ErwidCol Financial Services

PIANO DI CONTINUITA' OPERATIVA

Versione 1.1

Sommario

1. PREMESSA

La Business Continuity (BC) è l'insieme delle attività volte a minimizzare gli effetti distruttivi e dannosi di un evento che può colpire un'azienda o parte di essa, garantendone la continuità. In caso di interruzione, mantiene attive le attività aziendali, comprese le persone, le risorse, i fornitori, i servizi ai clienti. Ha una dimensione più ampia rispetto al mero disaster recovery, focalizzato sul solo recupero dei sistemi informatici e delle infrastrutture ICT e ricomprende tale disciplina, che ne è parte.

Elemento fondamentale della Business Continuity è il piano di continuità operativa. Si tratta di un documento che stabilisce come un'organizzazione deve rispondere e recuperare da un'interruzione non pianificata di attività critiche per mantenere le proprie funzioni essenziali. Scopo del piano è minimizzare l'impatto di eventi come disastri naturali, attacchi informatici o interruzioni di servizi, preservando la capacità produttiva, la reputazione e la fiducia di clienti, fornitori e terzi in generale. Esso include l'identificazione delle minacce, la definizione di procedure per la risposta all'emergenza, il ripristino delle attività e la verifica periodica della sua funzionalità.

Erwidcol Financial Services S.p.A. (qui di seguito anche Erwidcol) adotta le misure qui descritte in maniera proporzionale alle dimensioni aziendali, ai volumi ed alla complessità dell'attività svolta, nonché alla tipologia ed alla gamma dei servizi prestati.

1.1 Obiettivi del documento

Il presente documento descrive le misure organizzative, tecnologiche e logistiche adottate per garantire la continuità operativa dei processi critici di Erwidcol in caso di eventi avversi. Gli obiettivi principali sono:

- salvaguardia della continuità dei servizi essenziali;
- protezione dei dati e delle informazioni sensibili;
- limitazione delle perdite (finanziarie e reputazionali);
- conformità alle disposizioni della Banca Centrale di San Marino (BCSM).

1.2 Adozione, aggiornamento e diffusione del documento

Il presente documento ha immediata efficacia e sarà aggiornato al bisogno o qualora intervengano modifiche nella normativa di riferimento ovvero alla struttura organizzativa di Erwidcol.

Al fine di assicurare presso tutti i destinatari la conoscenza dei principi, degli indirizzi e delle procedure adottati da Erwidcol, il piano di continuità aziendale è distribuito a tutti i dipendenti e collaboratori aziendali, che vi si attengono puntualmente, in caso di attivazione.

1.3 Definizioni

Ai fini del presente documento, si intende per:

- backup dati: copia di sicurezza di file, applicazioni e sistemi, creata per poterli ripristinare in caso di perdita o danneggiamento;
- Business Continuity (BC): insieme delle attività volte a minimizzare gli effetti distruttivi e

dannosi di un evento che può colpire un'azienda o parte di essa, garantendone la continuità;

