INDICE

Rev.	Data	Motivazione	Redazione DIR	Riesame RSGI	Approvazione DIR
0	06.11.2020	Nuova emissione a dell'introduzione delle norma UNI CEI ISO/EIC 27001:2014			
Ed. 1 Rev. 0	20.06.2022	Cambio ragione sociale e adeguamento alle ISO 27017 e 27018			
Ed. 1 Rev. 1	01.09.2022	Adeguamento alle ISO 27017 e 27018			
Ed. 1 Rev. 2	09.01.2023	Integrazione sistema qualità ISO 9001			
Ed. 1 Rev. 3	08.01.2024	Transizione iso 27001:2022			

SCOPO E CAMPO DI APPLICAZIONE

CODEBASE SRL è un'azienda che opera nel campo della progettazione e assistenza di programmi informatici. Data la natura delle proprie attività, considera la sicurezza delle informazioni un fattore cruciale per la protezione del proprio patrimonio informativo ed un fattore di valenza strategica sul mercato.
Consapevole del fatto che i servizi offerti possono comportare l'affidamento di dati e informazioni critiche, applica il SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) ed il SGQ (Sistema di Gestione per la Qualità) a tutte le attività e ai servizi offerti.
Per questo motivo la società ***CODEBASE SRL*** adotta le misure, sia tecniche che organizzative, necessarie a garantire al meglio l'integrità, la riservatezza, la disponibilità e la qualità sia del patrimonio informativo interno che di quello affidatogli dai propri clienti. Su tali basi è implementato il Sistema integrato (SGSI e SGQ) definito secondo in conformità alle prescrizioni della norma internazionale UNI CEI ISO/IEC 27001:2022 estesa ai controlli UNI CEI ISO/IEC 27017:2015 e UNI CEI ISO/IEC 27018:2019, UNI CEI ISO/IEC 27002:2022 e alla norma UNI EN ISO 9001:2015.

OBIETTIVI E PRINCIPI

L'obiettivo del Sistema Integrato di ***CODEBASE SRL*** è di garantire un adeguato livello di sicurezza dei dati e delle informazioni attraverso l'identificazione, la valutazione e il trattamento dei rischi ai quali i servizi stessi sono soggetti. Inoltre, definisce un insieme di misure organizzative, tecniche e procedurali atte a garantire tale obiettivo.
I macro-obiettivi che ***CODEBASE SRL*** intende raggiungere con l'implementazione ed il mantenimento del Sistema Integrato (SGSI e SGQ) sono:

- Il soddisfacimento di tutti gli stakeholder interni ed esterni all'organizzazione.
- Monitorare il raggiungimento degli obiettivi per la qualità fissati.
- Monitorare il grado di raggiungimento di soddisfazione dei clienti in relazione ai servizi erogati.
- Di applicare e garantire la conformità ad un sistema di gestione per la qualità conforme ai requisiti della norma UNI EN ISO 9001:2015.
- Il soddisfacimento dei requisiti di riservatezza, integrità e disponibilità delle informazioni relative al business, ai clienti, ai fornitori e al personale interno.
- Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
- Garantire una chiara allocazione delle autorità e responsabilità per la sicurezza delle informazioni.
- Garantire una chiara allocazione dei Ruoli e responsabilità condivise all'interno di un ambiente di cloud computing.
- Garantire che il Personale interno abbia un elevato grado di consapevolezza e competenza sul tema della sicurezza delle informazioni;
- Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
- Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.

- Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza.

- Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.

- Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.

- Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.

- Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.

- Garantire la continuità del business aziendale attraverso l'applicazione di procedure di sicurezza stabilite.

