ospedale, azienda sanitaria, casa di cura) al cui interno operino più professionisti, attraverso il quale sono rese accessibili informazioni, inerenti allo stato di salute di un individuo, relative ad eventi clinici presenti e trascorsi (es., referti di laboratorio, documentazione relativa a ricoveri, accessi al pronto soccorso), volte a documentarne la storia clinica.
DPO	Data Protection Officer.

File di log	Raccolta di informazioni rappresentanti eventi avvenuti nell'ambito delle attività dell'infrastruttura IT, allo scopo di effettuare attività di diagnostica. Tali informazioni possono essere registrate sotto forma di file testuali o binari.
GDPR	Regolamento Generale per la Protezione dei Dati.
IAM	Identity and Access Management.
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
Log di accesso	Tipo di dato strutturato relativo ad un evento generato da un sistema di autenticazione al momento di effettuare (o tentare) l'accesso, inclusa la sua disconnessione, verso un sistema informatico.
NAC	Network Access Control.
NTP	Netwotk Time Protocol.
SIEM	Security Information and Event Management
ICT	Information and Communication Technologies
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante

	trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Violazione dei dati personali	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

6. Ruoli e Responsabilità

Si riportano di seguito le funzioni di riferimento e relative responsabilità in merito all'adozione delle presenti linee guida per la conservazione e gestione dei log:

- Titolare del trattamento di concerto con il DPO: funzione di Responsabile della definizione e della conformità della politica di gestione di conservazione e gestione dei log;
- Sistemi Informativi e Telecomunicazioni: funzione di Responsabile del recepimento e corretta applicazione delle politiche adottate in merito alla conservazione e gestione dei log, in quanto Gestore dei sistemi ICT aziendali.

DPO e Responsabile dei servizi ICT, inoltre, hanno l'obbligo di segnalare al Titolare del trattamento qualsiasi caso non espressamente regolamentato dalle politiche di seguito definite o che si presti a dubbi o mal interpretazioni.

7. Principi generali

Attraverso i file di log è possibile monitorare le attività che vengono effettuate sul sistema informativo aziendale. Gli accessi a cartelle di rete condivise o email aziendali, le attività svolte dal dipendente in un determinato lasso temporale, i tentativi di accesso fraudolento ai sistemi aziendali e molte altre informazioni vengono infatti sistematicamente annotate sui file di log. Consultando i file di log è

possibile, infatti, risalire agilmente ad anomalie negli accessi ai sistemi informatici e reperire importanti informazioni sulle attività svolte sui sistemi. Avere, pertanto, a disposizione un affidabile gestione dei file di log permette di analizzare eventuali problemi relativi a un dato sistema e di intervenire prontamente per risolverli.

Allo stesso tempo la registrazione dei file di log permette di individuare agevolmente accessi non autorizzati ad una rete o ad un archivio, o di ricostruire le dinamiche di un data breach (violazione di dati personali).

L'adozione di uno strumento di log management rappresenta quindi un importante strumento, utile a dimostrare l'impegno del Titolare del trattamento nella tutela dei propri archivi contenete dati personali.

Nel contempo, l'accesso e la registrazione dei file di log deve necessariamente confrontarsi con i principi e le disposizioni vigenti in materia di protezione dei dati personali e dei lavoratori: il datore di lavoro deve, infatti, rispettare le norme nazionali, che "includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati in particolare per quanto riguarda l'impiego di sistemi di monitoraggio sul posto di lavoro" (artt. 6, par. 2, e 88, par. 2, del Regolamento), quale può essere considerato quello attraverso i file log.

Sul punto il vigente Codice Privacy, confermando l'impianto anteriore alle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101, fa espresso rinvio alle disposizioni nazionali di settore che tutelano la dignità delle persone sul luogo di lavoro, con particolare riferimento ai possibili controlli da parte del datore di lavoro.

Il Titolare del trattamento è, comunque, tenuto a rispettare i principi in materia di protezione dei dati ed è responsabile dell'attuazione delle misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato in conformità al Regolamento (artt. 5, par. 2, e 24 del Regolamento UE 2016/679).