- cloud: server a cui si accede tramite Internet per sfruttare software e database che si eseguono su quei server. Di prassi, i server cloud si trovano in datacenter sparsi per tutto il mondo. Consente la delocalizzazione di dati e di procedure, con accesso da diversi dispositivi dovunque fisicamente presenti;
- disaster recovery: metodi, procedure e tecnologie usati dalle organizzazioni per ripristinare i dati e l'accesso IT dovuti al danneggiamento delle tecnologie aziendali;
- h24/7: operatività 24 ore al giorno, 7 giorni su 7;
- IT: Information Technology/Tecnologia dell'Informazione. Si tratta di un settore che comprende l'uso di sistemi informatici, reti, hardware e software per la gestione e l'elaborazione delle informazioni. Si concentra principalmente su tutto ciò che riguarda l'elaborazione, la gestione e l'archiviazione dei dati;
- ICT: Information and Communication Technology/Tecnologia dell'Informazione e della Comunicazione. In aggiunta all'IT, ricomprende anche i metodi e le tecniche utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni. Include anche le tecnologie di comunicazione, come internet e telefonia, che facilitano lo scambio di informazioni;
- malware: qualsiasi codice software o programma informatico, inclusi ransomware, Trojan horse e spyware, scritto intenzionalmente per danneggiare sistemi informatici o loro utenti;
- processi e servizi critici: funzioni la cui anomala o mancata esecuzione possa:
  1) mettere a repentaglio la capacità dell'impresa di investimento di continuare a conformarsi ai requisiti relativi alla sua autorizzazione o agli altri obblighi ad essa applicabili ai sensi delle presenti disposizioni;
  2) compromettere gravemente i suoi risultati finanziari o la solidità o la continuità dei servizi prestati nell'esercizio delle attività riservate.
- rischio di sostenibilità: evento o condizione di tipo ambientale, sociale o di governance, che, se si verificasse, potrebbe provocare un significativo impatto negativo effettivo o potenziale sul valore di un investimento.

1.4 Contesto normativo di riferimento

La normativa di riferimento è il Regolamento BCSM n. 2024-05 in materia di servizi e di attività di investimento.

Ulteriori riferimenti si possono ottenere dalla analisi della seguente normativa:

- europea
  1) Regolamenti e linee guida EBA/ESMA/EIOPA
  2) EBA Guidelines on ICT and security risk management (EBA/GL/2019/04): richiedono a banche e intermediari di predisporre piani di continuità operativa e disaster recovery.
  3) EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02): continuità operativa come requisito anche per gli outsourcer critici.
  4) ESMA Guidelines on outsourcing to cloud service providers (ESMA50-157-2403, 2021): focus sulla resilienza e BCP in caso di fornitori esterni.
  5) Regolamento (UE) 2022/2554 – DORA (Digital Operational Resilience Act) - In vigore dal 2025: introduce obblighi stringenti su resilienza operativa digitale, piani di continuità e test di disaster recovery per tutti gli operatori finanziari UE.

- italiana
    1) Banca d'Italia - Circolare n. 285/2013 ("Disposizioni di vigilanza per le banche"): nella Parte I, Titolo IV, Capitolo 7 richiede alle banche di dotarsi di piani di continuità operativa e Regolamento sulla gestione dei sistemi informativi (varie disposizioni successive).
    2) CONSOB - Regolamento Intermediari n. 20307/2018: include obblighi organizzativi e di gestione del rischio operativo che si riflettono anche sulla continuità operativa.
- standard tecnici
    1) ISO 22301:2019 – Standard internazionale per i sistemi di gestione della continuità operativa.
    2) ISO/IEC 27031 – Linee guida per la continuità dei sistemi informativi.
    3) COBIT / ITIL – Framework IT richiamati nella gestione dei processi ICT e nella resilienza operativa.

2. AMBITO DI APPLICAZIONE

La procedura si applica a:

- tutte le funzioni aziendali;
- locali operativi, archivi fisici ed elettronici;
- fornitori critici (fornitori di hardware e servizi IT, outsourcer IT, provider di connettività, banche depositarie, controparti di mercato);
- clienti (laddove pertinente).

3. ELEMENTI CHIAVE DEL PIANO DI CONTINUITA' AZIENDALE

Il piano di continuità operativa si articola in:

- Individuazione e classificazione dei processi e dei servizi critici: individuazione dei processi e servizi chiave di Erwidcol, finalizzata a dettare le priorità di intervento;
- identificazione delle minacce: individuazione delle possibili cause di interruzione che potrebbero impattare l'organizzazione;
- valutazione dei rischi: analisi dell'impatto potenziale delle minacce sulle attività aziendali e delle dipendenze critiche;
- pianificazione delle risposte: definizione delle procedure per gestire la crisi e minimizzare le perdite;
- ripristino delle attività: strategie per ripristinare le funzioni critiche e garantire il ritorno ai livelli operativi pre-incidente.
- verifica ed aggiornamento: test periodici e aggiornamenti del piano per garantirne l'efficacia nel tempo.