- Di applicare e garantire la conformità ad un sistema di gestione per la sicurezza delle informazioni conforme ai requisiti della norma UNI CEI EN ISO/IEC 27001:2022, integrando i controlli previsti dalla stessa norma con le linee guida definite:

    - ISO/IEC 27017:2015 – Prassi per i controlli di sicurezza delle informazioni per i servizi in Cloud

    - ISO/IEC 27018:2019 – Prassi per la protezione dei dati personali trattati nei servizi Cloud pubblici

- Di ottemperare ai requisiti richiesti dall'Agenzia per l'Italia Digitale (AgID) per la qualificazione come fornitori CSP e di servizi SaaS per il Cloud della PA, secondo le circolari AgID n. 2 e 3 del 9/04/2018, e per l'inserimento dei servizi SaaS di Codebase nel Marketplace Cloud previsto nelle circolari stesse.

- Assicurare il rispetto di tutte le normative Italiane cogenti, legali applicabili.

SERVIZI EROGATI IN MODALITÀ CLOUD

L'organizzazione eroga servizi di cloud computing in modalità SaaS (Cloud Service Provider), Software-as-a-Service) in quanto i servizi all'utente finale sono erogati tramite applicazioni basate sul Web.

Il modello SaaS è un metodo per la distribuzione di applicazioni software tramite Internet, dove i provider di servizi cloud ospitano e gestiscono tali applicazioni software per consentire l'uso della stessa applicazione da tutti i tuoi dispositivi accedendovi nel cloud.

Codebase nell'utilizzare l'infrastruttura IAAS a supporto dei propri processi acquisisce il ruolo di Cloud Service Customer.

La segregazione dei vari tenant (End User) è garantita tramite l'utilizzo di container Docker. Docker è un progetto open-source che automatizza il deployment di applicazioni all'interno di contenitori software, fornendo un'astrazione aggiuntiva grazie alla virtualizzazione a livello di sistema operativo di Linux.

Cloud service provider

Il Cloud Codebase offre all'utente finale i seguenti servizi a valore aggiunto:

Piattaforma di CRM per richiedere modifiche al servizio

Piattaforma di autenticazione centralizzata (single sign on)

La segregazione della parte amministrativa del fornitore e del cliente è garantita dalla tipologia di servizio erogato che limita gli accessi dell'end user alla sola piattaforma Codebase e non alla sottostante piattaforma IAAS.

L'accesso alle funzioni amministrative è disponibile anche la funzionalità di Two-Factor Authentication (Accesso con OTP) per accedere all'infrastruttura IAAS.

Nell'ambito della gestione dei cambiamenti Codebase comunica ai vari End User mediante email ogni attività di manutenzione e/o upgrade dei sistemi indicando eventuali disservizi previsti.

La sicurezza della virtualizzazione è garantita dalla infrastruttura IAAS che è basata sulla tecnologia Vmware vCloud Director che fornisce ambienti di rete separati logicamente e protetti da firewall per salvaguardare i requisiti di sicurezza aziendali e garantire protezione e isolamento adeguati.

La gestione ed il provisioning degli account clienti, avviene tramite richiesta del referente dell'Ente al sistema di CRM disponibile su portale utente.

La comunicazione dei data breach avviene in conformità alle procedure aziendali

L'accesso agli asset del cliente avviene in relazione alle disposizioni contrattuali ed in conformità con le dispositivi legislative.

Cloud service customer

Codebase utilizza un provider certificato CSP(Cloud Service Provider) qualificato Tipo C da AGID.

I servizi sono erogati da due Data Center in hosting, situati ad Arezzo e Milano presso la sede Aruba S.p.A. I Data Center utilizzati da Codebase, sono scelti secondo i più moderni standard in termini di affidabilità, prestazioni e sicurezza.

I Data Center, sono costruiti secondo i più moderni standard in termini di affidabilità, prestazioni e sicurezza.Connessi ad Internet con oltre 140 Gb/s, garantiscono una capacità trasmissiva doppia rispetto al fabbisogno effettivo,per assicurare continuità e qualità dei servizi.

I data center rispettano entrambi i massimi standard di resilienza previsti dal livello Rating 4 (former Tier 4) ANSI/TIA 942-B-2017.

