Sistema Socio Sanitario
Regione Lombardia
ASST Nord Milano

REGOLAMENTO SULLE MODALITA' DI CUSTODIA E SULLE MISURE DI SICUREZZA

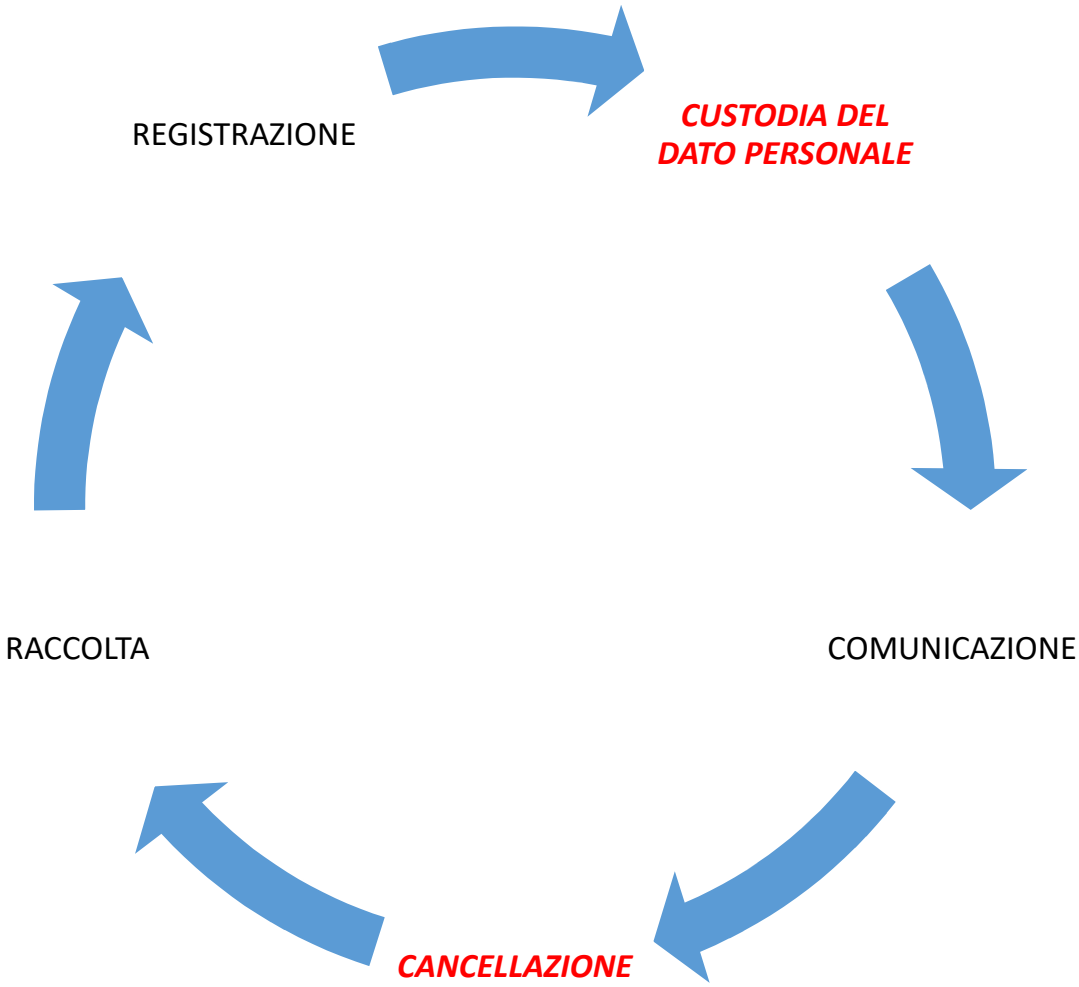
PER LA TUTELA DEGLI ARCHIVI INFORMATICI:

GESTIONE PROCEDURE DI BACKUP

approvato con deliberazione del Direttore Generale

n. 576 del 28/06/2021

FASE DEL CICLO DI VITA DEL DATO PERSONALE



RISCHI SPECIFICI

Il presente Regolamento consente di gestire i seguenti rischi:

- Accesso non autorizzato;
- Perdita dei dati;
- Distruzione accidentale dei dati personali;
- Dati di natura sensibile conservati unitamente ai dati di natura comune.