3.1 Individuazione e classificazione dei processi e dei servizi critici

I processi ed i servizi critici per Erwidcol sono stati identificati come segue, in ordine di tempestività d'intervento:

- operatività sui mercati finanziari;
- sistema gestionale Iridis, sia ambito extra contabile che contabilità generale;
- assolvimento pagamenti ed impegni (fornitori, dipendenti, imposte, ecc.);

- area credito (finanziamenti e leasing, in particolare) per riscontro incasso rate, canoni;
- intranet aziendale, data center, messaggistica interna;
- posta elettronica e telefonia (centralino);
- restanti processi operativi non sopra contemplati.

3.2 Identificazione delle minacce

Gli scenari di crisi considerati sono:

- indisponibilità dei locali (incendi, eventi naturali, violazioni con danneggiamenti, inagibilità in generale);
- guasti ICT (malfunzionamenti hardware/software, cyber attacchi);
- interruzione servizi esterni (energia, rete, connettività);
- eventi eccezionali (pandemie, emergenze, guerre);
- eventi reputazionali o normativi che richiedono attivazione immediata di misure straordinarie;
- adeguatezza patrimoniale.

3.3 Valutazione dei rischi

I rischi sono valutati in termini di rilevanza impattante e probabilità di realizzazione. Da quanto già indicato al punto precedente emerge l'importanza assegnata a ciascuno scenario di crisi.

In linea di massima, stando almeno all'esperienza maturata in circa 25 anni di storia aziendale (seppur sia pacifico che il passato non dia certezze e garanzie per il futuro), dal punto di vista degli impatti sull'operatività e delle probabilità, l'ambito più sensibile è quello dell'ICT, dove quasi quotidianamente si susseguono tentativi di intrusione, virus, malware e similari, ecc. ed a ciò sono state indirizzate molte risorse nel tempo.

Gli altri rischi identificati, seppur potenzialmente possibili, sono più sfumati e ritenuti più rari, e comunque sono, almeno parzialmente, già fronteggiati e limitati come descritto al punto seguente.

3.4 Pianificazione delle risposte

L'organizzazione di Erwidcol è pensata e strutturata per fronteggiare le minacce, eliminandole laddove possibile o almeno gestendole per mitigarle e limitarle.

Con specifico riferimento all'ICT, va precisato che il sistema informativo aziendale è compliance con le prescrizioni normative. In particolare:

- è affidabile, ridondante, sovradimensionato, in linea con gli standard internazionalmente adottati;
- è adeguato al contesto operativo ed ai rischi a cui Erwidcol è esposta;
- consente la pronta registrazione dei fatti di gestione con un elevato grado di attendibilità, così da consentire di ricostruire l'attività di Erwidcol a qualsiasi data e per ciascuno servizio prestato;
- garantisce elevati livelli di sicurezza, sia fisica che logica. L'hardware (server di rete e server dati virtualizzati, apparati di rete e di comunicazione) è posizionato in appositi locali. L'accesso al sistema è vigilato e protetto. Ciascun utente, che lascia traccia di ogni azione inserimento o modifica di dati (il software rileva e conserva i log), è dotato di specifica abilitazione compatibile al ruolo ed alla funzione che occupa. I firewall fisici e virtuali, ed i relativi controlli anche esternalizzati (h24/7) impediscono le intrusioni

dall'esterno, virus, malware, ecc. Sono comunque previste procedure di backup dati sia interne, su supporti fisici, che esterne in cloud. Lo stesso dicasi per le impostazioni e configurazioni di sistema, così da agevolare le strategie di disaster recovery adottate;
- le risorse umane assegnate alla funzione (interne ed esterne) sono adeguate adeguata all'operatività aziendale.