Il Rating 4 (former Tier 4) è il massimo livello previsto da ANSI/TIA 942-B-2017 e classifica un data center quale infrastruttura in grado evitare interruzioni dei servizi anche in presenza di guasti gravi grazie ad elevati livelli di ridondanza degli impianti.

Un data center di Rating 4 (former Tier 4) ha componenti ridondati sempre attivi, oltre a percorsi multipli di alimentazione e raffreddamento degli hardware.

Il data center è attrezzato per sopportare un guasto in un qualsiasi punto dell'impianto senza causare downtime ed è protetto nei confronti degli eventi fisici tra i quali anche le catastrofi naturali

(es. incendio, alluvione, terremoto, etc.).

Il servizio Cloud Backup offre la possibilità di cifrare i dati sottoposti a backup ancor prima del trasferimento con una password complessa (standard AES-256).

Di seguito le policy utilizzate:

- Le informazioni storicizzate nell'ambiente cloud possono avere accesso al cloud service, fermo restante che per le macchine a livello di sistema operativo viene applicato la cifratura del dato.
- I processi girano in un multi-tenant virtualizzato cloud service mediante tecnologie Vmware Vcloud Director.
- Gli utenti amministrativi e non che accedono ai servizi sono solo quelli di Codebase
- La locazione dei CED del cloud provider utilizzati è Italia.

RESPONSABILITÀ CONDIVISA E PROPRIETÀ DEGLI ASSET

CLOUD PRO

- L'infrastruttura e tutti gli asset fisici sono di proprietà del CSP
- Le licenze eventualmente fornite (sistema operativo ed applicazioni) sono di proprietà del CSP e vengono concesse in uso al cliente per tutta la durata della sua permanenza sulla piattaforma Aruba secondo le regole stabilite
- Ogni licenza fornita al cliente rimane di proprietà del CSP e viene concessa in uso al cliente per tutta la durata della sua permanenza sulla piattaforma
- Gli indirizzi IP forniti sono di proprietà del CSP.
- Eventuale software installato da Codebase sulla piattaforma messa a disposizione rimane di proprietà e sotto la responsabilità di Codebase.
- Tutto il contenuto a livello di dati prodotto o caricato da Codebase rimane di proprietà e sotto la responsabilità di Codebase.

CLOUD BACKUP

- L'infrastruttura erogante il servizio è di proprietà del CSP
- La licenza del software di backup compresi gli agenti da installare nelle macchine dei clienti è di proprietà del CSP e viene concessa in uso al cliente per tutta la durata della sua permanenza sulla piattaforma.
- I dati prodotti dalle operazioni di backup del cliente sono di proprietà e sotto la responsabilità di Codebase.

CLOUD MONITORING

- L'infrastruttura erogante il servizio è di proprietà del CSP.
- I dati di configurazione prodotti da Codebase sono di proprietà e sotto la responsabilità di Codebase.

SMALTIMENTO SICURO DELL'HARDWARE

Il CSP attua una specifica procedura per garantire che ogni dato presente negli storage che abbiano raggiunto il loro fine vita e che devono essere sostituiti e smaltiti sia completamente e definitivamente rimosso.

REVERSIBILITÀ E CANCELLAZIONE SICURA DATI E FILES

In base a quanto definito nel "Contratto di nomina a responsabile del trattamento dei dati personali ai sensi dell'articolo 28, Regolamento (UE) 2016/679" siglato dal Cliente, le tempistiche di salvaguardia dei dati memorizzati nel sistema informativo aziendale sono di 90 (novanta) giorni.

La tempistica è da intendersi come tempo tecnico necessario per il completamento delle verifiche sui dati da restituire e cancellare, da compiersi in coordinamento con il Cliente.

Così come previsto dalla propria procedura di reversibilità dei servizi SaaS, Codebase si assicura che lo spazio disco messo a disposizione dei clienti venga pulito al termine del tempo di salvaguardia concordato.