È necessario quindi dotarsi di sistemi e procedure di monitoraggio dei log che rispecchino un adeguato bilanciamento di interessi tra le esigenze di sicurezze dell'organizzazione e quelle di riservatezza dei dipendenti. Pertanto, per poter raccogliere e utilizzare i file di log devono essere necessariamente

rispettati alcuni principi generali, sanciti dal GDPR (v. art. 5, par. 1), ai quali corrispondono delle azioni che il Titolare deve intraprendere:

- principio di trasparenza: secondo tale principio il soggetto cui i dati personali vengono raccolti deve essere adeguatamente e preventivamente informato sugli aspetti fondamentali del trattamento (informativa pubblicata sul sito internet istituzionale e intranet);
- principio di limitazione della finalità: il trattamento dei dati riguardanti il lavoratore deve essere finalizzato al perseguimento di interessi legittimi da parte del datore di lavoro, quali, ad esempio, la prevenzione o la repressione di comportamenti illeciti;
- principio di proporzionalità o minimizzazione dei dati: i dati raccolti devono risultare proporzionati rispetto alla finalità perseguita. Il trattamento di dati che eccedono, o che comunque non trovano giustificazione nel perseguimento dello scopo, sono da considerarsi trattati irregolarmente;
- principi di integrità e riservatezza: il sistema di log management deve offrire garanzie di accuratezza, integrità ed immodificabilità. Allo stesso tempo è fondamentale che l'accesso ai registri di log sia consentito solo a soggetti appositamente individuati e che tale accesso sia tracciato, protetto da credenziali univoche e giustificato da esigenze connesse alla sicurezza dei sistemi;
- limitazione della conservazione: i dati devono essere conservati solo per un arco di tempo necessario al perseguimento delle finalità. In linea generale i tempi di conservazione dei file di log dovranno quindi essere correlati rispetto alle attività svolte ed alle caratteristiche oggettive dell'organizzazione. Per i log connessi alle attività degli amministratori di sistema, una indicazione dei tempi minimi ci viene fornita dal Provvedimento dell'Autorità Garante per la protezione dei dati del 2008, che prevede una conservazione dei log per un tempo non inferiore ai sei mesi.

Un utilizzo non conforme a tali principi, comporta una violazione delle norme sulla protezione dei dati personali, con il rischio di incorrere nelle pesanti sanzioni pecuniarie previste dall'art. 83, par. 5 del Regolamento UE 2016/679.

Non sono infine da sottovalutare i profili sanzionatori derivanti dalle norme del diritto del lavoro e in particolare dagli artt. 4 e 38 dello Statuto dei Lavoratori (L. 300/1970 e s.m.i.). Nel caso in cui le informazioni raccolte tramite file di log vengano utilizzate per effettuare un controllo a distanza dei lavoratori, l'art. 38 prevede anche delle sanzioni di carattere penale per il datore di lavoro.

8. Valore legale dei Log

I log consentono di acquisire elementi di evidenza probatoria (in informatica forense) per comprovare eventuali comportamenti illeciti, oppure, in altri casi, fornire prove di esplicita acquisizione del consenso dell'interessato. Nell'accezione puramente tecnica i log rappresentano un prezioso strumento di tracciamento. Tuttavia, se non correttamente trattati, possono fungere da "mezzo di controllo" dell'operato del lavoratore, in violazione dell'art. 4 della Legge n. 300 del 1970 (Statuto dei Lavoratori): l'attività di tracciamento di file di log deve, infatti, avvenire nel pieno rispetto dei principi e delle disposizioni vigenti poste a protezione dei dati personali dei lavoratori medesimi. Il monitoraggio delle attività svolte dai dipendenti, pertanto, comporta un trattamento di dati personali con la conseguenza che il Titolare del trattamento, deve dotarsi di sistemi e procedure di sicurezza a tutela dei dati di log, con un adeguato bilanciamento di interessi tra le esigenze di sicurezza aziendale e quelle di riservatezza dei dipendenti in quanto, l'uso non corretto di log potrebbe configurare fattispecie penalmente rilevanti.

9. Finalità del trattamento dei Log

I log devono essere raccolti e conservati esclusivamente per il perseguimento delle seguenti finalità:

- Conformità alle normative vigenti e applicabili;
- Monitoraggio dei sistemi informatici aziendali, al fine di rilevare eventuali violazioni nel loro utilizzo e permettere quindi la possibilità di svolgere analisi post-incidente;

- Monitoraggio dei sistemi informatici aziendali (troubleshooting), al fine di garantire la continuità dei servizi erogati mediante la rilevazione di anomalie di funzionamento e la loro risoluzione;
- Adempimenti contrattuali, laddove applicabile.

