COMUNE DI SAONARA

PROVINCIA DI PADOVA

Decorato con medaglia d' argento al merito civile per l' eccidio del 28 Aprile 1945

POLITICA PER LA GESTIONE DI BACKUP & RESTORE

Approvato con Deliberazione di Giunta Comunale n. ____ del __.__.____

1 SCOPO E CAMPO DI APPLICAZIONE

La disponibilità delle informazioni e dei sistemi è essenziale per garantire l'operatività stessa di un'organizzazione. Il controllo primario da attuare è rappresentato dal salvataggio delle informazioni per l'erogazione dei servizi e delle configurazioni dei sistemi, su supporti dedicati, da impiegare in caso di disastri, guasti o errori umani, favorendo il ripristino della normale operatività.

2 DEFINIZIONI:

A fini del presente documento si intende con il termine:

- *"Backup"*: copia di file e programmi realizzata per facilitare il ripristino, se necessario.
- *"Restore"*: l'attività di ripristino delle informazioni in precedenza salvate.

3 RESPONSABILITÀ

L'assegnazione dei ruoli e delle responsabilità è un elemento indispensabile per assicurare un corretto governo dei rischi e permettere un'efficace operatività, intesa come attuazione dei controlli di prevenzione e/o contrasto delle minacce di cyber security a cui le organizzazioni sono esposte. E' fondamentale che tutto il personale sia consapevole dei ruoli e delle responsabilità di sicurezza, correlate allo svolgimento della attività lavorative. In particolari ai vertici dell'organizzazione, che difatti sono i responsabili ultimi per i rischi cyber all'interno dell'organizzazione.

Amministratore di Sistema (process owner)

Tale figura è il soggetto che corrisponde a quanto indicato nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, pubblicato nella G. U. n. 300 del 24 dicembre 2008, e successive modificazioni intervenute con il Provvedimento del 25 giugno 2009, pubblicato nella G.U. n. 149 del 30 giugno 2009; ovverosia, colui che sovrintende alla gestione dell'infrastruttura informatica e che tratta i dati per finalità di sviluppo, gestione, implementazione, manutenzione dei componenti hardware e software di tale infrastruttura, più nello specifico ai fini della presente procedura sarà il soggetto che:

- Individua le necessità manutentive delle infrastrutture
- Mantiene aggiornato il database dei beni
- Effettua i controlli di monitoraggio
- Verifica che i backup siano stati eseguiti correttamente e che siano correttamente conservati
- Monitora l'infrastruttura informatica di competenza attraverso l'analisi dei log, identificando e prevenendo potenziali problemi
- Introduce ed integra nuove tecnologie negli ambienti esistenti
- Installa e configura nuovo hardware/software sia lato client sia lato server
- Applica le patch e gli aggiornamenti necessari al software di base ed applicativo
- Modifica le configurazioni di base dei nuovi dispositivi in base alle esigenze dell'organizzazione
- Gestisce e tiene aggiornati gli account utente ed i relativi profili di autorizzazione
- Documenta le operazioni effettuate (eventualmente con l'ausilio di Logbook), le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni ai problemi
- Opera secondo le prescrizioni di sicurezza e le procedure interne previste.

Componenti dell'Ufficio dell'Amministratore di Sistema

- Seguono le istruzioni impartite dall'Amministratore di sistema

Direzione generale

- Monitora sulla corretta esecuzione delle attività dell'Amministrazione di Sistema

Utenti

- Seguono le indicazioni impartite dall'Amministrazione di sistema nell'ambito di quanto sancito dal regolamento per la protezione dell'informazione dell'organizzazione

Oltre a tali figure che ricoprono un ruolo prevalentemente tecnico, si ricorda che per una corretta protezione delle informazioni da parte dell'Organizzazione, ai sensi del Reg. UE 2016/679, l'Organizzazione dovrà aver provveduto ad individuare ulteriori figure quali:

- Titolare del trattamento, in persona del legale rappresentante pro tempore, così previsto dall'art. 4 n.7 Reg. UE 2016/679 e i compiti a lui attribuiti ex art. 32 della medesima fonte normativa e che monitora sulla corretta esecuzione delle attività.
- Responsabile della Protezione dei Dati personali (D.P.O / R.P.D) previsto dall'art. 37 Reg. UE 2016/679 con i compiti di cui all'art. 39 della medesima norma, dove normativamente previsto.
- Devono altresì essere previsti per ogni singola area e per ciascun ufficio quali sono i soggetti deputati a utilizzare le risorse fornite dall'Organizzazione con apposite istruzioni e a trattare dati personali con tali strumenti. Singole Aree con relativi singoli Uffici
- Gli interessati, intendendo con ciò sia soggetti a cui sono destinati i servizi, sia i soggetti a cui fanno riferimento i dati personali trattati.