SVILUPPO SICURO E TESTING

Gli ambienti di sviluppo di Codebase sono chiusi e inaccessibili ad esclusione del personale Codebase formalmente autorizzato (Area Information Technology).

I deploy vengono effettuati attraverso procedure di progettazione e sviluppo degli applicativi web e rigorose linee guida di sviluppo sicuro, atte ad assicurare il rispetto dei principi di Privacy by Design e Privacy by Default.

Ogni modifica/aggiornamento viene testato secondo fasi di test (di funzionalità, di sicurezza e di non regressione) predefinite e rigorose, il sistema di rilascio in produzione, oltre a richiedere la supervisione di figure di comprovata esperienza, prevede una tracciatura delle attività e delle implementazioni svolte (Tracking System). Infine, tanto per le attività di sviluppo e test è garantito un ambiente sicuro e separato da quello di produzione

BACKUP

I servizi del CSP permettono ai clienti di creare ed impostare i propri backup automatizzati attraverso le soluzioni Cloud Backup, scegliendo le proprie politiche in termini di cifratura, periodicità, tipologia (completi o incrementali) e altre specifiche esigenze.

Il backup giornaliero dei database viene mantenuto per 15 giorni, dal sedicesimo giorno in poi viene mantenuta solo una copia settimanale, per un massimo di 52 settimane. Le prime 15 versioni giornaliere dei database vengono conservate anche sul server principale in modo da permettere una riattivazione rapido nel caso si presentasse un problema ai database o per consentire al cliente di creare dei punti di ripristino per verificare lo stato dei dati nei precedenti 15 giorni.

LOGGING

Codebase raccoglie e conserva i log dei server per assicurare ai propri clienti alti livelli di sicurezza dei servizi SaaS erogati oltre che la conformità normativa. Tali log vengono periodicamente verificati dall'Area Information Technology di Codebase. Codebase registra e conserva i log applicativi nell'utilizzo del servizio SaaS.

Log degli Accessi ai Software Cloud SaaS	Il cliente può accedere in autonomia ai log degli accessi effettuati al servizio SaaS erogato da Codebase. I Log degli accessi alle piattaforme online sono conservati nel database per finalità difensive e nei limiti dei termini stabiliti nel Registro dei Trattamenti.
Log delle Attività	I Log delle operazioni svolte dagli utenti (sia interni - dipendenti - che esterni - clienti - a Codebase.) sono registrate nell'infrastruttura per un periodo di 12 mesi, al termine di tale tempistica i Log vengono cancellati da una procedura automatica e non sono più accessibili. Oltre alle operazioni svolte, i Log delle Attività registrano anche l'utenza personale di colui che le ha compiute.

COMUNICAZIONE CIFRATA

Tutti i servizi SaaS di Codebase rivolti all'esterno utilizzano dei canali di comunicazione cifrati (ad esempio canale HTTPS, che è il risultato dell'applicazione di un protocollo di crittografia asimmetrica al protocollo di trasferimento di ipertesti http e che viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti ed evitare diffusioni e modifiche non autorizzate).

Il seguente elenco descrive il dettaglio dei protocolli utilizzati su rete pubblica dei servizi SaaS Cloud:

Software Cloud SaaS	Il software SaaS Cloud di Codebase è accessibile solo previa autenticazione dell'utente e sono raggiungibili online tramite certificato cifrato SSL/HTTPS.
Assistenza Tecnica	Tutte le attività di assistenza erogate nei confronti dei clienti consentono l'accesso a dati solo previa autenticazione da parte dell'operatore, registrazione delle operazioni svolte, autorizzazione formale da parte del cliente ed in caso di utilizzo di servizi di tele-assistenza crittografia delle sessioni AES (a 256 bit).
IAAS e CSP	L'accesso all'infrastruttura è possibile solo tramite connessione nominale VPN con autenticazione SHA-1 e cifratura a 256 bit.

