Allegato al Manuale di gestione documentale

PIANO PER LA SICUREZZA INFORMATICA

1. Premessa e Obiettivi

Il presente Piano per la Sicurezza Informatica costituisce parte integrante del Manuale di Gestione Documentale, in ottemperanza alle disposizioni vigenti in materia di gestione e conservazione dei documenti informatici.

La sua redazione è prevista dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, emanate da AgID. Nello specifico, il paragrafo 3.4, "Compiti del responsabile della gestione documentale", stabilisce che il responsabile della gestione documentale (o il coordinatore, ove nominato) ha il compito di predisporre il Manuale di gestione documentale, il quale "conterrà inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza". Tale previsione è ulteriormente dettagliata nel paragrafo 3.9, "Misure di sicurezza", che ribadisce i requisiti per tale piano.

Il Piano di Sicurezza ha lo scopo di garantire la protezione, l'affidabilità e la resilienza del sistema di gestione informatica dei documenti dell'Amministrazione. In particolare, il Piano è finalizzato a:

- contrastare le minacce di natura informatica (ICT) che possono compromettere l'integrità, la disponibilità e la riservatezza delle informazioni;
- assicurare la protezione dei dati personali trattati nell'ambito della gestione documentale, in conformità alla normativa vigente;
- tutelare la corretta formazione, gestione, accessibilità e conservazione dei documenti informatici, quale patrimonio informativo dell'Amministrazione.

Il Piano è redatto in conformità alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate da AgID, nonché alla Circolare AgID n. 2/2017 – Misure minime di sicurezza ICT per le pubbliche amministrazioni, adottando i principi e le misure ivi previsti come quadro di riferimento per la sicurezza.

Il documento si colloca nell'ambito del più ampio Piano generale di sicurezza dell'Amministrazione, con il quale è integrato e coordinato. Esso è inoltre elaborato in coerenza con le linee di indirizzo strategiche del Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente, al fine di assicurare un approccio unitario e armonizzato alla gestione della sicurezza informatica, alla continuità operativa e alla protezione del patrimonio informativo dell'Ente.

2. Ruoli e Responsabilità

La predisposizione, l'attuazione e il monitoraggio del presente Piano di Sicurezza coinvolgono diversi soggetti dell'Amministrazione, ciascuno con compiti e responsabilità specifiche nell'ambito della gestione documentale e della sicurezza delle informazioni.

Coordinatore della gestione documentale

Assicura l'applicazione del Piano di Sicurezza nell'ambito delle attività di formazione, registrazione, classificazione, archiviazione e conservazione dei documenti informatici.

Coordina le attività con i responsabili delle altre funzioni, al fine di garantire un approccio unitario alla sicurezza.

Responsabile della conservazione

Vigila sul corretto trasferimento, archiviazione e conservazione dei documenti informatici e dei fascicoli digitali.

Verifica che le misure di sicurezza adottate garantiscano integrità, leggibilità, reperibilità e protezione dei documenti nel lungo periodo.

Responsabile per la transizione digitale (RTD)

Assicura la coerenza del Piano di Sicurezza con le strategie generali di digitalizzazione dell'Amministrazione.

Coordina le azioni di sicurezza ICT in sinergia con i responsabili dei sistemi informativi e con i referenti di ACI Informatica.

Responsabile della protezione dei dati personali (DPO)

Esprime parere sul Piano di Sicurezza, verificandone la conformità al Regolamento UE 679/2016 (GDPR) e alla normativa nazionale in materia di protezione dei dati personali.

Fornisce indicazioni operative per garantire il rispetto dei principi di minimizzazione, proporzionalità e accountability.

Titolare e Responsabile del trattamento dei dati

Ai sensi dell'art. 28 del Regolamento UE 679/2016:

- Automobile Club d'Italia (ACI) è individuato quale Titolare del trattamento (art. 4 GDPR).
- ACI Informatica S.p.A. è individuata quale Responsabile del trattamento (art. 28 GDPR), per le attività di gestione tecnica e manutenzione dei sistemi informatici .

