Avv. Giuseppe Serafini
Law Firm
G. | S.
L. | F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Cyber Security.

Digital Forensics e data breach, tecnologie, tecniche e procedure di risposta agli incidenti.

ISACA – Roma Chapter 23.05.2017

About

- Avvocato del Foro di Perugia;
- Perf. UNIMI - Cloud, Data Protection, Digital Forensics;
- BSI ISO/IEC 27001:2013 Lead Auditor;
- Master Privacy Officer;

- European Certificate on Cybercrime Evidence;
- Digital Forensics Expert Witness;
- UNI-PG (Giurisprudenza) / Scuola Forense (Perugia)

- ISACA - Roma;
- D.F.A. - Digital Forensics Alumni;
- C.S.A. - Cloud Security Alliance;

- CLUSIT - Associazione Italiana per la Sicurezza Informatica;
- $(ISC)^2$ - Int. Information Systems Security Certification Consortium;
- Centro Studi Informatica Giuridica - Perugia.

Avv. Giuseppe Serafini
Law Firm

G. | S.
L. | F.

ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Agenda

- Introduzione.
- EU Cyber Security Framework
- Digital Forensics & GDPR
- Data Breach Notification
- NIST 800-86
- Question & Answers

Scenario - Tags

```
Dim multiline = <![CDATA[
[configuration]
name=Fred
age=40
]]>.Value
```

Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Legal Framework

Art. 24 (R).
Responsabilità del titolare del trattamento

1. - Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il **titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare,** che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

EU GDPR - Reg. 679/2016 - *Data Protection.*

Responsabile del Trattamento - (Art. 28);
Registro dei Trattamenti - (Art. 30);
Sicurezza - (Art. 32);
Data Breach Notification - (Art. 33 e ss);
Privacy Impact Assessment - (Art.35);
Data Protection Officer - (Art. 37 - 39);

NIS Dir. (UE) 2016/1148 - *Network Information Security.*

CSIRT - ENISA;
Operatori Servizi Essenziali - (All. II);
Fornitori Servizi Digitali - (All. III);

NIST 800-86 - *Guide to Integrating Forensic Techniques into Incident Response.*
NIST SP 800-61, R2 - *Computer Security Incident Handling Guide*

Provv. Garante & Codice Privacy

Dossier Sanitario;
Biometria;
Video-sorveglianza.

Cod. Proc. Pen. - *Digital Forensics.*

Information Security.

ISO/IEC 27000 Family (ISO/IEC 27037:2012);
NIST 800 Series;
Cloud Control Matrix - (CSA);
SANS - Digital Forensics

Reg. E.U. *27.04.2016* Nr. 679. C (81)

Articolo 37
Designazione del responsabile della protezione dei dati

(1). *- Il* ***titolare*** *del trattamento e il* ***responsabile*** *del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:*

Il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino *garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento.*

L'esecuzione dei trattamenti da parte di un responsabile del trattamento dovrebbe essere disciplinata da **un contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri che vincoli il responsabile del trattamento al titolare del trattamento.

Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Reg. E.U. *27.04.2016* Nr. 679.

Art. 32 - Sicurezza del Trattamento.

(1). - Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, **il titolare del trattamento e il responsabile del trattamento** mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- ***(a). -*** *la* ***pseudonimizzazione*** *e la* ***cifratura*** *dei dati personali;*
- ***(b). -*** *la capacità di assicurare su base permanente la* ***riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;***
- ***(c). -*** *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*
- ***(d). - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.***

(2). - Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

NIS Directive
Art. 4. c.1. nr. 2
Sicurezza della rete e dei sistemi informativi.

La capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, **l'autenticità, l'integrità** o la **riservatezza** dei **dati** conservati o trasmessi o trattati e dei relativi **servizi** offerti o accessibili tramite tale rete o sistemi informativi.

Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Considerando - Art. 33

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;*

(88). - Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla **notifica delle violazioni** di dati personali:

- *è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso.*
- *Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.*

*

(33.3). - La notifica di cui al paragrafo 1 deve almeno:

(a). - *descrivere la **natura** della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione (...);*

(b). - *comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;*

(c). - *descrivere le **probabili conseguenze** della violazione dei dati personali*

(d). - *descrivere le misure **adottate o di cui si propone l'adozione** da parte del titolare del trattamento per porre **rimedio** alla violazione dei dati personali e anche, se del caso, per **attenuarne** i possibili effetti negativi.*

Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Incident Response - Digital Forensics

Digital Evidence

Any data stored or transmitted using a computer that support or refuse a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi.

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

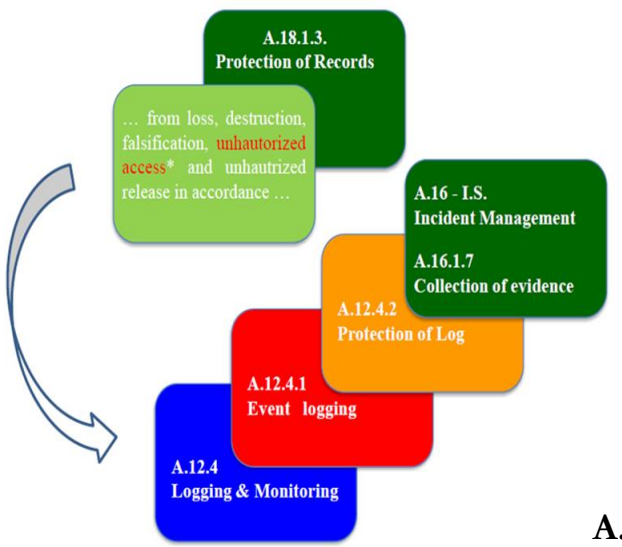
Special Publication 800-86

Guide to Integrating Forensic Techniques into Incident Response

Recommendations of the National Institute of Standards and Technology

Karen Kent
Suzanne Chevalier
Tim Grance
Hung Dang

ISO/IEC 27001:2013



A.12.4 Logging and monitoring.

