Il processo di sanitizzazione del dato come parte integrante della Privacy e sicurezza informatica

Rel. Roberto Tursini
General Manager
Data Sanitization Specialist

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

ADISA

DATA WIPE

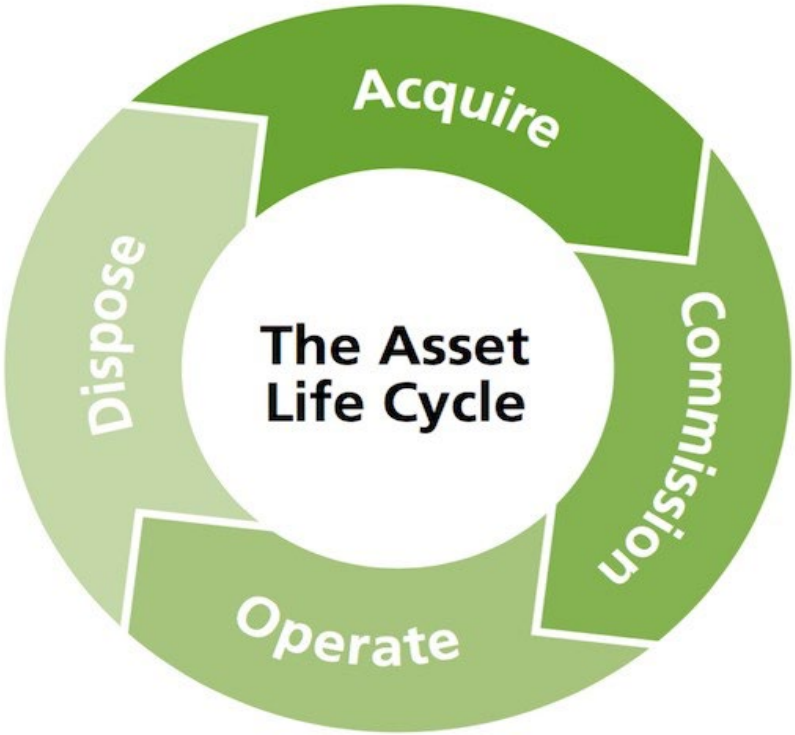
Overview

- Criticità nella dismissione IT
- Sanitizzazione del dato
- Responsabilità aziendali
- Approccio mitigativo – Utilizzo di schemi certificativi & standard
- Responsabilità del DPO

DATA WIPE
SECURE ASSET IT DISPOSAL
powered by DISTRUZIONE DOCUMENTI

Criticità nella dismissione asset IT

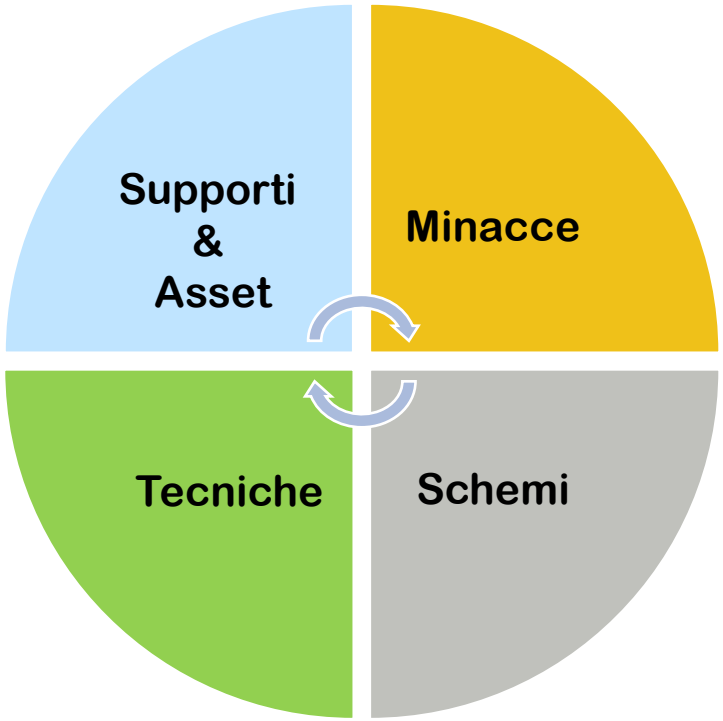
La dismissione degli asset IT e dei dati in essi contenuti rappresenta una fase critica con il più alto rischio aggregato di data breach e potenziali non conformità normative