ACI Informatica

Partner tecnologico di ACI, responsabile della gestione dell'intero ciclo di vita degli incidenti di sicurezza delle informazioni e dell'implementazione del sistema di Business Continuity.

2. Norme di Riferimento

Il Piano di Sicurezza si basa e si conforma alle seguenti norme e direttive principali:

- Decreto Legislativo 7 marzo 2005, n. 82 (C.A.D.) e successive modifiche e integrazioni, con particolare riferimento all'Art. 14-bis (funzioni di AgID in materia di sicurezza informatica), all'Art. 51 (sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni) e all'Art. 71 (Linee Guida AgID).
- Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015, che impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici.
- Circolare AGID 18 aprile 2017, n. 2/2017 (già n. 1/2017 del 17 marzo 2017), che indica le misure minime di sicurezza ICT per le pubbliche amministrazioni.
- DPCM 17 febbraio 2017, recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali (Piano nazionale per la protezione cibernetica e la sicurezza informatica).
- Regolamento UE 2016/679 (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, in particolare gli Artt. 25 (Protezione dei dati fin dalla progettazione), 28 (Responsabile del trattamento), 32 (Sicurezza del trattamento), 33 (Notifica di una violazione dei dati personali all'autorità di controllo) e 34 (Comunicazione di una violazione dei dati personali all'interessato).
- Linee guida EDPB 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita.
- Linee guida EDPB 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del regolamento generale sulla protezione dei dati (GDPR).
- UNI CEI EN ISO/IEC 27001:2017 (Sistemi di Gestione della Sicurezza delle Informazioni – Requisiti), come standard di riferimento per la gestione della sicurezza IT.
- UNI EN ISO 22301:2019 (Sistemi di gestione della continuità operativa – Requisiti), per il sistema di gestione della Business Continuity.
- ISO/IEC 20000-1:2018 ("Tecnologie informatiche - Gestione del servizio - Parte 1: Requisiti per un sistema di gestione del servizio").
- UNI EN ISO 9001:2015 (Sistemi di gestione per la qualità – Requisiti).
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (AgID, Maggio 2021).
- DPR 445/2000 (Testo Unico sulla Documentazione Amministrativa - TUDA), in particolare gli articoli relativi al sistema di gestione informatica dei documenti e del protocollo.
- SANS 20 / CCSC «CIS Critical Security Controls for Effective Cyber Defense» versione 6.0 di ottobre 2015, utilizzato come base per le misure minime di sicurezza.
- ITIL v3 – Service Operations e altre best practice di settore come ENISA e SANS Institute per la gestione degli incidenti.

3. Documenti di Riferimento

Il presente Piano di Sicurezza si integra con e fa riferimento ai seguenti documenti interni ed esterni:

- Politiche di Sicurezza dei Sistemi e delle Informazioni.
- Regolamento Data Breach – Violazioni dei Dati Personali.
- Manuale della Business Continuity.

- Business Impact Analysis (BIA), che identifica i servizi essenziali e i relativi tempi di recupero.
- Manuale di gestione documentale
- Manuale di conservazione.
- Piano Triennale per l'Informatica nella Pubblica Amministrazione.

4. Analisi del Rischio e Misure di Sicurezza

Analisi del rischio

L'Amministrazione adotta una metodologia strutturata di analisi e gestione del rischio, basata sui principi delle norme internazionali in materia di sicurezza delle informazioni (ISO/IEC 27001, ISO/IEC 27701 e ISO/IEC 27005), nonché sui criteri indicati dalle Linee Guida AgID e dall'ACN (Agenzia per la Cybersicurezza Nazionale).

L'analisi è finalizzata a:

- identificare i beni informativi e i processi critici relativi alla gestione documentale;
- valutare le minacce e le vulnerabilità cui i sistemi sono esposti;
- stimare l'impatto potenziale su riservatezza, integrità e disponibilità delle informazioni;
- definire le misure di sicurezza necessarie per garantire un livello di protezione adeguato, in relazione alla tipologia dei dati trattati.