Objective: To record events and generate evidence.

A.12.4.1 Event logging
Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

A.12.4.2 Protection of log information
Logging facilities and log information shall be protected against tampering and unauthorized access.

A.12.4.3 Administrator and operator logs
System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

A.12.4.4 Clock synchronisation
The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.

A.16 Information security incident management.

A.16.1.7 Collection of evidence
The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

ISO/IEC 27037:2012

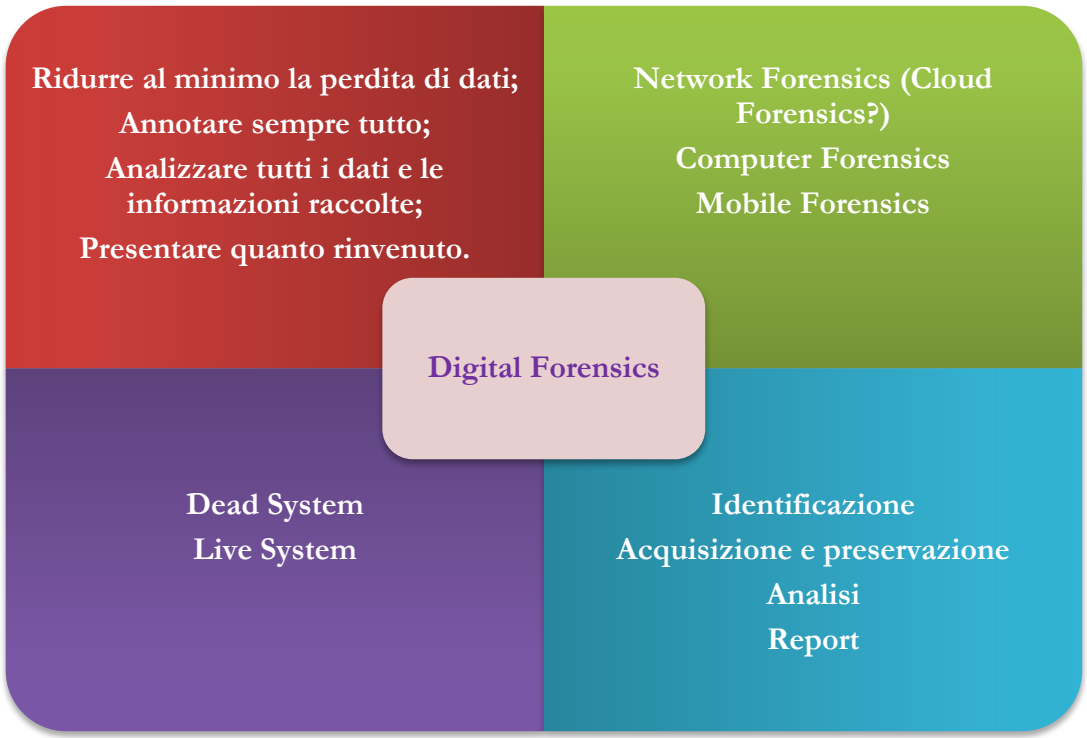
Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence

Chain of Custody

A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer .

Forensic Copy

An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm.



Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Digital Forensics – PCI - DSS

Art. 354
Cod. Proc. Pen.

In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità.

1.4 Executive Summary of Findings

▪ Summary of environment reviewed *Details must be documented under "Findings" section below.*	
▪ Was there conclusive evidence of a breach?	☐ Yes ☐ No
If yes (there is conclusive evidence of a breach), complete the following:	
▪ Date(s) of intrusion	
▪ Cause of the intrusion *List applicable attack vectors as per Appendix C.*	
▪ Has the breach been contained?	☐ Yes ☐ No
▪ *If yes*, specify how the breach has been contained.	
▪ Is there evidence the cardholder data environment was breached? *Provide reasons for Yes or No under "Findings" section below*	☐ Yes ☐ No
If no (there is no conclusive evidence of a breach), complete the following:	
▪ Were **system** logs available for all relevant systems?	☐ Yes ☐ No
▪ Were **network** logs available for all relevant network environments?	☐ Yes ☐ No
▪ Did the available logs provide the detail required by PCI DSS Requirement 10?	☐ Yes ☐ No
▪ Were the log files in any way amended or tampered with prior to your investigation starting?	☐ Yes ☐ No
▪ Were changes made to the environment prior to your investigation starting?	☐ Yes ☐ No
▪ Was data pertaining to the breach deleted prior to your investigation starting?	☐ Yes ☐ No

Conclusioni

Grazie per l'attenzione.

Avv. Giuseppe Serafini
www.giuseppeserafini.legal
giuseppe.serafini@ordineavvocati.perugia.it