Considerata la facile modificabilità del contenuto dei file di log, essendo gli stessi spesso file di testo, è opportuno adottare idonee ed efficaci misure per garantirne l'attendibilità, oltre che la sicurezza, affinché gli stessi possano essere considerati una valida prova nell'ambito di un processo giudiziario. Tale aspetto risulta ancor più rilevante poiché la memorizzazione dei file di log avviene generalmente tramite sovrascrittura cioè, una volta esaurito lo spazio di archiviazione a disposizione nel sistema nativo per la memorizzazione dei file log, il sistema procede in automatico a sovrascrivere i file di log più vecchi con quelli più nuovi, per cui le semplici copie, fatte al fine di evitarne la perdita su dispositivi al di fuori del sistema nativo di registrazione, possono essere ritenute non attendibili in ambito probatorio. A tale proposito per una corretta e valida gestione dei file di log si rende necessario ricorrere a sistemi e piattaforme specifiche di Log Management (es. SIEM – Security Information and Event Management) che sono in grado di assicurare l'inalterabilità e la disponibilità del contenuto degli stessi tramite l'adozione di meccanismi di time stamping ed hashing.

10. Trasparenza informativa

Il personale dipendente che accede ai sistemi informatici è informato, a mezzo di specifica informativa pubblicata sul sito interne istituzionale e/o tramite il portale intranet, dell'esistenza e delle modalità di tracciamento dell'utilizzo dei sistemi informatici aziendali, nonché delle attività di conservazione delle informazioni relative al tracciamento. Per il personale esterno le indicazioni devono essere riportate nel contratto di collaborazione o nei capitolati di riferimento.

11. Classificazione dei Log

A seconda della natura del sistema informatico sorgente, è possibile raggruppare i file di log nelle seguenti macro-categorie:

- Log di sistema operativo: informazioni generate da sistema operativo;

- Log di servizi di rete: informazioni generati da router, switch, proxy, servizi di posta, ecc.;
- Log di sicurezza: informazioni generate da apparati di sicurezza quali IDS, IPS, Firewall. Antivirus, SIEM, IAM, NAC, ecc.;
- Log applicativi: informazioni generate da applicazioni commerciali o sviluppate ad hoc;
- Log middleware: informazioni generate da DBMS, Web server, Application server, sistemi di gestione dei contenuti, ecc.;
- Log dei sistemi dedicati alla rilevazione e controllo degli accessi fisici.

Ognuna delle suddette macro-categorie, può essere associata ad una o più delle seguenti macro-classi di log che possono essere raccolti e conservati:

- Log di accesso;
- Log degli eventi di sistema;
- Log di utilizzo.

Nei paragrafi seguenti viene fornita una descrizione di ogni macro-categoria.

12. Log di accesso

Rientrano nella macro-classe dei Log di accesso, tutte le tipologie di log contenenti le seguenti informazioni:

- User ID: identificativo dell'utenza che sta effettuando l'accesso (es. utente, servizio, processo);
- Descrizione evento di autenticazione: sono da tracciare le azioni di log-in e log-out ivi compresi i tentativi di accesso;
- Sistema acceduto: descrizione/identificazione del target su cui è stato effettuato il log-in o il log-out;
- Sistema sorgente: i dati identificativi della linea di comunicazione e del terminale utilizzato;
- Timestamp: Data e ora dell'operazione, preferibilmente in formato ISO 8601 (es. YYYY-MM-DD hh:mm:ss) indicante l'istante nel quale il server ha riscontrato l'evento tracciato;

- TimeZone: Il Timezone del server che ha generato il log in formato ISO 8601 (es. +hh:mm oppure – hh:mm). Il timezone è opzionale se il sistema è configurato con UTC +01:00, altrimenti deve essere espressamente indicato.