Particolare attenzione è riservata al trattamento delle categorie particolari di dati personali di cui agli artt. 9 e 10 del Regolamento UE 679/2016 (GDPR), che richiedono un livello di protezione rafforzato.

Misure tecniche e organizzative di sicurezza (Art. 32 GDPR)

In coerenza con l'analisi del rischio, l'Amministrazione adotta misure tecniche e organizzative idonee a garantire un livello di sicurezza proporzionato al rischio, tra cui:

- la pseudonimizzazione e la cifratura dei dati personali in transito e in conservazione, ove applicabile;
- la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico, attraverso procedure di backup e disaster recovery;

- l’adozione di una procedura periodica di test, verifica e valutazione dell’efficacia delle misure tecniche e organizzative implementate, mediante audit di sicurezza e simulazioni di incidente.

Misure minime di sicurezza ICT (Circolare AgID n. 2/2017)

Nel rispetto della Circolare AgID n. 2/2017, l’Amministrazione assicura l’applicazione delle misure minime di sicurezza ICT, adattandole ai tre livelli di sicurezza (Minimo, Standard, Alto) in funzione della classificazione dei dati e dei sistemi trattati. Le principali classi di misure implementate comprendono:

- Inventario dei sistemi e delle applicazioni: mantenimento di un registro aggiornato delle risorse ICT utilizzate nel sistema di gestione documentale.

- Protezione della configurazione dei sistemi: adozione di configurazioni sicure e aggiornate, con applicazione costante delle patch di sicurezza.

- Analisi delle vulnerabilità: monitoraggio periodico delle vulnerabilità e applicazione di misure correttive tempestive.

- Gestione degli utenti e privilegi di accesso: applicazione del principio del “minimo privilegio”, con controlli specifici sugli utenti con funzioni di amministrazione.

- Difesa contro i malware: utilizzo di strumenti di protezione avanzata e aggiornamenti automatici delle definizioni antivirale/antimalware.

- Copie di sicurezza: esecuzione regolare di backup, custoditi in ambienti protetti e verificati periodicamente per garantirne l’efficacia in caso di ripristino.

- Protezione dei dati rilevanti: applicazione di misure di prevenzione e rilevamento contro i rischi di esfiltrazione o perdita di dati sensibili.

Modulo di implementazione

Per ciascuna delle misure sopra indicate, l’Amministrazione predispone un apposito modulo di implementazione, contenente:

- descrizione della misura;

- livello di sicurezza applicato (Minimo, Standard, Alto);

- modalità di attuazione tecnica e organizzativa;

- periodicità dei controlli e dei test;

- referenti responsabili dell’attuazione.

5. Sicurezza del Sistema di Protocollo Informatico

Il sistema di protocollo informatico rappresenta un elemento centrale della gestione documentale dell'Amministrazione, in quanto assicura la registrazione, la classificazione e la tracciabilità dei documenti. Per tale ragione, esso è soggetto a requisiti di sicurezza specifici, volti a garantire l'affidabilità, la protezione e la conformità normativa del trattamento delle informazioni.

I principali requisiti minimi di sicurezza previsti sono:

Univoca identificazione ed autenticazione degli utenti

Ogni utente è identificato in maniera univoca mediante credenziali personali non condivisibili. L'accesso al sistema avviene attraverso procedure di autenticazione sicura, basate su nome utente e password complesse o, ove previsto, su sistemi di autenticazione a più fattori.

Gestione dei profili di accesso

L'accesso alle risorse e alle funzioni del sistema è consentito esclusivamente agli utenti abilitati, sulla base di profili predefiniti che distinguono i livelli di autorizzazione. I profili di accesso sono configurati in modo da consentire a ciascun utente soltanto le operazioni necessarie allo svolgimento delle proprie attività, garantendo la separazione dei compiti e la protezione dei dati sensibili.