Tra gli scenari di crisi di cui al punto 3.3, ve ne sono alcuni fronteggiabili da Erwidcol in autonomia, mentre altri, di carattere esogeno, esulano dalla mera sfera aziendale.
Rientrano nel primo gruppo le iniziative sinteticamente qui di seguito elencate:

- protezione fisica ed assicurativa dei locali per violazioni o per incendi ed in parte per eventi naturali;
- strategie di protezione dati e sistemi da intrusioni anche con vigilanza h24/7, ridondanza hardware, backup dati in locale ed in cloud e disaster recovery in cloud;
- gruppi di continuità UPS per l'energia;
- normativa interna e ufficio di compliance per venti normativi e reputazionali;
- disponibilità di capienti fondi di riserva e di accantonamento a bilancio per far fronte ad eventuali eventi avversi generanti esigenze patrimoniali.

In contrapposizione, gestire interventi nell'ambito degli eventi eccezionali (e come tali non prevedibili ed a bassa probabilità di realizzazione), piuttosto che innalzare il livello di protezione (ad esempio dislocando copie di documenti, sistemi hardware e software, dati, ecc. in altri locali con gruppi elettrogeni e connessioni in fibra ottica e satellitari ridondanti, a sé stanti) comporta impegni, fisici, organizzativi, tecnici ed economici che rendono tale strategia in parte o in toto inefficace ed inopportuna, alla luce sia delle probabilità di realizzazione che dei modelli di ripristino adottati.

3.5 Attivazione piano e ripristino delle attività

Coerentemente con quanto già indicato, qualora le strategie di contrasto si rivelassero in toto o in parte inefficaci, sono previste strategie di ripristino basate sulla tempestività e sulla necessità di rimetter in linea l'operatività. Così, rilevato l'evento critico, il suo impatto e la sua portata, è compito del Capo della Struttura Esecutiva decidere se il piano vada attivato o meno. In sua mancanza, la funzione passa ad un membro del Consiglio di Amministrazione o, in mancanza anche di quest'ultimo, al dipendente più in alto in grado nella gerarchia aziendale presente. Post attivazione, è necessario coinvolgere direttamente il team di crisi.
In linea generale, se l'emergenza non è prontamente ed autonomamente superabile, neppure con l'attivazione del piano di continuità, ne va data tempestiva notizia al Consiglio di Amministrazione ed al Collegio Sindacale, ed eventualmente, anche agli Azionisti ed a seconda della natura dell'evento avverso, del suo protrarsi nel tempo e dell'impatto sull'operatività e/o sul patrimonio aziendale, anche alla Banca Centrale della Repubblica di San Marino, compatibilmente con lo stato delle comunicazioni. Laddove pertinente, vanno informati anche i clienti.
Ciò premesso, il ripristino delle attività avverrà come qui di seguito descritto:

- indisponibilità dei locali e connessi guasti ICT (sezione del piano di continuità dedicata al sistema informativo-contabile)

  Rilevata la problematica connessa ai locali (ad esempio un incendio) è necessario agire per la sicurezza dei presenti ordinandone l'evacuazione, secondo il relativo piano. Se i locali aziendali non possono esser bonificati in brevissimo tempo, è necessario prontamente trovare, anche in via emergenziale e provvisoria, nuovi locali da cui operare. Alla luce del parco immobiliare direttamente o indirettamente riconducibile alla

proprietà, si stima che ciò possa richiedere indicativamente una giornata lavorativa. Definiti i locali presso cui posizionarsi, avvisati a seconda dl bisogno i partner ICT, l'urgenza sarà quella di preservare quanto in essere (ciò vale anche in caso di guasti ICT). L'ordine con cui procedere, la descrizione delle primissime attività da intraprendere in emergenza e la stima dei tempi di attuazione sono i seguenti:

- operatività sui mercati finanziari, anche con ricorso a sistemi esterni (pc portatili, connessioni anche via telefono cellulare), al fine di mantenere in essere la possibilità di intervento per gestire i rischi dei portafogli attivi e, conseguentemente, limitarne le potenziali perdite finanziarie. Ricomprende sia i portafogli dei terzi clienti che quello di proprietà. Include l'accesso agli info provider ed ai sistemi di compensazione, ed alle posizioni presso i depositari di liquidità e strumenti finanziari, così da poter ovviare all'eventuale indisponibilità del sistema informativo aziendale in generale, in particolare del gestionale Iridis. Tempi d'intervento previsti: entro due ore;
- sistemi di comunicazione esterna (posta elettronica e telefonia) per i quali si agirà in via provvisoria con telefoni cellulari e pc esterni, essendo il server di posta elettronica virtuale ed in cloud. Tempi d'intervento previsti: entro due ore;
- gestione di pagamenti ed impegni urgenti (fornitori, dipendenti, imposte, compensi titoli, ecc.), per i quali sarà necessario aver l'accesso ad Internet anche con pc esterno o telefono cellulare, così da poter operare direttamente nelle aree riservate delle banche depositarie. Lo stesso dicasi per riscontrare l'incasso di rate di rimborso di finanziamenti e canoni di leasing. Tempi d'intervento previsti: entro quattro ore.

Se i locali aziendali sono disponibili (o, in mancanza, lo siano nuovi locali, almeno provvisori, ma dotati di cablaggi e connessioni) si potrà cominciare la ricostruzione. In tal senso, l'ordine con cui procedere, la descrizione delle attività da intraprendere e la stima dei tempi di attuazione sono i seguenti:

- riattivazione in toto del sistema informativo, sia hardware (server ed apparati di rete) che software di sistema, anche a mezzo di soluzioni tampone, da valutarsi al bisogno unitamente al fornitore tecnico con il quale sussistono pattuizioni in tema di disaster recovery, sfruttando le impostazioni di sistema già disponibili in quanto salvate in cloud. Tempi d'intervento previsti: indicativamente entro la giornata, al massimo entro il secondo giorno lavorativo;
- reinstallazione del sistema gestionale Iridis, utilizzando gli specifici backup disponibili. Tempi d'intervento previsti: entro il giorno successivo al ripristino dell'infrastruttura di rete, le linee di connessione incluse;
- ripristino ordinarietà per intranet aziendale, data center, messaggistica interna, sistemi di comunicazione esterna (posta elettronica e telefonia/centralino). Tempi d'intervento previsti: entro il secondo giorno successivo al ripristino dell'infrastruttura di rete;
- immissione delle registrazioni dell'operatività svolta in emergenza (vedasi il primo ed il secondo punto) nel sistema gestionale Iridis. Tempi d'intervento previsti: attività da implementarsi non appena disponibile agli addetti il gestionale Iridis, a seconda dei volumi si stima possa richiedere da una a due giornate lavorative;
- ripristino pieno e totale dell'attività in via definitiva. Tempi di sviluppo previsti: da valutarsi, sulla base della necessità di sostituire l'hardware e sui relativi tempi di ordine e consegna, stimabile probabilmente in due o tre settimane.

- interruzione di servizi esterni (energia, rete, connettività)

  In attesa del ripristino di tali servizi, si dovrà operare in via temporanea. A tal fine, vale quanto già detto sopra. L'ordine con cui procedere, la descrizione delle attività da

intraprendere in emergenza e la stima dei tempi di attuazione sono i seguenti:

- operatività sui mercati finanziari, anche con ricorso a sistemi esterni (pc portatili, connessioni anche via telefono cellulare o via rete telefonica tradizionale), al fine di mantenere in essere la possibilità di intervento per gestire i rischi dei portafogli attivi e, conseguentemente, limitarne le potenziali perdite finanziarie. Ricomprende sia i portafogli dei terzi clienti che quello di proprietà. Include l'accesso agli info provider ed ai sistemi di compensazione, ed alle posizioni presso i depositari di liquidità e strumenti finanziari, così da poter ovviare all'eventuale indisponibilità del sistema informativo aziendale in generale, in particolare del gestionale Iridis. Tempi d'intervento previsti: entro due ore;
- sistemi di comunicazione esterna (posta elettronica e telefonia) per i quali si agirà in via provvisoria con telefoni cellulari e pc esterni, essendo il server di posta elettronica virtuale ed in cloud. Tempi d'intervento previsti: entro due ore;
- gestione di pagamenti ed impegni urgenti (fornitori, dipendenti, imposte, compensi titoli, ecc.), per i quali sarà necessario aver l'accesso ad Internet anche con pc esterno o telefono cellulare, così da poter operare direttamente nelle aree riservate delle banche depositarie. Lo stesso dicasi per riscontrare l'incasso di rate di rimborso di finanziamenti e canoni di leasing. Tempi d'intervento previsti: entro quattro ore.