FONTI

- Dlgs 196/03 aggiornato dal D. Lgs 101/18
- Regolamento (UE) 2016/679
- Normativa per la Sicurezza Informatica AGID

DESTINATARI

- Amministratori di sistema
- Dipendenti incaricati della gestione, verifica e manutenzione della procedura di backup.

INTRODUZIONE

L'intera procedura di backup viene gestita, mantenuta e verificata direttamente dal reparto IT dell'Azienda Socio Sanitaria Territoriale di Nord Milano; Responsabile della stesura e della gestione della procedura è pertanto l'ing. Pietro Lanzoni, Direttore UOC Sistemi informativi Aziendali.

La procedura è stata condivisa con l'UOS Privacy e con la DPO aziendale nell'ambito della congiunta definizione e attuazione delle misure tecniche e organizzative previste dall'Art.32 del Regolamento (UE) 2016/679.

La procedura implementata tratta tre sorgenti di backup distinte:

- Server fisici;
- Server virtuali;
- Database;

Indipendentemente dalla natura e dalla frequenza di ciascun backup, è attiva una procedura che sistematicamente, effettua una copia di tutti i backup eseguiti all'interno di un "tape library" (30 tape); con questo metodo viene gestito il backup per il *lungo termine*.

Dal punto di vista procedurale il metodo è il seguente:

- All'interno della cassaforte sono predisposti tre cassetti per la raccolta dei tape (un primo cassetto per i tape che gestiscono la settimana (6 slot), un secondo cassetto per la gestione dei tape che gestiscono lo storico di tre mesi (3 slot) e un terzo cassetto per la gestione dei backup su tape semestrale (1 slot).
- Ogni martedì vengono prelevati i tape che sono oggetto dell'ultimo backup della settimana (in produzione) e vengono posizionati nello slot libero del primo cassetto (nella cassaforte); successivamente vengono prelevati i tape dello slot successivo del primo cassetto e posizionati all'interno del sistema di backup in produzione. Se il martedì coincide con il fine mese, questo scambio viene effettuato con lo slot più "vecchio" (3 mesi fa) del secondo cassetto.
- I backup su tape semestrali vengono effettuati manualmente su tape nuovi.

SERVER FISICI

Si identificano in questa categoria i sistemi "fisici" che svolgono direttamente una o più funzioni specifiche nel processo di gestione dei dati aziendali.

SERVER VIRTUALI

Si identificano in questa categoria tutte le "macchine virtuali" che son state configurate e che sono in esecuzione all'interno di uno o più server fisici. Si evidenzia come un singolo server fisico possa contenere al suo interno una o più macchine virtuali.

DATABASE

Si identificano in questa categoria tutti i server che svolgono la funzione di DBMS (Database Management System). Questi sistemi consentono il funzionamento di tutti gli applicativi che, per la loro esecuzione, necessitano di una base di dati configurata all'interno dell'azienda. Questa tipologia di server viene considerata in modo indipendente in quanto la presenza di dati e la centralità della loro funzione risulta particolarmente critica per l'intera operatività aziendale.

LIVELLI DI BACKUP

I livelli di backup sono determinati da 7 policy:

- **Policy 1**
  - **Identificativo della policy:** daily_snapshot_vm
  - **Descrizione della policy:** questa policy prevede il backup via snapshot di macchine virtuali in esecuzione in ambienti XenServer
  - **Implementazione della policy:** all'interno della console di gestione (XenCenter) viene creata una VM Protection Policy con frequenza giornaliera. La policy viene eseguita ogni giorno della settimana alla stessa ora. Per evitare un eccessivo stress sullo storgare, il numero di VM per ciascuna PP non deve superare le 6. Ogni PP viene quindi mandata in esecuzione differita di 30 minuti rispetto alla precedente a partire dalle 1.00.
  - **Retention** Lo scheduler di XenServer prevede la rotazione automatica degli snapshot. Nelle PP giornaliere viene definita una retention di 4 snapshot che coprono quindi una settimana intera.
  - **Dettaglio PP attualmente installate:**