Tracciamento e audit delle operazioni

Il sistema assicura il tracciamento permanente di tutte le operazioni rilevanti, comprese la registrazione, la modifica, la cancellazione e la consultazione dei documenti. Ogni evento è registrato nei log di sistema, con l'indicazione dell'utente autore dell'operazione, della data e dell'ora, nonché della tipologia di azione compiuta.

I registri di tracciamento sono protetti da alterazioni e conservati per un periodo adeguato, al fine di consentire eventuali verifiche, audit interni e controlli di conformità.

6. Gestione degli Incidenti di Sicurezza e Violazioni dei Dati Personali (Data Breach)

Il presente piano descrive le procedure da adottarsi per la gestione di eventi e incidenti di sicurezza delle informazioni, con particolare enfasi sulle violazioni dei dati personali (Data Breach), in conformità agli Artt. 33 e 34 del Regolamento UE 679/2016 (GDPR) e alle Misure Minime di Sicurezza ICT emanate dall'AgID con Circolare n. 2/2017. L'obiettivo è garantire un approccio strutturato e sistematico per minimizzare i rischi per le operazioni, i sistemi e i dati personali, assicurando tempestività, efficacia e conformità normativa.

6.1. Scopo e Principi Guida

Obiettivo primario: Implementare politiche e controlli per la gestione degli incidenti di sicurezza e delle violazioni dei dati personali, allineandosi agli standard e alle best practice internazionali di settore (es. ISO/IEC 27035:2016, SANS Institute).

Ambito di applicazione: Le politiche e le procedure si applicano a tutti gli eventi e agli incidenti di sicurezza delle informazioni che possono impattare la riservatezza, l'integrità e la disponibilità del patrimonio informativo dell'Amministrazione, coinvolgendo tutto il personale e le terze parti che hanno accesso a tale patrimonio.

6.2. Definizioni Chiave

Evento di Sicurezza: ogni occorrenza che indichi una potenziale infrazione di una policy, il fallimento di un controllo o una situazione precedentemente ignota e potenzialmente rilevante per la tutela delle informazioni.

Incidente di Sicurezza delle Informazioni: uno o più eventi di sicurezza indesiderati che comportano una significativa probabilità di compromissione delle operazioni di business e della sicurezza delle informazioni (integrità, disponibilità e riservatezza). Un incidente può essere deliberato (es. malware, infrazioni intenzionali) o accidentale (es. errori umani, fenomeni naturali).

Non tutti gli incidenti costituiscono una violazione dei dati personali.

Violazione dei Dati Personali (Data Breach): una 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. Le violazioni possono essere classificate in base alla compromissione di:

- Riservatezza: divulgazione o accesso non autorizzato o accidentale ai dati personali.
- Integrità: modifica non autorizzata o accidentale dei dati personali.
- Disponibilità: perdita o distruzione accidentale o non autorizzata dei dati personali.

Una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

6.3. Ruoli e Responsabilità nella Gestione degli Incidenti

I principali attori coinvolti e le loro responsabilità sono:

- Utenti (personale interno e terze parti): richiesti a segnalare tempestivamente qualsiasi evento o punto di debolezza relativo alla sicurezza delle informazioni osservato o sospettato nei sistemi o servizi. Le segnalazioni di tentativi sospetti di accesso indebito devono essere indirizzate alla casella cybersecurity@aci.it (o equivalente). In caso di sospetta violazione dei dati personali, la segnalazione deve essere inviata senza ritardo al Titolare del trattamento (es. privacy@aci.it) e al DPO (es. m.annibalidpo@aci.it).