13. Log eventi di sistema

Rientrano nella macro-classe dei Log degli eventi di sistema, tutte le tipologie di log contenenti le seguenti informazioni:

- Modifiche alla configurazione di sistema;
- Operazioni di restart, shutdown e relative sequenze;
- Errori di varia natura e genere;
- Avvio e chiusura di servizi, daemon ed altri processi di sistema;
- Accesso/modifica/cancellazione dei file di log;
- Timestamp: Data e ora dell'operazione, preferibilmente in formato ISO 8601 (es. YYYY-MM-DD hh:mm:ss) indicante l'istante nel quale il server ha riscontrato l'evento tracciato;
- TimeZone: Il Timezone del server che ha generato il log in formato ISO 8601 (es. +hh:mm oppure – hh:mm). Il timezone è opzionale se il sistema è configurato con UTC +01:00, altrimenti deve essere espressamente indicato.

14. Log di utilizzo

Rientrano nella macro-classe dei Log di utilizzo, tutte le tipologie di log contenenti le seguenti informazioni:

- Comandi amministrativi in genere;
- Comandi eseguiti, comprensivi sia di quelli andati a buon fine che falliti;
- Gli eventuali dati coinvolti nei trattamenti o nelle transazioni effettuate;
- Il numero delle transazioni effettuate in un determinato periodo e la dimensione delle transazioni;

- La natura e il dettaglio delle operazioni effettuate sulle applicazioni e sulle basi dati, anche se in sola consultazione;
- Timestamp: Data e ora dell'operazione, preferibilmente in formato ISO 8601 (es. YYYY-MM-DD hh:mm:ss) indicante l'istante nel quale il server ha riscontrato l'evento tracciato;
- TimeZone: Il Timezone del server che ha generato il log in formato ISO 8601 (es. +hh:mm oppure – hh:mm). Il timezone è opzionale se il sistema è configurato con UTC +01:00, altrimenti deve essere espressamente indicato.

15. Processo di gestione dei Log

Il processo di gestione dei log ha come obiettivo quello di identificare, nell'ambito dei sistemi e servizi ICT aziendali, l'opportuno livello di tracciamento degli stessi e definire le misure di sicurezza da attuare in funzione del tipo di trattamento effettuato e della classificazione delle informazioni in essi contenute. L'attività di gestione deve essere in linea con i requisiti definiti nei "Provvedimenti del Garante per la protezione dei dati personali del 27/11/2008", circa le misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".
Il processo di gestione dei log adottato deve includere le seguenti fasi principali:

- Identificazione: identificazione dei log e del loro livello di dettaglio da abilitare sui sistemi di interesse;
- Classificazione: sulla base di quanto identificato nella fase precedente, i log vengono classificati in relazione al loro livello di criticità;
- Generazione: attivazione delle funzionalità di logging e verifica della loro consistenza;
- Archiviazione ed accesso: implementazione delle misure di sicurezza necessarie a garantire l'integrità e la riservatezza dei log;
- Conservazione e cancellazione: definizione dei tempi di conservazione dei log sulla base di quanto previsto dalla normativa o sulle esigenze operative aziendali;
- Change management: fase trasversale al processo di gestione dei log che prevede, a seguito di cambi normativi o di strategie aziendali sulla gestione dei log, la verifica degli impatti di tale cambiamento sui sistemi.

Si riporta di seguito il dettaglio delle fasi precedentemente identificate.

15.1 Identificazione e classificazione dei Log

La fase di identificazione del processo di gestione dei log ha l'obiettivo di individuare i sistemi e/o i servizi ICT da sottoporre a tracciamento, affinché registrino, con un livello di dettaglio consono (pertinente e non eccedente) alla finalità:

- gli accessi al sistema (log di accesso);
- ove necessario, le azioni compiute e/o informazioni accedute (log di utilizzo);
- gli eventi di sistema (log di eventi di sistema).