SINCRONIZZAZIONE

Così come previsto dallo standard internazionale ISO/IEC 27001, tutti i sistemi Cloud di Codebase utilizzano il sistema NTP per sincronizzare i propri orologi e mantenere coerenza degli eventi.

La fonte autoritativa per la sincronizzazione dell'orologio è INRiM - Istituto Nazionale di Ricerca Metrologica - http://www.inrim.it).

Il fuso orario su tutti i sistemi utilizzato è CEST su cui viene utilizzato GMT+1.

SICUREZZA ORGANIZZATIVA

In accordo alla propria Politica SGSI, Codebase SRL assicura che tutti coloro che operano per l'erogazione dei servizi siano adeguatamente formati e consapevoli dell'importanza del patrimonio informativo gestito.

Questa misura applica in particolar modo per le nuove figure aziendali con i quali viene condivisa la politica adottata ed il rispetto dei termini previsti nello specifico accordo di riservatezza (Non Disclosure Agreements) per coloro che svolgono funzioni di sviluppo e manutenzione dell'area IT. Per ciascuna area aziendale sono stati sviluppati programmi di formazione specifici, che vengono ripetuti e testati con cadenza periodica.

Per garantire la sicurezza dei propri servizi, Codebase controlla gli accessi ai dati ed ai sistemi e limita e monitora gli accessi ad essi.

Tra i principi adottati per la gestione della sicurezza organizzativa ci sono:

- "need to know" (Allegato B del D.Lgs. 196/2003) secondo il quale i soggetti che devono compiere attività di trattamento di informazioni sono autorizzati a trattare i soli dati essenziali allo svolgimento dell'attività attribuita;
- "least privilege" secondo il quale ad ogni operatore è concesso il privilegio minimo necessario per poter svolgere i propri compiti in modo da ridurre per quanto possibile il rischio di accesso/modifica/cancellazione degli asset e dei dati gestiti;
- "privacy by design" per il quale l'obiettivo già in fase di sviluppo dei servizi SaaS Cloud il tema del trattamento dei dati sia prioritario per garantire sicurezza e trasparenza oltre al fine ultimo di prevenire un problema;
- "privacy by default" secondo cui si debbano trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste (art. 5 p. 1 lett. b) e per il periodo strettamente necessario a tali fini (art. 5 p. 1 lett. c).

Nello specifico caso in cui si renda necessario l'intervento di Amministratori di sistema Codebase sui sistemi Cloud, è garantito che i privilegi di accesso siano forniti solo sulla base di specifiche procedure definite e che tutte le attività siano eseguite secondo iter ed istruzioni predeterminate per le quali sia possibile mantenere traccia.

GESTIONE DELLE VULNERABILITÀ

Codebase riconosce che la gestione delle vulnerabilità tecniche dei sistemi informatici rappresenti una delle attività cruciali per poter garantire la sicurezza dei propri servizi: per questo motivo sono predisposte delle misure per ricercare, governare e risolvere le vulnerabilità tecniche individuate per evitare che possano comportare impatti negativi sul servizio e sui dati gestiti.

Il Resp. dell'Area Information Technology coadiuvata dall'Amministratore di Sistema compongono il gruppo deputato a eseguire periodiche e regolari scansioni di vulnerabilità e penetration-test sia sui servizi offerti alla clientela, sia sull'infrastruttura IT.

GESTIONE DEGLI INCIDENTI

Codebase ha definito controlli e procedure per poter permettere un approccio organizzato e regolato alla gestione degli incidenti come parte della propria strategia di sicurezza delle informazioni.

Codebase ha individuato nello standard ISO/IEC 27001 i propri principi di riferimento per le attività di pianificazione e predisposizione ad una corretta e tempestiva risposta a eventuali eventi di sicurezza, anche con il supporto di una specifica squadra incaricata in base alla peculiarità della problematica riscontrata.