- ACI Informatica (o soggetto tecnico/responsabile esterno del trattamento): è responsabile per la gestione dell'intero ciclo di vita degli incidenti di sicurezza delle informazioni. Le attività includono il monitoraggio proattivo, la presa in carico delle segnalazioni, la classificazione degli incidenti, le attività di analisi e risposta, nonché la comunicazione e il reporting verso la Direzione per lo Sviluppo, la Gestione, la Sicurezza dei Sistemi Informativi e l'Innovazione digitale di ACI e l'attivazione delle procedure di escalation (es. Crisis Management, fornisce i dati e gli elementi necessari per la gestione di eventuali

Data Breach). Insieme alla Funzione per i Sistemi Informativi, opera come Unità Tecnologica del Comitato di Crisi, individuando le azioni di risposta.

- Direzione per lo Sviluppo, la Gestione, la Sicurezza dei Sistemi Informativi e l'Innovazione digitale (DSII): Coinvolta con ruolo consultivo e autorizzativo nella gestione degli incidenti di particolare severità. Collabora con ACI Informatica per la revisione della reportistica periodica e per l'identificazione di incidenti che possono portare alla dichiarazione dello stato di crisi.

- Responsabile della Sicurezza Informatica: valuta la gravità degli incidenti e, in caso di potenziale data breach, informa immediatamente il DPO e il Direttore Centrale Organizzazione e Gestione della Privacy e Monitoraggio dei Sistemi di Qualità dell'Ente.

- Data Protection Officer (DPO): è componente del Comitato di Crisi. Conduce la verifica post-incidente per valutare l'efficacia della risposta, l'adeguatezza delle misure preventive e identificare eventuali lacune, informandone il Comitato di Crisi. È parte integrante del Comitato di Crisi per l'adozione delle conseguenti misure.

- Comitato di Crisi: organismo interno preposto a fronteggiare tempestivamente e in modo coordinato situazioni di emergenza che comportano rischi e minacce per la gestione dei dati personali. È responsabile della gestione strategica e tattica della crisi, definendo priorità e risorse. Se la violazione di dati personali comporta un rischio elevato per i diritti e le libertà delle persone, fornisce al Titolare, per il tramite della Struttura di privacy compliance, gli elementi per la notifica all'Autorità di controllo nei termini di legge e indicazioni per l'eventuale comunicazione agli interessati. Redige il Piano di risposta agli incidenti (Remediation plan).

- Responsabile della gestione documentale: in accordo con il responsabile della conservazione, il responsabile per la transizione digitale e acquisito il parere del DPO, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, che include le procedure per la gestione delle violazioni dei dati personali.

6.4. Fasi del Processo di Gestione degli Incidenti e Data Breach

Il processo è articolato nelle seguenti attività:

1. Monitoraggio e Rilevazione degli Eventi di Sicurezza:

- Attività continuative (H24 7x7) di monitoraggio, rilevazione e analisi di eventi anomali attraverso dispositivi informatici di monitoraggio e analisi periodica dei log.

- Raccolta e valutazione delle segnalazioni di comportamenti anomali o sospetti provenienti da utenti, amministratori di sistema o fonti esterne autoritative (es. alert, bollettini di sicurezza).

2. Segnalazione e Prima Classificazione:

L'incidente viene segnalato dagli utenti o dai sistemi di monitoraggio.

Ogni incidente che determina una violazione dei dati personali deve essere registrato e documentato senza ritardo nell'apposito "Registro delle violazioni" (Allegato al Regolamento Data Breach). Il Registro è detenuto dalla Struttura di privacy compliance dell'Ente e deve essere costantemente aggiornato e mantenuto in sicurezza.

Gli eventi vengono valutati per stabilire se classificarli come incidenti di sicurezza dei dati e delle informazioni, con i risultati registrati per il riesame di misure tecnico-organizzative migliorative.

3. Assessment e Valutazione della Gravità:

- ACI Informatica (o soggetto analogo) esegue un assessment per valutare la gravità e l'impatto dell'incidente.

- Se l'incidente è considerato grave o potenzialmente a rischio, il Responsabile della Sicurezza Informatica informa la Direzione per lo Sviluppo, la Gestione, la Sicurezza dei Sistemi Informativi e l'Innovazione digitale che ne dà notizia al Titolare ai fini dell'attivazione del Comitato di crisi.