Si identifica come necessario il tracciamento dei sistemi/servizi ICT che concorrono al trattamento di dati personali.
In particolare, ove possibile, per alcune tipologie di dati personali (ad es. dati riconducibili allo stato di salute), il log dovrebbe registrare quale dato personale è stato acceduto, quale operazione è stata eseguita (ad esempio, lettura, creazione, modifica, cancellazione), quando e da chi è stata eseguita.
L'elenco dei sistemi sottoposti a logging deve essere riportato all'interno di uno specifico documento, aggiornato periodicamente dal Responsabile dei Sistemi informativi aziendali ed esibito su richiesta del DPO o del Titolare del trattamento.
Tale elenco deve riportare per ogni sistema, le seguenti informazioni minimali:

- Nome servizio/archivio/applicazione di riferimento;
- Owner;
- Tipologia di dati trattati dal sistema (personali, categorie particolari di dati personali, dati personali relativi a condanne penali e reati);
- Dettaglio sulle configurazioni dei log:
  - Macro classificazione dei log;
  - Impostazione dei log a livello di sistema operativo, di middleware e di applicazione;
  - Esempi anonimi dei log presenti ed attivi;
  - Modalità di archiviazione (locale o centralizzata);
  - Tipologia di accesso da parte di Amministratori di Sistema (lettura, scrittura, cancellazione);
  - Tempi di conservazione definiti;
- Validità:
  - Data di abilitazione delle funzionalità logging;
  - Data di terminazione delle funzionalità di logging;
- Elenco dei log distribuiti su richiesta, con indicazione delle seguenti informazioni:
  - Richiedente;
  - Motivazione della richiesta;
  - Responsabile dell'autorizzazione;
  - Data di consegna;
  - Dettaglio dei log consegnati;
  - Modalità di consegna dei log.

15.2 Generazione dei Log

La fase di generazione dei log, legata all'attivazione delle funzionalità di logging, ha l'obiettivo di garantire che le informazioni presenti nei file di log siano consistenti e complete. In particolare, è necessario:

- Assicurare la consistenza temporale dei file di log, attraverso sistemi l'utilizzo di un server NTP (Network Time Protocol) univoco e configurato per ognuno dei sistemi di interesse;
- Verificare che tutti i campi previsti nel log siano correttamente valorizzati.

15.3 Archiviazione e accesso

La fase di archiviazione e accesso, ha l'obiettivo di definire le regole per la raccolta, accesso, conservazione, estrazione e distribuzione dei log, in ossequio ai principi di pertinenza e non eccedenza di cui all'art. 5 del Regolamento UE 2016/679.

In particolare:

- Regole di raccolta: la raccolta e l'invio dei log verso gli eventuali sistemi esterni adibiti all'archiviazione, deve avvenire nel rispetto delle misure di sicurezza associate al livello di classificazione del log. La frequenza di raccolta dei log viene individuata sulla base della tipologia dei log, del livello di criticità delle informazioni presenti, dei volumi di dati da gestire, e della capacità temporale di conservazione. Si riportano di seguito le frequenze di raccolta dei file di log, in funzione della sola classificazione: settimanale, giornaliera, tempo reale;

Nella tabella riportata in Allegato 1, sono riportate, a titolo puramente indicativo, le frequenze di raccolta associate alla tipologia di log;

- Regole di archiviazione: l'archiviazione deve avvenire nel rispetto dei requisiti previsti dalla classificazione dei file log, secondo quanto definito nella fase di classificazione;
- Regole di accesso: l'accesso ai file dei log, per le finalità individuate precedentemente, deve avvenire nel rispetto delle misure di sicurezza associate al livello di classificazione del log, e deve essere consentito esclusivamente alle seguenti figure di riferimento:
  - Gestore del Sistema ICT: per finalità di monitoraggio e gestione dell'infrastruttura informatica, inclusi i soggetti formalmente autorizzati dallo stesso per lo svolgimento le suddette attività;
  - Responsabile della funzione Security, ai fini della gestione della sicurezza ICT;
  - Soggetti investigativi e ispettivi in ottemperanza alle normative vigenti con il coinvolgimento del Titolare al trattamento dei dati e di eventuali altri soggetti interessati.
- Regole di distribuzione: fermo restando le regole per l'accesso ai file di log, il Gestore del sistema ICT, in quanto responsabile dell'accesso e del recupero dei log, deve definire delle procedure che ne regolamentano l'accesso e il recupero sulla base del livello di classificazione dell'informazione trattata nei log.

Tali procedure devono essere condivise, per competenza, dai soggetti autorizzati all'utilizzo dei log e devono descrivere puntualmente le modalità di:

- Invio e ricezione delle richieste di log da parte di soggetti interni o esterni;
- Estrazione ed accesso ai file di log;
- Distribuzione dei log;
- Gestione dal punto di vista della sicurezza dei flussi informativi tra le strutture coinvolte nell'attività di richiesta dei log.