PP	XENSERVER	ORARIO ESECUZIONE	GIORNO ESECUZIONE	RETENTIO N
PP Daily	ICP_Pool_01	1.00	Ogni giorno	7 giorni

- **Policy 2**
  - **Identificativo della policy:** weekly_snapshot_vm
  - **Descrizione della policy:** questa policy prevede il backup via snapshot di macchine virtuali in esecuzione in ambienti XenServer
  - **Implementazione della policy:** all'interno della console di gestione (XenCenter) viene creata una VM Protection Policy con frequenza giornaliera. La policy viene eseguita ogni giorno della settimana alla stessa ora. Per evitare un eccessivo stress sullo storgare, il numero di VM per ciascuna PP non deve superare le 6. Ogni PP viene quindi mandata in esecuzione differita di 30 minuti rispetto alla precedente a partire dalle 1.00.
  - **Retention** Lo scheduler di XenServer prevede la rotazione automatica degli snapshot. Nelle PP giornaliere viene definita una retention di 7 snapshot che coprono quindi una settimana intera.
  - **Dettaglio PP attualmente installate:**

PP	XENSERVER	ORARIO ESECUZIONE	GIORNO ESECUZIONE	RETENTION
PP_Lun	ICP_Pool_01	0.00	Lunedì	4 settimane
PP_Mar	ICP_Pool_01	0.00	Martedì	4 settimane
PP_Mer	ICP_Pool_01	0.00	Mercoledì	4 settimane
PP_Gio	ICP_Pool_01	0.00	Giovedì	4 settimane
PP_Ven	ICP_Pool_01	0.00	Venerdì	4 settimane
PP_Sab	ICP_Pool_01	0.00	Sabato	4 settimane
PP_Dom	ICP_Pool_01	0.00	Domenica	4 settimane

- **Policy 3**
  - **Identificativo della policy:** nonno padre figlio NPF
  - **Descrizione della policy:** questa policy prevede il backup via software backup exec di dati / database in esecuzione su pc fisici e macchine virtuali Questa policy prevede il backup via software backup exec di dati / database in esecuzione su pc fisici e macchine virtuali
  - **Implementazione della policy tramite attuazione del modello "figlio":** All'interno della policy "nonno padre figlio" viene creato un modello che prevede il backup INCREMENTALE tutti i giorni esclusa la domenica. Il Modello della policy viene eseguito nei giorni sopra elencati a partire dalle 23.00 e non oltre le 04:00. Per il backup viene utilizzato un set di supporti GIORNALIERO.
  - **Retention:** nella PP "nonno padre figlio" il modello di backup giornaliero definisce un periodo di protezione da sovrascrittura di 1 settimana.
  - **Implementazione della policy tramite attuazione del modello "Padre":** all'interno della policy "nonno padre figlio" viene creato un modello che prevede il backup COMPLETO dei dati tutte le domeniche. Il Modello della policy viene eseguito nei giorni sopra elencati a partire dalle 23.00 e non oltre le 04:00. Per il backup viene utilizzato un set di supporti SETTIMANALE.
  - **Retention:** nella PP "nonno padre figlio" il modello di backup settimanale definisce un periodo di protezione da sovrascrittura di 5 settimane.
  - **Implementazione della policy tramite attuazione del modello "Nonno**": all'interno della policy "nonno padre figlio" viene creato un modello che prevede il backup COMPLETO dei dati il primo giorno di tutti i mesi. Il Modello della policy viene eseguito nei giorni sopra elencati a partire dalle 23.00 e non oltre le 04:00. Per il backup viene utilizzato un set di supporti MENSILE.
  - **Retention:** nella PP "nonno padre figlio" il modello di backup mensile definisce un periodo di protezione da sovrascrittura di 1 anno.