- Valutazione Data Breach: Se l'assessment conferma un potenziale data breach, viene attivata la procedura di gestione delle violazioni dei dati. Il Responsabile della Sicurezza Informatica informa immediatamente il Titolare, il Direttore della Struttura di privacy compliance e il DPO.

- Valutazione del rischio e analisi delle conseguenze: Il DPO dell'ACI coordina una valutazione del rischio per determinarne l'entità e le conseguenze (es. tipologia e volume dei dati compromessi, categorie di interessati, effetti a lungo termine). Tale valutazione viene effettuata utilizzando strumenti standardizzati (es. diagramma di flusso operativo fornito dall'EDPB nelle apposite Linee Guida) e include la classificazione della gravità dell'incidente.

4. Contenimento, Risposta e Recupero:

Il Comitato di Crisi (o l'Unità Tecnologica del Comitato di crisi) adotta misure tecniche e organizzative immediate per limitare l'estensione della violazione, come la sospensione degli account utente compromessi o il blocco degli accessi non autorizzati.

Pianificazione e preparazione delle azioni di risposta, incluse le procedure di escalation (es. Crisis Management).

Recupero dei dati compromessi: Deve essere eseguito tempestivamente, cercando di ripristinare i dati allo stato originario precedente alla violazione.

5. Notifica all'Autorità Garante (Art. 33 GDPR) e Comunicazione agli Interessati (Art. 34 GDPR):

- Notifica al Garante: In caso di data breach che comporti un rischio per i diritti e le libertà delle persone fisiche, la violazione deve essere notificata all'Autorità di Controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui

l'Amministrazione ne è venuta a conoscenza. La notifica deve essere dettagliata e includere la natura della violazione, le categorie e il numero degli interessati, i contatti del DPO, le probabili conseguenze e le misure adottate. L'istruttoria è condotta dal Comitato di Crisi.

- Comunicazione agli Interessati: Se la violazione comporta un rischio elevato per i diritti e le libertà degli interessati, questi devono essere informati senza ingiustificato ritardo. La comunicazione deve essere chiara, concisa e facilmente comprensibile, includendo la descrizione della violazione, i contatti del DPO, le probabili conseguenze e i consigli per tutelarsi. La comunicazione non è necessaria in specifiche condizioni (es. dati cifrati, misure successive che evitano il rischio elevato, sforzi sproporzionati).

6. Chiusura, Reporting e Analisi Post-Incidente (Remediation Plan):

Al termine della gestione, si procede alla chiusura dell'evento e alla redazione di un report dettagliato sull'intero processo di gestione dell'incidente, inviato al Responsabile della Sicurezza Informatica.

Il Comitato di Crisi redige il Piano di risposta agli incidenti (Remediation Plan) che definisce le procedure specifiche per ripristinare la normale operatività e minimizzare l'impatto sugli interessati, garantendo la continuità operativa. Tale piano deve essere periodicamente testato attraverso simulazioni.

Il DPO conduce una verifica post-incidente per valutare l'efficacia della risposta, l'adeguatezza delle misure preventive esistenti e identificare eventuali lacune nei sistemi di sicurezza, informandone il Comitato di Crisi. Redige un rapporto per il Titolare.

Le politiche e le procedure interne saranno aggiornate in base ai risultati delle verifiche per migliorare la gestione dei trattamenti dei dati personali e prevenire lacune nei sistemi di sicurezza e future violazioni.

5.5. Modulo di Implementazione delle Misure Minime di Sicurezza ICT (MMS-PA)

Le modalità con cui ciascuna delle misure minime di sicurezza ICT (MMS-PA) è implementata presso l'Amministrazione devono essere sinteticamente riportate nel modulo di implementazione di cui all'allegato 2 della Circolare AgID n. 2/2017.