DATA WIPE
SECURE ASSET IT DISPOSAL
powered by DISTRUZIONE DOCUMENTI

Sanitizzazione Dato

“Eliminazione dei dati tramite tecniche fisiche e logiche che rendano impossibile il recupero degli stessi mediante avanzate tecniche di laboratorio"



DATA WIPE
SECURE ASSET IT DISPOSAL
powered by DISTRUZIONE DOCUMENTI

Criticità nella dismissione asset IT

MEDIA TYPE	CLEAR- LOW	PURGE - MEDIUM	DESTROY - HIGHT
Papers and microforms	N/A	N/A	Destroy paper with cut shredders and microforms to be burnt.
Routers and Switches	Perform Manufacturer's reset to reset the router or return back to the factory default settings.	See if the media has a Purge capability or not to perform data rewriting or block erase.	Shred, Disintegrate, Pulverize, or Incinerate in a licensed incinerator.
Mobile Device	Select the full sanitize option for iOS and Android devices. Delete and perform factory reset for other mobile devices. Opt for an Overwrite using certified data eraser software.	Overwrite or block erase if the device supports purge capability	Same as above
Magnetic Media Disks HDDs or SSHD,LTD LTO	Overwrite using a certified data eraser tool.	Overwrite with dedicated sanitize commands (Overwrite EXT, Crypto Erase, SECURITY ERASE UNIT), Degauss, or Disassemble and degauss the enclosed platters.	Same as above
NVM Express SSDs	Overwrite using a certified data eraser tool.	Overwrite with dedicated sanitize commands (NVM Express Format command, Cryptographic Erase)	Shred, Disintegrate, Pulverize, or Incinerate in a licensed furnace.

DATA WIPE
SECURE ASSET IT DISPOSAL
powered by DISTRUZIONE DOCUMENTI

Sanitizzazione Dato

LIVELLO DI MINACCIA	ATTORI & METODI DI COMPROMISSIONE	TIPO DI ATTACCO	COMPARAZIONE
1 Basso (Low)	Minacce casuali o opportunistiche dettate da attori in grado di sferrare attacchi software di alto livello non invasivi e non distruttivi utilizzando strumenti gratuiti, COTS e OS.	Attacchi tramite tastiera da parte di un individuo motivato o organizzato professionalmente	CLEAR NIST 800-88 Rev 1 ISO 27040 ADISA 8.0
2 Medio (Medium)	Recupero dati commerciali da parte di organizzazioni informatiche forensi in grado di sferrare attacchi software e hardware invasivi/distruttivi, utilizzando sia COTS che software specifici	Attacchi di laboratorio da parte di esperti nel recupero dati commerciali o scienziati forensi specializzati.	PURGE NIST 800-88 Rev 1 ISO 27040 ADISA 8.0
3 ALTO (High)	Organizzazioni sponsorizzate da governi che utilizzano tecniche avanzate per montare tutti i tipi di attacchi software e hardware con tempo e risorse illimitate per recuperare i dati sanitizzati.	Un agente di attacco di capacità sconosciuta e risorse economiche e temporali illimitate.	DESTROY NIST 800-88 Rev 1 ISO 27040 ADISA 8.0