Le richieste di accesso ai file di log, devono essere formalizzate al Responsabile dei Sistemi informativi e Telecomunicazioni, in qualità di Gestore del sistema ICT, e possono pervenire esclusivamente dai soggetti autorizzati individuati precedentemente nelle regole di accesso.
Tutte le operazioni effettuate dal Gestore del sistema ICT attraverso i soggetti incaricati all'accesso e al recupero dei log, devono essere tracciate e possono essere oggetto di verifica su esigenza specifica e/o periodica. Tutti i dati prodotti dalle attività di logging ed auditing devono essere sottoposti a backup ed i tempi di conservazione sono equiparati a quelli degli altri log.

15.4 Conservazione e cancellazione

La fase di conservazione ha l'obiettivo di definire un periodo di conservazione dettato sia dal quadro normativo vigente, sia dalle esigenze aziendali.
In particolare:

- Per i log soggetti a vincoli derivanti da pronunciamenti legali e normativi cogenti, il periodo di conservazione deve essere commisurato a quanto di volta in volta specificato dai singoli provvedimenti e/o richieste provenienti dall'Autorità Giudiziaria;
- Per i log non soggetti a vincoli normativi cogenti, il periodo di conservazione deve essere stabilito sulla base delle direttive fornite dal Responsabile dei Sistemi informativi e Telecomunicazioni, in relazione alle specifiche esigenze aziendali, nel rispetto dei principi di minimizzazione dei dati e di limitazione della conservazione, di cui all'art. 5 del Regolamento UE 2016/679.

Un eventuale prolungamento dei tempi di conservazione deve essere considerato come eccezionale e può verificarsi solo nei seguenti casi:

- per esigenze tecniche o di sicurezza del tutto particolari e comunque giustificate;
- in relazione all'esistenza di specifici ulteriori vincoli normativi o contrattuali;
- sia necessaria alla risoluzione di un contenzioso, anche in sede giudiziale (e.g. dati necessari ai fini dello svolgimento delle investigazioni difensive o, comunque, per far valere o difendere un diritto in sede giudiziaria);
- rientri nei casi individuati dall'Autorità Garante per la protezione dei dati, sulla base dei princìpi sanciti dalla legge.

Detto prolungamento dei tempi di conservazione dei log deve essere sempre opportunamente documentato e condiviso con il DPO e con il Titolare del trattamento.
Al termine del periodo di conservazione, si deve procedere alla cancellazione di tali log, indipendentemente dalla loro ubicazione (supporto logici, fisici fissi o removibili), implementando misure tecniche e organizzative atte a garantire la sicurezza delle informazioni in essi contenute.

Nei casi in cui i log estratti siano stati consegnati per scopi di analisi (al di fuori delle richieste da parte dell'Autorità Giudiziaria), il Gestore del sistema deve comunicare la necessità di cancellare le informazioni estratte perché decorsi i termini di mantenimento delle stesse.

15.5 Gestione dei cambiamenti

La fase di change management ha come scopo di gestire i cambiamenti del processo di Gestione dei log derivanti da mutamenti relativi a:

- Normative nazionali ed internazionali;
- Sistema di classificazione delle informazioni;
- Politiche di sicurezza aziendali;
- Finalità di trattamento dei dati sui sistemi ed archivi.

I cambiamenti introdotti nel processo di gestione dei log devono essere opportunamente documentati e storicizzati.

16. Log degli Amministratori di Sistema

Il ruolo dell'Amministratore di Sistema assume una particolare rilevanza giuridica, tenuto conto della sua concreta capacità, per atto intenzionale ma anche per caso fortuito, di accedere in modo privilegiato alle risorse del sistema informativo aziendale e a tutti i dati personali cui non si è legittimati al trattamento, rispetto ai profili di autorizzazione attribuiti.
In ragione dei rischi e delle criticità implicite nell'affidamento di questo specifico incarico, e ai fini della conformità normativa, in linea con i "Provvedimenti del Garante per la protezione dei dati personali del 27/11/2008" circa le Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", devono essere tracciati i log appartenenti alla seguente macro-classe precedentemente definita:

- Log di accesso, con particolare riferimento agli accessi e tentativi di accesso effettuati dagli amministratori di sistema sui sistemi operativi, sui Middleware (es. DBMS, ecc.), sistemi elaborativi ed archivi strutturati e destrutturati, sugli apparati di sicurezza e di rete e sugli applicativi complessi.