Tale modulo deve essere firmato digitalmente con marcatura temporale dal responsabile dell'attuazione delle misure e dal Rappresentante legale, conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

7. Continuità Operativa (Business Continuity - BC) e Disaster Recovery (DR)

La Continuità Operativa (Business Continuity - BC) e il Disaster Recovery (DR) sono elementi fondamentali per garantire l'erogazione dei servizi, in particolare per le Pubbliche Amministrazioni (PA), a fronte di eventi imprevisti e potenzialmente disastrosi. L'obiettivo è

assicurare che l'organizzazione possa continuare a fornire prodotti o servizi a livelli predefiniti accettabili anche in seguito a interruzioni.

1. Contesto Normativo e Standard di Riferimento:

Le PA sono tenute a predisporre piani di emergenza per assicurare la continuità delle operazioni, come indicato dall'Art. 51, comma 2-quater, del Codice dell'Amministrazione Digitale (CAD). L'Agenzia per l'Italia Digitale (AgID) definisce le linee guida tecniche e verifica annualmente l'aggiornamento dei piani di Disaster Recovery.

Le Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni (MMS-PA), stabilite dalla Circolare AgID 18 aprile 2017, n. 2/2017, devono essere adottate per contrastare le minacce più comuni ai sistemi informativi e sono richiamate per l'attuazione delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

ACI Informatica si è dotata di un Sistema di Gestione della Continuità Operativa (BCMS) progettato e realizzato in conformità con la norma ISO 22301:2019, detenendo inoltre le certificazioni ISO 27001 (sicurezza IT), ISO 20000 (gestione servizi IT) e UNI EN ISO 9001 (qualità).

Le politiche di sicurezza sono allineate a standard e best practice internazionali come ISO/IEC 27001, ISO/IEC 27035:2016, ITIL v3, ENISA e SANS Institute, ISO/IEC 27701.

2. Obiettivi e Parametri Chiave della Continuità Operativa:

Per i servizi in ambito BC, ACI Informatica definisce e monitora i seguenti parametri:

- Recovery Time Objective (RTO): Il tempo massimo di ripristino del servizio. È fissato a 24 ore, includendo 8 ore per la dichiarazione di disastro, 6 ore per la messa a disposizione del sito di recovery e il trasferimento del personale, e 10 ore per la ripartenza delle applicazioni.

- Recovery Point Objective (RPO): Il valore massimo di perdita dei dati tollerabile. ACI Informatica mira a 0, ovvero nessuna perdita di dati.

- Maximum Tolerable Data Loss (MTDL): La massima perdita di dati tollerata, tendente al 100% di salvaguardia della coerenza e consistenza dei dati.

- Minimum Business Continuity Objective (MBCO): Il livello di servizio minimo accettabile. Si prevede un decremento massimo del 10% delle prestazioni delle applicazioni durante l'erogazione dal sito secondario.

- Maximum Tolerable DownTime (MTDT): Il massimo intervallo di tempo ammissibile di interruzione della disponibilità del sito primario, fissato a 6 mesi.

3. Struttura Organizzativa per la Gestione della Continuità Operativa:

ACI Informatica ha istituito strutture permanenti per la Business Continuity, che includono:

- Unità di Crisi: la struttura centrale per la gestione delle emergenze. Ha la responsabilità di dichiarare ufficialmente lo stato di crisi, notificare formalmente la "Dichiarazione di Disastro" ad ACI e ad Enti Esterni, attivare le procedure operative e organizzative, attivare il sito secondario e monitorare l'andamento del ripristino. Si occupa anche dell'organizzazione del rientro sul sito primario. La sua composizione include figure apicali come il Direttore Generale, il Business Continuity Manager, il Responsabile Sicurezza Aziendale e il Responsabile Sicurezza Informatica. All'interno dell'Unità di Crisi operano una Unità Tecnologica (composta da DSII e ACI Informatica, con sede nella War Room) e una Unità Strategica (composta dai membri permanenti per le decisioni strategiche e comunicazionali).