GESTIONE DELLE CAPACITÀ E DEL CAMBIAMENTO

Al fine di garantire la corretta consegna/erogazione del servizio Codebase ritiene fondamentale monitorare le risorse a disposizione e adottare gli opportuni accorgimenti per lo sfruttamento ottimale delle stesse.

A tal fine sono state individuate alcune risorse cui applicare un costante monitoraggio ed analisi delle capacità per poter permettere di assicurare la normale fruizione dei servizi.

I livelli di connettività, i livelli di occupazione delle risorse, lo spazio su disco ed il dimensionamento dell'infrastruttura sono monitorati con specifici strumenti di monitoraggio.

Gli strumenti di monitoraggio permettono l'impostazione di controlli specifici per ciascun servizio, rilevando le anomalie e permettendo di anticipare le necessità di cambiamento.

I cambiamenti resi necessari dalle attività di monitoraggio e di gestione delle capacità vengono gestiti in modo controllato per permettere di verificarne i risultati e di mantenere traccia delle attività svolte.

POLICY DI SICUREZZA LOGICA E FISICA

Per conoscere in dettaglio le politiche di sicurezza logica e fisica adottate da Codebase nella propria infrastruttura presente nei due Data Center in housing si rimanda si rimanda ai documenti disponibili nei rispettivi siti internet.

RESPONSABILITÀ E RIESAME DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

La Direzione coordina ed è responsabile del rispetto dei principi e della corretta implementazione del SGSI, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- Evoluzioni significative del business.
- Cambiamenti significativi del contesto in cui opera l'azienda.
- Cambiamenti significativi rispetto alle aspettative ed esigenze delle parti interessate alle attività dell'azienda.
- Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio.
- Significativi incidenti di sicurezza.
- Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni.

La Politica della Sicurezza delle Informazioni è formalizzata come documento del SGSI, e viene periodicamente riesaminata e aggiornata per assicurare il suo continuo miglioramento ed è condivisa con il personale interno, i clienti, i fornitori e terze parti rilevanti.

Caltanissetta, 08 Gennaio 2024

La Direzione

Codebase srl
Via Degli Orti, 72
93100 Caltanissetta
P.I.: 02098260850

INDICE

Rev.	Data	Motivazione	Redazione RSGI	Riesame RSGI	Approvazione DIR
0	06.11.2020	Prima emissione			
Ed. 1 Rev. 0	20.06.2022	Cambio ragione sociale e adeguamento alle ISO 27017 e 27018			
Ed. 1 Rev. 1	08.01.2024	Transizione iso 27001:2022			

SCOPO E CAMPO DI APPLICAZIONE

Lo scopo di questa procedura è garantire che i provvedimenti in atto per la continuità della sicurezza delle informazioni dell'Organizzazione siano mantenuti attivi ed efficaci. Si applica a tutte le attività comprese nell'ambito di applicazione del SGI al verificarsi di eventi che possano compromettere la sicurezza delle informazioni.

RIFERIMENTI NORMATIVI

- UNI CEI ISO IEC 27001:2022
- ISO /IEC 27017:2015
- ISO /IEC 27018:2019

TERMINI E DEFINIZIONI

Si fa riferimento alle definizioni contenute nella norma UNI EN ISO 27000, UNI CEI ISO IEC 27001:2022, UNI CEI ISO IEC 27002:2022, ISO /IEC 27017:2015, ISO /IEC 27018:2019 e nella Sezione 3 del manuale del Sistema di Gestione per la sicurezza delle informazioni.

Nell'ambito del SGSI per Continuità operativa si intende: l'insieme di attività volte a minimizzare gli effetti distruttivi, o comunque dannosi, di un evento che ha colpito un'organizzazione o parte di essa, garantendo la continuità nella disponibilità, integrità e disponibilità delle informazioni.

Mission Critical Activity (MCA) è l'attività critica o di supporto al business relativamente ai servizi o prodotti offerti dall'organizzazione (internamente o esternamente), che permettono all'organizzazione di raggiungere i suoi obiettivi di business considerando le stagionalità e/o tempi di rilascio critici.

