POLITICA DI GESTIONE DEI LOG

Approvazione
Data: **15/09/2021**
Dirigente ASI: **Dott.ssa Francesca Pruneti**
Firmato digitalmente ai sensi del D.Lgs. n. 82/2005

Informazioni sul documento		
Redazione a cura di: *U.O. Sicurezza IT*	**Destinatari:** *I gestori dei sistemi IT che forniscono servizi agli utenti dell'Università di Parma*	**Deposito del documento:** *www.unipr.it/regolamento-sicurezza-IT*

Sommario

1. Scopo del documento 3
2. Ambito di applicazione 3
3. Necessità di conservazione dei log 3
4. Persistenza dei log 3
5. Correlazione dei log 3
6. Tabella dei log 4

1. Scopo del documento

Lo scopo di questo documento è definire le tipologie di log da tenere e le regole di conservazione da applicare, in particolare evidenziando quali informazioni devono essere tracciate e per quanto tempo.

2. Ambito di applicazione

La politica descritta in questo documento si applica ai log dei sistemi IT che forniscono servizi agli utenti dell'Università di Parma.

3. Necessità di conservazione dei log

La gestione dei log da parte dell'Ateneo è necessaria per assicurare il rispetto della normativa a tutela dei dati personali, poiché consente di ricostruire l'attività di un sistema informatico e individuare eventuali responsabilità in caso di errore, violazioni di legge e databreach (art. 33 comma 3 del Regolamento UE 2016/679). Il principio di responsabilità (art. 5 comma 2 del Regolamento UE 2016/679) introduce per la prima volta, l'obbligo, in capo al Titolare del trattamento, di dimostrare il rispetto della normativa decidendo autonomamente modalità, garanzie e limiti del trattamento dei dati personali, in considerazione del contesto operativo in cui ci si trova. Da una parte, quindi, i titolari del trattamento non solo devono compiere tutte le attività necessarie per la salvaguardia degli interessati, ma devono anche precostituirsi le prove degli adempimenti in caso di ispezioni da parte delle autorità competenti.

4. Persistenza dei log

I log devono essere conservati e mantenuti in modo appropriato per prevenire eventuali perdite di informazioni o la possibile compromissione da parte di intrusi. La conservazione dei log deve inoltre rispettare i requisiti normativi e fornire le informazioni necessarie per attività forensi e di risposta agli incidenti.

5. Correlazione dei log

I log devono essere gestiti in modo centralizzato e accessibili alla U.O. Sicurezza IT per poter effettuare una correlazione anche automatizzata delle informazioni in essi contenuti. al fine di soddisfare i requisiti normativi e fornire le sufficienti informazioni necessarie per le attività forensi, di risposta agli incidenti e di analisi di databreach.

6. Stato di attuazione

I log attualmente tracciati sono quelli delle righe di colore verde

I dati di tracciamento a livello applicativo (evidenziali nella tabella sottostante in colore marrone), vanno conservati seguendo le disposizioni normative, applicando la cifratura, l'anonimizzazione, minimizzando i tempi di conservazione e dandone adeguata informativa agli interessati in osservanza delle disposizioni di legge e gli accordi sindacali; quindi, potranno essere implementati solo dopo aver compiuto tutti i passi succitati.

7. Tabella dei log

Categorie e tipologie	Cosa tracciare	Sistemi interessati	Tempo di conservazione	Norme di riferimento	Descrizione
Accesso amministratori di sistema e profili privilegiati	• Username • Timestamp • Descrizione evento: Log-in, Log-out, Tentativi falliti • Sistema di elaborazione acceduto	• Sistemi operativi • Software complessi • Apparati di rete	Min 6 mesi Max 2 anni	1. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 Gazzetta Ufficiale n. 300 del 24/12/2008 2. Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, 26 aprile 2016	1. *"…la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software…"* (Log-in, log-out e tentativi falliti) 2. 5.5.1 Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa. N.B. gli Amministratori di Sistema non devono poter accedere a tali log che devono avere caratteristiche di non modificabilità
Modifiche utenze amministrative	• Aggiunta utenti con privilegi amministrativi • Eliminazione utenti con privilegi amministrativi	• Sistemi operativi • Software complessi • Apparati di rete	Min 1 anno Max 2 anni	Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, 26 aprile 2016	*5.4.1 Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.*
Attività di amministratori di sistema e profili privilegiati	• Username • Timestamp • Operazioni svolte	• Sistemi operativi • Software complessi	Min 1 mese Max 6 mesi	1. ISO 27001 2. Misure minime di sicurezza ICT per le Pubbliche	1. 12.4.3 Le attività degli amministratori e degli operatori devono essere sottoposte a log, e questi devono