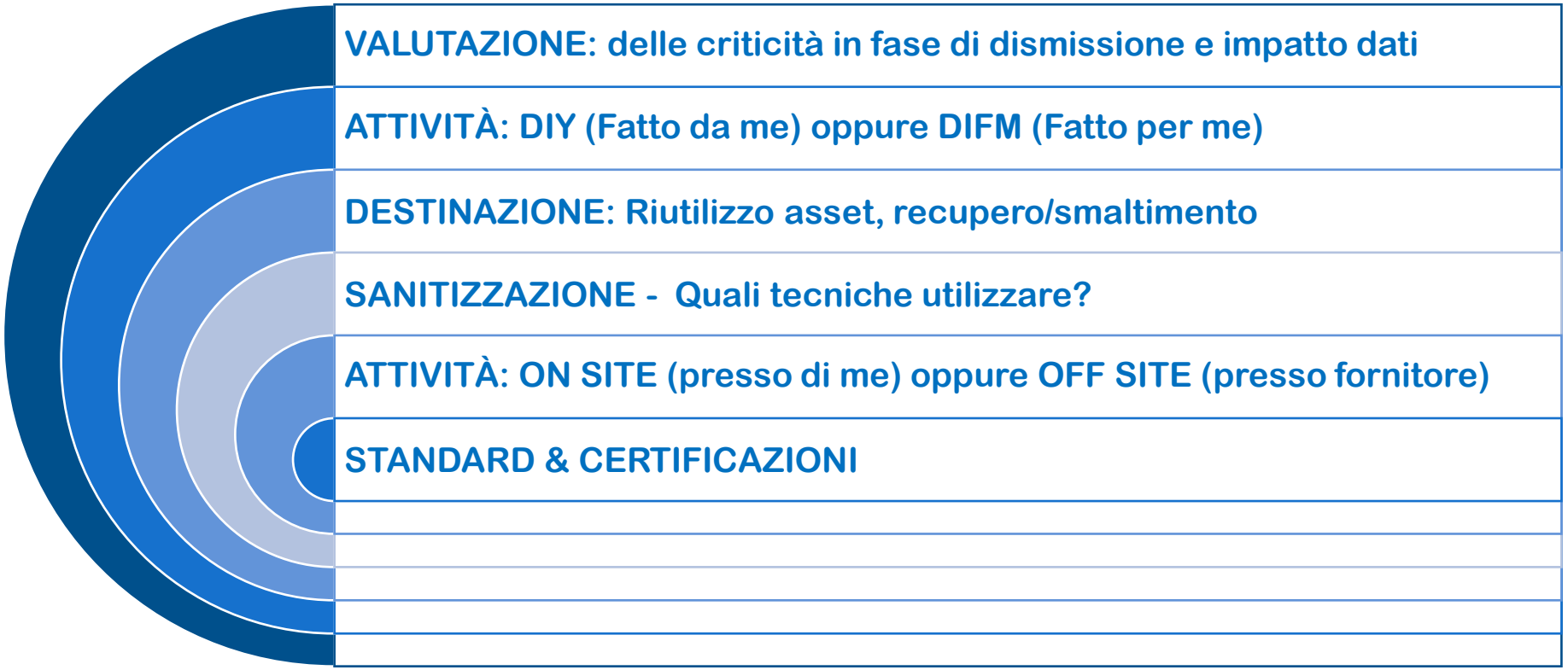
DATA WIPE
SECURE ASSET IT DISPOSAL
powered by DISTRUZIONE DOCUMENTI

Sanitizzazione - Tecniche

METODO SANITIZZAZIONE	PRO	CONTRO
OVER WRITING WIPING CANCELLAZIONE  	• Riutilizzo supporto	❑ Non tutti supporti ❑ Non supporti danneggiati ❑ Tempistica associata costi ❑ Validazione data recovery ❑ Possibile recupero dati
DEGAUSSING 	• Utilizzabile su supporti danneggiati • Velocità	○ Non utilizzabile su tutti supporti ○ Safety ○ Non riutilizzo supporto ○ Non garanzia cancellazione completa (Ibride HDD SSD) ○ Possibile recupero dati
SHREDDING 	• Velocità • Non ricostruibilità del supporto /dato • Utilizzabile su tutti i supporti	❖ Non riutilizzabilità del supporto