1. GENERALITÀ

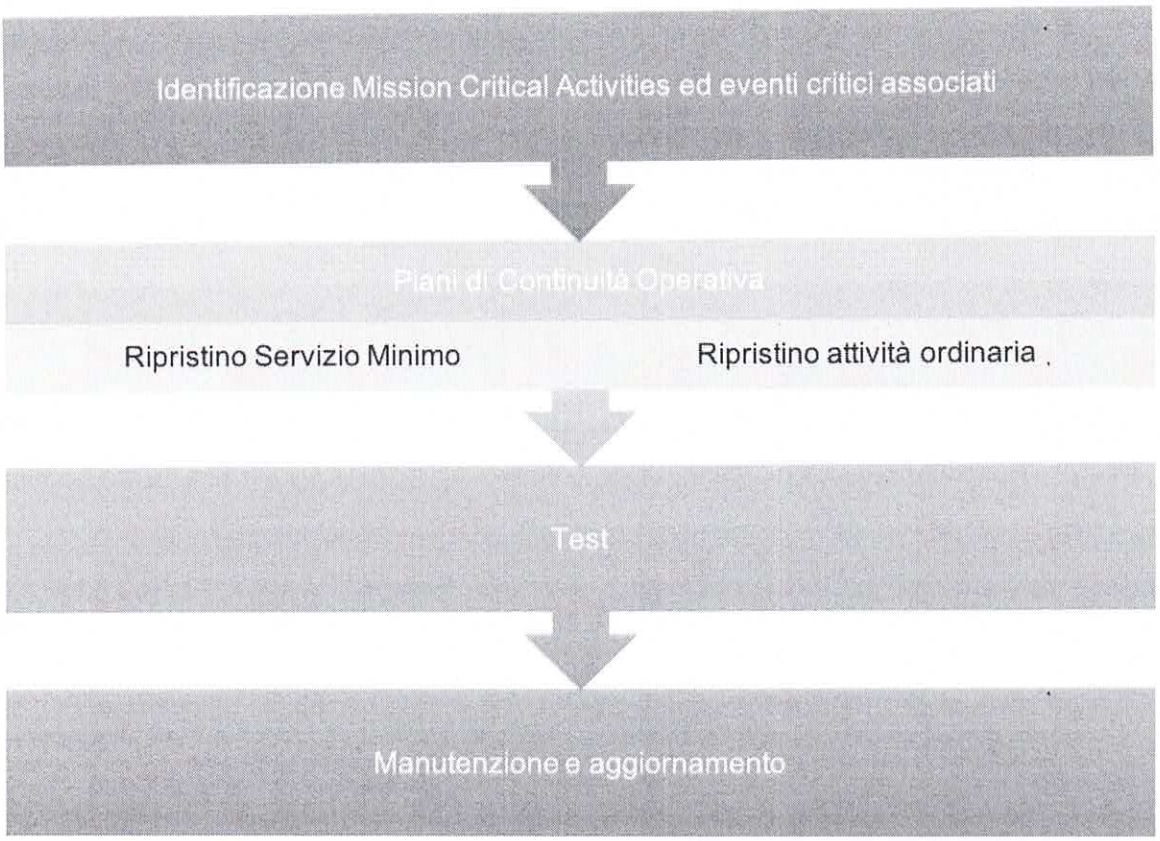
La procedura mira a soddisfare i requisiti di controllo così come riportato nella tabella.

Paragrafo allegato A norma UNI EN ISO 27001:2022	Descrizione
5.29	Sicurezza delle informazioni durante le interruzioni
8.14	Ridondanza delle strutture di elaborazione delle informazioni

2. GESTIONE DELLA CONTINUITÀ OPERATIVA

La gestione della continuità operativa si configura come descritto nel grafico sottostante, in cinque fasi principali. Lo scopo principale è l'elaborazione e l'utilizzo di Piani di Continuità Operativa (PCO).