	• Sistema di elaborazione acceduto			Amministrazioni, 26 aprile 2016	essere protetti e riesaminati periodicamente. 2. 5.1.4 Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.
Autenticazione e Single Sign On per tutti i servizi web federati con il sistema di autenticazione dell'Ateneo	• Timestamp • Username • Log-in, • Log-out • Servizio • IP	Server di autenticazione (LDAP, AD, Radius, Shibboleth, CAS etc.)	Min 1 mese Max 1 anno	1. Lavoro: le linee guida del Garante per posta elettronica e internet Gazzetta Ufficiale n. 58 del 10 marzo 2007 2. Linee guida in materia di privacy e protezione dei dati personali in ambito universitario del CODAU	1. *"…l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni…"* 2. *"Tracciamento sistemistico e di rete Ricadono in questo ambito i dati di tracciamento generati da apparati di rete e componenti infrastrutturali."*
Navigazione web (attivabile a seguito di incidenti e su sottinsiemi specifici)	• IP sorgente • IP destinazione • Porta sorgente • Porta destinazione • Protocollo • URL visitato	Apparati che gestiscono l'accesso alla rete Internet (es.: Firewall, IPS etc.)	A seconda della finalità da perseguire	Lavoro: le linee guida del Garante per posta elettronica e internet Gazzetta Ufficiale n. 58 del 10 marzo 2007	"…l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni…"
Operazioni server DHCP	• Associazione macaddress-IP • Associazione utente-mac	Sistemi per il rilascio automatico	Min 1 anno Max 2 anni	1. Misure minime di sicurezza ICT per le Pubbliche	*1.2.1 Implementare il "logging" delle operazioni del server DHCP.*

	address (conservata separatamente dall'associazione precedente)	degli indirizzi IP		Amministrazioni, 26 aprile 2016 2. Rispondere a una richiesta da parte delle autorità amministrative di vigilanza, ispettive o giudiziarie competenti	
Accesso WIFI	• ID utente • Indirizzo IP e MAC address • Nome AP • Timestamp (inizio e fine sessione) • Tipo e versione SO • Numero byte scambiati	Sistemi per l'accesso WIFI	Min 1 anno Max 2 anni	Rispondere a una richiesta da parte delle autorità amministrative di vigilanza, ispettive o giudiziarie competenti	
Accesso VPN	• ID utente (con eventuali ruoli di accesso alla rete) • Indirizzo IP (sia esterno che interno) • Timestamp	Concentratori VPN	Min 1 anno Max 2 anni	Rispondere a una richiesta da parte delle autorità amministrative di vigilanza, ispettive o giudiziarie competenti	
Eventi firewall, IPS e altri apparati di rete	Attivare moduli IPS del firewall	Apparati di controllo e di rete	Min 15 giorni Max 6 mesi	1. Misure minime di sicurezza ICT per le Pubbliche Amministrazioni 26 aprile 2016 (classificazione standard) 2. ISO 27001	1. *8.1.3 Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.* 2. *13.1.1 Appropriate attività di logging e monitoraggio dovrebbero essere applicate per registrare e rilevare azioni che potrebbero avere un impatto sulla sicurezza delle informazioni*

Attività utente su repository di file	• Timestamp • Username • Hostname • Accesso ai file • Creazione file • Cancellazione file • Modifica file	Depositi centralizzati dei dati di Ateneo (es.: File server, SharePoint etc.)	Min 15 giorni Max 6 mesi	1. ISO 27001 2. Regolamento Ue 2016/679 (art. 5, art. 33 e art. 34) 3. Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, 26 aprile 2016	1. *12.4.1 I log degli eventi che registrano le attività degli utenti, le eccezioni, i guasti e gli eventi di sicurezza delle informazioni dovrebbero essere prodotte, mantenute e regolarmente riesaminate.*
Utilizzo e gestione delle postazioni di lavoro	• Timestamp • Log-in, • Log-out • Username • Hostname • IP • Inventario dell'Hardware e del Software installato / utilizzato	• PDL • VDI	Min 6 mesi Max 1 anno	1. Regolamento Ue 2016/679 (art. 5, art. 33 e art. 34) 2. Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, 26 aprile 2016 3. Rispondere a una richiesta da parte delle autorità amministrative di vigilanza, ispettive o giudiziarie competenti	
Accesso alle postazioni dei laboratori informatici	• Timestamp • Log-in, • Log-out • Username • Hostname • IP	Aule informatiche e fisiche e virtuali	Min 6 mesi Max 1 anno	1. Regolamento Ue 2016/679 (art. 5, art. 33 e art. 34) 2. Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, 26 aprile 2016 3. Rispondere a una richiesta da parte delle autorità amministrative di vigilanza, ispettive o giudiziarie competenti	
Gestione del traffico telefonico per finalità di	Dati telefonate in/out (non contenuto e numeri in parte con asterischi)	Sistemi di telefonia tradizionale e VOIP	Min 1 mese Max 6 mesi	Regolamento Ue 2016/679 (art. 5, art. 33 e art. 34)	

contabilizzazione					
Applicazioni per richieste di intervento	• Anagrafica utente • Motivo ticket	Sistemi di gestione dei Ticket	Min 1 anno dopo il dato viene anonimizzato	Regolamento Ue 2016/679 (art. 5, art. 33 e art. 34)	
Utilizzo dei servizi di stampa	• Timestamp • Username • Hostname	Sistemi di stampa centralizzati	Min 1 anno dopo il dato viene anonimizzato	Regolamento Ue 2016/679 (art 5, art. 33 e art. 34)	
Registro degli incidenti	• Tipologia incidente • Veicolo • n. impattati • n. danneggiati • fonte segnalazione • note • Azioni di contenimento e ripristino • Riaperture caso • Responsabile attività malevola • Databreach • Notifica garante • Notifica interessati		Min 2 anni dopo il dato viene anonimizzato	Rispondere a una richiesta da parte delle autorità amministrative di vigilanza, ispettive o giudiziarie competenti	

Revisioni del documento

Ver.	Descrizione modifiche	Autore	Data modifica
1.0	*Versione iniziale*	*U.O. Sicurezza IT*	*02/07/2020*