Tali log devono avere caratteristiche di completezza, inalterabilità dei dati raccolti e possibilità di verifica della loro integrità.
La completezza è riferita all'insieme degli eventi censiti nel sistema di log che deve comprendere tutti gli eventi di accesso interattivo generati dalle attività degli amministratori di sistema su tutti i sistemi di elaborazione (server, client, database) con cui vengono trattati, anche indirettamente, dati personali. Le registrazioni devono inoltre comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate. Devono essere implementate idonee soluzioni tecnologiche atte a garantire la creazione e la raccolta dei log di accesso degli Amministratori di Sistema, rispettando le suddette caratteristiche.

16.1 Durata di conservazione Log Ads

Allo scopo di garantire l'integrità, la riservatezza e la disponibilità delle informazioni contenute nei log di accesso degli Amministratori di Sistema, è necessario implementare le seguenti misure di sicurezza:

- Proteggere i log archiviati tramite meccanismi di time stamping ed hashing, al fine di impedire qualsiasi alterazione dei dati e garantirne la successiva inalterabilità;
- Regolamentare l'accesso ai log sia a livello procedurale che eventualmente tramite i sistemi di Identity Management;
- Dimensionare opportunamente, in termini di performance e capacità di memorizzazione, i sistemi di conservazione dei log.

L'inalterabilità dei dati raccolti può anche essere soddisfatta ad esempio, attraverso l'implementazione di una piattaforma centralizzata per la gestione dei log (SIEM) con l'utilizzo di canali di trasmissione sicuri e la conservazione dei log in cloud qualificato AgiD.
I log di accesso ai sistemi di elaborazione e agli archivi elettronici effettuati dagli Amministratori di Sistema, devono essere conservati per un congruo periodo, non inferiore a 6 mesi. Trascorso tale periodo, dovrà esserne prevista la cancellazione definitiva da ogni supporto di archiviazione.

16.2 Tracciamento accesso ai Log Ads

L'accesso ai log degli Amministratori di Sistema da parte del personale autorizzato deve:

- Consentire la tracciabilità dell'utente che accede, garantendo il non ripudio dell'accesso, e delle attività condotte sui log file;
- Prevedere meccanismi di timestamping.

17. Gestione Log posta elettronica e internet

Per quanto concerne la registrazione delle informazioni relative all'utilizzo della Posta Elettronica e dell'accesso ad Internet, è necessario attenersi alle "Linee guida del Garante per posta elettronica e internet" (G.U. n. 58 del 10 marzo 2007).
In particolar modo, nell'osservanza dei principi di trasparenza, limitazione delle finalità, proporzionalità e minimizzazione, è consentita la registrazione delle seguenti informazioni:

Per la Posta Elettronica:

- Indirizzo IP del mittente del messaggio;
- Indirizzo IP del destinatario;
- Giorno e ora dell'invio;
- Esito dell'invio;
- Criterio di filtro applicato e suo esito;
- Responso fornito dal server di posta (messaggi di conferma od errore);

- Dimensioni del messaggio.

Per Internet:

- Identificativo utente non direttamente riconducibile alla persona fisica intestataria dell'utenza;
- Giorno e ora della navigazione;
- L'indirizzo Web del sito visitato;
- Il tempo di connessione;
- Criterio di filtro applicato e suo esito;
- Responso fornito dal server remoto;
- Byte trasmessi e ricevuti.

Ulteriori informazioni possono essere registrate nel rispetto del principio di necessità e pertinenza. Tale valutazione deve essere eseguita dal Responsabile dei Sistemi informativi e Telecomunicazioni, di concerto con il DPO.

17.1 Durata di conservazione Log posta elettronica e internet

Per i log relativi all'utilizzo di posta elettronica (email/pec) e internet, il periodo di conservazione non dovrebbe superare i 7 giorni, nel rispetto del principio di pertinenza e non eccedenza di cui all'art. 5 del Regolamento UE 2016/679.