Tali identificazioni si rendono necessarie in quanto ogni ufficio può avere in dotazione dispositivi e personale differente che andrà a trattare dati e informazioni con modalità e finalità differenti.

4 BACKUP & RESTORE

L'organizzazione deve adottare adeguati meccanismi e strumenti finalizzati al salvataggio e ripristino di Informazioni e dati.

In particolare:

- Deve essere effettuata almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
  L'Amministratore di sistema (o eventuali soggetti esterni fornitori di software e servizi informatici dell'organizzazione) potrà effettuare copie di sicurezza in maniera parziale o totale in base alle esigenze di erogazione dei servizi dell'organizzazione, ai requisiti di sicurezza delle informazioni, agli obblighi di legge e alle criticità delle informazioni, trattate rispetto al mantenimento delle attività operative;
- L'organizzazione deve assicurarsi che la riservatezza delle informazioni contenute nella copia di sicurezza avvenga mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. (si ricorda che la codifica effettuata prima della trasmissione consente la remotizzazione del backup anche del cloud)
- L'organizzazione deve assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza;
- Nell'ottica di protezione del perimetro informatico, per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati. Nel caso l'organizzazione si avvalesse di soluzioni esterne, i fornitori dovranno consentire il salvataggio dei dati ivi contenuti ed il ripristino degli stessi della funzionalità degli applicativi;

- L'ufficio dedicato alla gestione dei sistemi informatici deve prevedere backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di *restore*;
- Almeno una volta ogni 6 mesi, l'ufficio dedicato alla gestione dei sistemi informativi, verifica l'utilizzabilità delle copie mediante ripristino di prova.

5 RISPETTO DEL PRINCIPIO "CLOUD FIRST"

Secondo il piano triennale per l'informatica nella PA (https://www.agid.gov.it/it/agenzia/piano-triennale), e secondo le circolari di AgiD (ex. multis) n. 2 e 3 del 2018 e n .1 del 2022, la Pubblica Amministrazione nel rispetto del principio di "cloud first" dovrebbe avvalersi di soluzioni in cloud, certificate/accreditate, presenti sul marketplace ACN.
Per tale aspetto, pertanto, l'ufficio dedicato alla gestione dei sistemi informatici dell'Ente deve coordinarsi con l'R.T.D nominato dall'organizzazione per individuare soluzioni che utilizzino servizi o sistemi cloud qualificati secondo quanto previsto dall'Agenzia per la Cybersicurezza Nazionale.
In tale contesto le soluzioni di backup selezionate devono garantire soluzioni di *Disaster Recovery* e ***continuità operativa***, fondamentale nel rispettO del *Codice dell'Amministrazione Digitale*, che all'art. 51 *"sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni"*, al primo comma recita: *"con le regole tecniche adottate ai sensi dell'articolo 71, sono individuate le soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità, la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture".*

6 ACCOUNTABILITY DEL FORNITORE

Nel caso di soluzioni in cloud, devono essere selezionate soluzioni che forniscono una adeguata sicurezza. Pertanto, il fornitore dovrà essere in grado di garantire adeguate misure di sicurezza sul servizio di backup offerto in modo da assicurare riservatezza, integrità e disponibilità dei dati dei backup.
In particolare, il fornitore del servizio cloud dovrà garantire almeno:

- Standard di sicurezza conformi alle norme ISO di settore come la ISO 27001, ISO 27017, ISO 27018 e ISO 22301.
- Che I supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.
- Che le copie di backup di informazioni, software e immagini di sistema del servizio cloud siano protette adottando standard crittografici allo stato dell'arte e migliori pratiche di settore.
- Che qualora i backup siano trasmessi ad un sito remoto tramite rete, la trasmissione deve essere protetta adottando standard crittografici allo stato dell'arte e migliori pratiche di settore.
- Che i dati siano trattati mediante infrastrutture localizzate sul territorio dell'Unione europea, salvo motivate e documentate ragioni di natura normativa o tecnica.
- Che in caso dei metadata relativi al funzionamento dell'infrastruttura, che possono essere trattati mediante infrastrutture localizzate anche al di fuori del territorio dell'Unione europea, i metadata relativi all'amministrazione sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea, salvo motivate e documentate ragioni di natura normativa o tecnica.
- Che per l'infrastruttura digitale siano garantiti tempi di ripristino (RTO e RPO) conformi alle specifiche emanate dall'Agenzia per la Cybersicurezza Nazionale.
- Che ha formalmente adottato procedure per la gestione delle emissioni dei gas prodotti, o per la gestione dell'energia consumata o per la gestione ambientale dei propri Data Center. A tale riguardo, il soggetto può fare riferimento, rispettivamente, agli standard ISO 14064, ISO 50001 e ISO 14001, o equivalenti.