DATA WIPE
SECURE ASSET IT DISPOSAL
powered by DISTRUZIONE DOCUMENTI

Responsabilità aziendali nella fase di dismissione



DATA WIPE
SECURE ASSET IT DISPOSAL
powered by DISTRUZIONE DOCUMENTI

Schemi certificativi & standard

- Valido supporto al Titolare/Responsabile del Trattamento
- Adozione consente dimostrazione di responsabilità e diligenza
- Specificità della certificazione o degli standard, deve impattare non solo sulla data protection ma anche sulla gestione ambientale

DATA WIPE
SECURE ASSET IT DISPOSAL
powered by DISTRUZIONE DOCUMENTI

Standard ADISA 8.0

Con l'approvazione ICO e con l'autorizzazione UKAS, in questo momento ADISA Standard 8.0 è ora uno schema di certificazione GDPR ufficiale del Regno Unito che fornisce ai clienti la certezza che il servizio di sanitizzazione è conforme alla normativa vigente.

SEZIONE 1

Credenziali aziendali

- Credit Score
- Assicurazioni
- Procedure
- Certificazioni ISO 27001
- Autorizzazioni ambientali
- Qualificazioni del personale
- Codici di condotta

SEZIONE 2

Conformità al UK EU GDPR

- ❑ Contrattualistica
- ❑ Trasparenza ed accuratezza nelle affermazioni
- ❑ Registro dei trattamenti
- ❑ Gestione di incidenti e notifiche di Data Breach
- ❑ Governance delle informazioni
- ❑ Trasferimento dei dati
- ❑ Filiera del trattamento e gestione di sub-contratti

SEZIONE 3

Risk Management

- ❖ DIAL (Data Impact Assurance Level)
- ❖ Logistica
- ❖ Data capability Sanitiz
- ❖ Sicurezza fisica e logica per attività in impianto che dal cliente

SEZIONE 4

Servizi no Data

- ➢ Riutilizzo
- ➢ Riciclo
- ➢ Smaltimento

DATA WIPE
SECURE ASSET IT DISPOSAL
powered by DISTRUZIONE DOCUMENTI

Standard ADISA 8.0 & GDPR

GDPR art.29 utilizzo di data processors in grado di dare garanzie di appropriate misure tecniche
GDPR art. 32 data breach notification al data controller dal data processor

GDPR art.28 2,4 contratto scritto tra DC e DP inclusa nomina di subfornitori con stesse obbligazioni

GDPR art.24 misure tecnico organizzative prese al DC
GDPR art.35 Impact assestment in caso di dati particolari

GDPR art.24 e 26 misure tecnico organizzative prese da DC e DP
GDPR art 32§2 misure sicurezza appropriate prese da DP
GDPR art 24 reporting necessario per dare evidenza

GDPR art. 26 misure tecnico organizzative prese da DP
GDPR art 32§2 misure sicurezza appropriate prese da DP

GDPR art.28 2,4 contratto scritto tra DC e DP inclusa nomina di subfornitori con stesse obbligazioni
GDPR art.24 e 26 misure tecnico organizzative prese da DP
GDPR art 32§2 misure sicurezza appropriate prese da DP

DATA WIPE
SECURE ASSET IT DISPOSAL
powered by DISTRUZIONE DOCUMENTI

Responsabilità del DPO

E che cosa rischia il DPO?

DATA WIPE
SECURE ASSET IT DISPOSAL
powered by DISTRUZIONE DOCUMENTI

Grazie per l'attenzione

www.datawipe.it
www.distruzionedocumenti.com

r.tursini@distruzionedocumenti.com
r.tursini@datawipe.it

393 9138675
800-089458