I dati personali dei dipendenti cessati dal servizio sono tempestivamente comunicati dall'Ufficio personale al Responsabile dei Sistemi informativi e Telecomunicazioni. Il blocco della mailbox avviene non prima di un mese dalla comunicazione di cessazione. Dopo ulteriori 30 giorni è eseguita la completa disattivazione dell'account (login e password) del dipendente cessato.

17.2 Tracciamento accesso ai Log posta elettronica e internet

L'accesso ai file di log contenenti le informazioni di cui sopra, incluse le attività effettuate sugli stessi ed il relativo time stamping di accesso, deve essere tracciato in modo tale da poter permettere l'identificazione dell'utenza che ha effettuato l'accesso e garantire il requisito di non repudio.

18. Disposizioni finali

La presente procedura, proposta dal Responsabile dei Sistemi informativi e Telecomunicazioni dell'ASL di Foggia, è adottata dal Direttore Generale, d'intesa con il DPO ed entra in vigore il giorno successivo alla sua approvazione ed è pubblicazione nell'apposita sezione Privacy del sito internet istituzionale. Il suo contenuto è soggetto ad aggiornamento periodico. È fatto obbligo a chiunque spetti di osservarlo.

19. Norma di rinvio

Per quanto non espressamente previsto dalla presente procedura, si applicano le disposizioni di legge e i provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali che regolamentano la materia in oggetto.

TIPOLOGIA DI LOG E PERIODO DI CONSERVAZIONE

Si riporta di seguito, a titolo puramente indicativo e non esaustivo, una tabella di esempio relativa alla frequenzadi raccolta dei log in funzione della tipologia.

MACRO CATEGORIE SORGENTI DI LOG	SOTTO CATEGORIE SORGENTI DI LOG	MACRO-CLASSI	FREQUENZA DI RACCOLTA DEILOG	STORICIZZAZIONE
Log di sicurezza	Sistemi Anti-malware/virus	Log di utilizzo	Giornaliera	60gg
	Sistemi Autenticazione su Dominio MS Active Directory	Log di utilizzo	Tempo Reale	6 mesi
	Sistemi VPN	Log di utilizzo	Tempo Reale	60gg
	IDs / IPs	Log di utilizzo	Tempo Reale	60gg
	Sistemi di Vulnerability Assessment / Patch management	Log di utilizzo	Giornaliera	6 mesi
	Firewall	Log di utilizzo	Tempo Reale	60gg
	Sistemi di elaborazione e archivi elettronici di dati	Log di accesso Utenti	Giornaliera	7gg
	Sistemi di elaborazione e archivi elettronici di dati	Log di accesso AdS	Giornaliera	6 mesi
	Tutti	Log di eventi di sistema	Settimanale	10gg
	Router	Log di utilizzo	Tempo Reale	30gg
	Proxy	Log di utilizzo	Tempo Reale	30gg

Log dei servizi di rete	Servizi di posta	Log di utilizzo	Tempo Reale	30gg
	Tutti	Log di accesso	Giornaliera	30gg
	Tutti	Log di eventi di sistema	Settimanale	30gg
Log di sistema operativo	Tutti	Log di accesso utenti	È funzione della tipologia dei dati trattati nel log file	7gg
		Log di accesso AdS		6 mesi
		Log di eventi di sistema	Settimanale	10gg

MACRO CATEGORIE SORGENTI DI LOG	SOTTO CATEGORIE SORGENTI DI LOG	MACRO-CLASSI	FREQUENZA DI RACCOLTA DEILOG	STORICIZZAZIONE
Log applicativi	Tutti	Log di accesso	È funzione della tipologia dei dati trattati nel log file	60gg
		Log di eventi di sistema	Settimanale	60gg
		Log di utilizzo	È funzione della tipologia dei dati trattati nel log file	7gg
Log middleware	Tutti	Log di accesso	È funzione della tipologia dei dati trattati nel log file	60gg
		Log di eventi di sistema	Settimanale	60gg
		Log di utilizzo	È funzione della tipologia dei dati trattati nel log file	7gg

Log dei sistemi dedicati alla rilevazione e controllo degli accessi fisici	Tutti	Log di accesso	Tempo Reale	30gg
		Log di eventi di sistema	Settimanale	30gg
		Log di utilizzo	Tempo Reale	30gg

IL DIRETTORE GENERALE

ASL FOGGIA