Le attività svolte per garantire la continuità operativa in funzione della sicurezza delle informazioni sono:



2.1 Identificazione delle Mission Critical Activities

Attraverso l'analisi dei rischi effettuata sia per la valutazione della sicurezza delle informazioni che per la definizione del sistema di gestione della qualità, l'organizzazione definisce le attività critiche e i possibili scenari di crisi ad esse associate che possono minare la continuità operativa. Il **Mod. "Piani di Continuità Operativa"** riporta quanto sopra descritto.

2.2 Definizione dei piani di continuità operativa

Successivamente l'organizzazione per ogni scenario identificato fissa degli obiettivi per il ripristino della continuità operativa. Se necessario, un primo livello di obiettivi identifica il **ripristino di un servizio minimo** dopo l'interruzione (tempi, risorse, attività). Un secondo livello che sancisce il ripristino **dell'attività ordinaria** (tempi, risorse, attività).

Per i due scenari l'organizzazione definisce:

- Obiettivi
- Attività per fronteggiare la crisi
- Responsabilità
- Risorse da utilizzare
- Tempi di ripristino

2.3 Manutenzione e aggiornamento

Il piano viene mantenuto operativo ed aggiornato con cadenza periodica annuale e nel caso in cui ci siano cambiamenti nei processi dell'organizzazione che possano influire sull'efficacia dei PCO.

3. RIDONDANZE

Tutti i sistemi interni che assolvono dei compiti critici per l'organizzazione e di tutti i clienti sono su server, storage e apparati di connettività in alta affidabilità ed in caso di guasto l'organizzazione è protetta dalla perdita di dati e dell'indisponibilità delle informazioni.

Nel dettaglio l'infrastruttura primaria Aruba Enterprise e Aruba Cloud risiedono nel datàcenter di Arezzo di proprietà di Aruba Spa certificato ISO 9001:2015, ISO 27001:2022, ISO 27018:2014, ISO 27017:2015, ISO 27035:2016, ISO 14001:2015 e ISO 50001:2018, la connettività è in alta affidabilità e gli apparati di rete switch e firewall, nel rack sono tutti ridondati.

Tutta l'infrastruttura è virtualizzata con hypervisor Citrix XenServer.

Tutte le nostre infrastrutture sono composte da più server configurati in cloud con attivi i sistemi di alta affidabilità che in caso di failure sono in grado di far ripartire i server virtuali sui nodi rimanenti nel cluster.

Gli storage dedicati alle infrastrutture sono connessi con interfacce 10 Gigabit tutte in alta affidabilità.

4. DISASTER RECOVERY

Il sito di disaster recovery si trova a Milano presso il datacenter di ARUBA, è connesso attraverso una connessione a 10 Gigabit.

L'infrastruttura secondaria è composta da server cloud dove sono attive le repliche asincrone dal sito primario di Arezzo, tutti i sistemi di connettività rete, storage e internet sono configurati in alta affidabilità in modo da garantire la massima disponibilità in caso di problemi.

5. MONITORAGGIO

Le infrastrutture sono sotto monitoraggio attraverso M/Monit che permette, nella maggioranza dei casi, di risolvere problematiche in modo proattivo prima che generino un fermo.

Dalla console di gestione del software di monitoraggio è possibile verificare tutti i servizi configurati.

Inoltre M/Monit è configurato per inviare notifiche dettagliate via mail al gruppo di monitoraggio principalmente o alle mail configurate all'interno del contact group.

Attraverso M/Monit sono monitorati molti tipi di servizi, a titolo di esempio non esaustivo sono monitorati i seguenti servi:

- Consumo CPU;
- Consumo RAM;
- Spazio libero sui dischi rigidi;
- Raggiungibilità da internet dei portali di servizi;
- Raggiungibilità server sulla rete;
- Stato dei servizi pubblicati sui server;

6. ALLEGATI

Nessuno