- Gruppo di Coordinamento Squadre: Costituito dai responsabili dei settori operativi, è coinvolto sia nella gestione ordinaria del piano (aggiornamento, approvazione modifiche, pianificazione test) sia in condizioni di emergenza (valutazione del danno, coordinamento delle squadre di intervento, comunicazione con l'Unità di Crisi).

- Squadre di Intervento: Personale tecnico-operativo dell'IT Operation, dei Gruppi Applicativi e della Security Operation, organizzato in squadre e reperibile per le attività di ripristino.

- Il Responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie (o dirigente designato, spesso il Responsabile per la Transizione Digitale - RTD) ha la responsabilità dell'attuazione delle MMS-PA. Il Responsabile della Sicurezza Informatica spesso svolge il ruolo di "Segretario della Business Continuity", curando la gestione operativa del piano e la distribuzione della documentazione.

4. Strategie e Misure Tecniche e Organizzative:

La definizione delle misure di protezione si basa su analisi del rischio (Risk Assessment - RA) e analisi di impatto sul business (Business Impact Analysis - BIA), che identificano servizi essenziali, impatti e tempi massimi di indisponibilità.

- Continuità sul Sito Primario: L'infrastruttura di ACI Informatica è progettata per alta affidabilità, con sistemi ridondati, distribuzione su più sale CED per resilienza, bilanciamento del carico e soluzioni di backup veloci.

- Continuità sul Sito Secondario: ACI Informatica si avvale di un data center esterno, configurato in modalità "Campus" con il primario. La soluzione tecnica prevede:

    - Replica sincrona dei dati: L'intera base informativa e di sistema è replicata in sincrono, garantendo che ogni modifica sia contemporaneamente registrata sul sito primario e sul secondario, minimizzando la perdita di dati;

    - Connettività dedicata: La comunicazione tra i due Data Center avviene tramite due circuiti in fibra scura con percorsi distinti, permanentemente attivi per la replica dei dati;

    - Risorse HW e SW disponibili: Il sito secondario dispone di hardware e software necessari per la ripartenza delle applicazioni critiche in caso di disastro;

    - Spazio logistico: È previsto uno spazio di appoggio per il personale che deve operare al sito secondario.

- Gestione Quotidiana della BC: Comporta la verifica e il controllo continuo dei sistemi di storage, dell'allineamento della replica, dei collegamenti in fibra e delle configurazioni hardware e software.

- Procedure di Backup: Oltre alla replica sincrona, i salvataggi delle basi dati sul sito primario vengono copiati progressivamente, in modalità asincrona, su un Datadomain sul sito secondario. È in fase di realizzazione anche la collocazione di un terzo Datadomain, replica del primario, presso un terzo sito.

5. Il Contingency Plan:

Il Contingency Plan è l'insieme di manuali e procedure che descrivono le azioni da intraprendere prima, durante e dopo la dichiarazione dello stato di crisi. È composto dal Manuale Organizzativo (che descrive le funzioni, i ruoli e le responsabilità) e dal Manuale Tecnico (che dettaglia le operazioni tecniche di recupero). Le fasi previste sono:

- Notifica ed Attivazione: Le azioni da svolgere quando si registra o si prevede un'emergenza, allertando il personale preposto e stabilendo il danno. L'attivazione del piano avviene se la valutazione del danno indica un tempo di ripristino sul sito primario superiore alle 6 ore;
- Valutazione del Danno: L'individuazione della natura e dell'estensione del danno subito per determinare gli interventi necessari;
- Recovery sul Sito Secondario: Le procedure dettagliate per attivare i server di infrastruttura e di servizio, verificare la rete, attivare i database server (con verifica della consistenza dei dati), i web e application server e riattivare il servizio;
- Rientro sul Sito Primario: Le operazioni da eseguire al termine della fase di emergenza per ripristinare l'operatività standard, inclusa la sincronizzazione delle basi dati, le prove e lo switch back della rete.