- **Policy 4**
  - **Identificativo della policy:** Veem
  - **Descrizione della policy**: questa policy prevede il backup via software Veeam delle intere macchine virtuali poste nell'ambiente Vmware.
  - **Implementazione della policy**: l'infrastruttura vmware è stata organizzata in "directory" nelle quali sono state inserite le macchine virtuali. Veeam è impostato per backuppare a giorni alterni tutte le macchine poste all'interno di queste cartelle direttamente sul datadomain. Per i dettagli della configurazione rifarsi alla scheda server "icq100"
  - **Retention**:
    job PRODUZIONE: esegue il backup delle vm nel folder vmware “PRODUZIONE” direttamente sul DATADOMAIN completo una volta al mese il primo lunedi e incrementali nei giorni LUN-GIO alle 20. Retention 8 restore point.
    job PRODUZIONE2: esegue il backup delle vm nel folder vmware “PRODUZIONE2” direttamente sul DATADOMAIN completo una volta al mese il secondo lunedì ed incrementali nei giorni MAR-VEN alle 20. Retention 8 restore point.
    job SANTER esegue il backup delle vm nel folder vmware “SANTER” direttamente sul DATADOMAIN completo una volta al mese il terzo martedì ed incrementali nei giorni MER-SAB alle 20. Retention 4 restore point.
    job TEMPLATE esegue il backup delle vm nel folder vmware “TEMPLATE” su NAS QNAP eseguito una volta al mese il giorno 15. A mesi alterni fa il backup completo. Retention 1 backup.
    Job FILESERVEREsegue il backup delle vm nel folder “FILESERVER” su NAS QNAP**.** Esegue il backup COMPLETO l’ultimo sabato del mese. Completo una volta al mese, Incrementale sempre. Retention 64 backup.

- **Policy 5**
  - **Identificativo della policy**: file Configurazione
  - **Descrizione della policy**: Questa policy prevede il backup manuale dei file di configurazione di quei sistemi che non contengono dati variabili o condivisi tra gruppi di utenti. L'esecuzione dei backup è manuale e viene implementata ogni volta che si procede alla modifica dei file suddetti.
  - **Implementazione della policy**
  - **Retention:** vengono conservate fino a 3 versioni dei file di configurazioni.
  - **Domain Controler**
    -schedulato un backup del system state sul disco E tutti i giorni alle 21. Usato windows backup. Retention fino a che c'è spazio su disco.
    -schedulato snapshot della vm ogni domenica per i 3 dc 2008r2.
    -Per windcbas01 presente un job su backupexec per il backup giornaliero del system state.

- **Policy 6**
  - **Identificativo della policy**: export su disco
  - **Descrizione della policy:** questa policy prevede l'export in locale dei database attraverso processi batch.
    Implementazione della policy: i batch vengono attivati attraverso gli scheduler del sistema operativo.
    Retention: viene effettuata una copia completa ogni settimana che va a sovrascrivere la precedente.
    icx058 backup su partizione disco locale /backup
    icx052 backup del db effettuato da itinerissystem su filesrvbas01\itineris
    icx048 backup su partizione disco locale /backup + copia su nas esterno
    icx078 backup su partizione disco locale /backup file Configurazione

- **Policy 7**
  - **Identificativo della policy**: DATADOMAIN
  - **Descrizione della policy**: backup effettuato sul datadomain.
  - **Implementazione della policy**: i processi vengono lanciati da backup exec installato su icq050 destinazione DATADOMAIN - con sistema deduplica.
    Retention: 185 gg per i totali, 90 gg per gli incrementali.

NOTIFICHE

I software di backup al termine delle singole procedure inviano l'esito, sia esso positivo, sia esso negativo direttamente all'amministratore IT. Le notifiche in oggetto vengono trasmesse in formato di posta elettronica.

ALLEGATO 1: ALL SERVER

ASST Nord Milano stabilisce che il luogo di ubicazione dei backup deve essere rintracciabile e rispondere alle seguenti caratteristiche:

hostname	IP	note	Target Backup			policy 1	policy 2	policy 3	policy 4	policy 5	policy 6	policy 7
citrix lic server	10.141.12.195	XenServer License Server	snapshot				PP_Lun					
ethw6996vm		application server datawarehouse		Disco								
icq003	*10.141.128.25*	*domain controller*		Disco	Disco							
icq005	10.141.12.21	openwork			Nastro			NPF				
icq008	10.141.12.30	SQL server portale e intranet	snapshot		Nastro	PP_Daily		NPF				
icq009	10.141.8.24	application server jobtime			Nastro			NPF				
icq015		File server		DATADOMAIN					Veeam			NPF
icq019	10.141.12.63	estrazioni tempi attesa		DATADOMAIN					Veeam			
icq015		file server		DATADOMAIN					Veeam			NPF
icq019	10.141.12.63	estrazioni tempi attesa	snapshot				PP_Mar					
icq023	10.141.128.11	server appoggio langate	snapshot				PP_Mar					
icq027	10.141.128.27	server Compacs (kardia)		DATADOMAIN	Nastro			NPF	Veeam			
icq028	10.141.12.42	Server sw Mystar - METEDA			Nastro			NPF				
icq030		server pasti SSG - nova srl			Nastro			NPF				
icq033	10.141.128.42	server antivirus Symantec INet								config files		
icq036	10.141.12.64	Server Priamo (BCS)						NPF				
icq037	10.141.12.37	server psyche	snapshot	Disco			PP_Mar					
icq038	10.29.33.73	file server buzzi 02		DATADOMAIN								NPF
icq043	10.141.128.54				Nastro			NPF				
icq044	10.141.128.39	Server TAO-Stagio			Nastro			NPF				
icq046		application server OSLO		DATADOMAIN					Veeam			
icq050	10.141.128.65	Server DFSR con icq038			Nastro			File server				
icq051	10.141.128.76	Application NFS		DATADOMAIN	Nastro			NPF	Veeam			
icq053	10.141.8.20	protocollo			Nastro			NPF	Veeam			
icq054	10.141.12.116	holter poliambulatori	snapshot		Nastro		PP_Dom	File server				
icq056	copia backup su icq048											
icq058	10.141.12.113	server pasti bassini - novasrl		DATADOMAIN	Nastro				Veeam			
icq065	10.141.12.123	server tempo		DATADOMAIN	Nastro				Veeam			
icq070	10.141.12.49	server quix			Nastro			NPF				
icq071	10.141.12.71	calcolo drg hopera, euol	snapshot				PP_Mar					
icq072	10.141.12.46	Meteda mystar x bassini			Nastro			NPF				
icq077	10.141.12.33	nuovo nefro-srv		DATADOMAIN	Nastro				Veeam			
icq078	10.141.12.19	Meteda mystar x poliambulatori (insieme a icq015)			Nastro							
icq079	10.141.12.15	Nuovo documentale efiles vecchio karthadoc			Nastro			NPF				
icq082	10.141.128.82	file server virtuale		DATADOMAIN								NPF
icq086	10.141.12.78	application Akropolis			Nastro			NPF				
icq088	10.141.128.88	Archivio pst PEC		DATADOMAIN					Veeam			
icq091		server timbrature fracassi			Nastro			NPF				
icq098		database quani-sdo		DATADOMAIN					Veeam			
icq099		file server bassini		DATADOMAIN								NPF
icq100	10.141.13.6	server Veeam		Qnap								
compacsdb	10.32.33.63	db sever Medimatic VM su icq074			Nastro			File server				
icx004	10.141.12.112	nuovo portale flussi		Disco				NPF			Export	
icx007	10.141.12.187 / 25	nuovo application server ormaweb	snapshot				PP_Mer					
icx009	10.141.12.210	nuovo hoperabk	snapshot				PP_Mer					
icx010	10.141.128.12	target iscsi per backup icx016 (backup presente nel processo del server icx016)	snapshot				PP_Gio					
icx013	10.141.12.26	server ossec								config files		
icx014	10.141.12.32	server (windows) di appoggio per infoline										
icx015	10.141.12.211 / 122	nuovo hopera monitorPS	snapshot				PP_Mer					
icx017	10.141.128.19	DB server NFS reale			Nastro							
icx018	10.141.12.36	DB server Neonatal		Disco							Export	
icx022		eseguibili rabbit										
icx023	10.141.12.50	DB server Datawarehouse Controllo Gestione		Disco	Nastro			NPF				
icx025	10.141.12.213	Application server Hopera Test	snapshot				PP_Mer					
icx028	10.141.12.218	App srv + DB oracle per MIRTH	snapshot				PP_Gio					
icx029	10.141.12.188	cluster hopera nodo 1 - blade 6		Disco	Nastro			NPF			Export	