- eventi eccezionali (pandemie, emergenze, guerre)

  Per loro natura, si tratta di eventi imprevedibili. E' quindi piuttosto arduo definire delle regole per porvi rimedio senza conoscerli a priori. Tuttavia, alla luce dell'esperienza maturata con il Covid 19, si può ragionevolmente ipotizzare che l'organizzazione aziendale, flessibile, radicata, delineata, possa risponder efficacemente all'evento straordinario. La vera incognita, che certamente colpirebbe Erwidcol ed i suoi clienti, ma che avrebbe una enorme portata mondiale, riguarda lo scenario nel quale i mercati finanziari sospendano la loro attività, rendendo i titoli, di fatto, non negoziabili. Si tratterebbe di uno shock che minerebbe le nostre economie, con ripercussioni rilevanti ben oltre la finanza. Se da una parte le probabilità che si possa verificare un accadimento avverso di questo tipo sono veramente molto basse, dall'altra si tratterebbe di uno scenario che Erwidcol può solo subire, di uno stravolgimento epocale al quale è davvero complesso contrapporre contromisure preventive efficaci. La speranza è che, nella remota ipotesi in cui dovesse accadere qualcosa di simile, i mercati possano esser ripristinati nella loro piena operatività nell'arco di pochi giorni, prima che l'intero sistema finanziario e bancario ne sia corrotto.

- eventi reputazionali o normativi che richiedono attivazione immediata di misure straordinarie

  Fin tanto quanto non è chiarita la natura dell'evento verificatosi, non si può definire ed attuare alcuna reazione. Immediatamente, avuta notizia dell'emergenza, l'ufficio compliance nello specifico, e la struttura dei controlli interni più in generale, affiancano il Capo della Struttura esecutiva (o chi per Egli) nella delineazione del quadro e delle strategie di superamento, avvalendosi, se ritenuto opportuno, anche di professionisti esterni. Definite quindi le misure, si passa prontamente alla fase attuativa. In caso di necessità l'Assemblea dei Soci ed il Consiglio di Amministrazione, in presenta di tutti gli Azionisti (nel primo caso) e di tutti gli Amministratori (nel secondo), si possono riunire anche senza la formalità della convocazione, quindi con estrema rapidità e tempismo.

  Si noti che, comunque, il Regolamento Interno Generale e, in via più ampia, la normativa interna, delineano regole e procedure a cui attenersi anche in mancanza della presenza di una guida e/o di decisioni straordinarie, ed in linea di massima, comunque, dovrebbero

consentire l'ordinaria continuazione operativa.

- adeguatezza patrimoniale
  In prima battuta è necessario attivarsi immediatamente per contenere eventuali perdite, minusvalenze, sopravvenienze o insussistenze passive. Poi ne va valutata la portata e va verificato se i fondi accantonamento e le riserve stanziate siano sufficienti per farvi fronte, e se del caso, occorre procedere in tal senso. Qualora così non fosse, sarà necessario coinvolgere prontamente gli Azionisti, ai quali compete assumere le decisioni inerenti. A stretto giro, ne andrà poi data piena informativa alla Banca Centrale della Repubblica di San Marino.

3.6 Verifica ed aggiornamento

L'Internal Audit, affiancato di volta in volta, dalla funzione direttamente coinvolta, promuove periodiche verifiche attraverso simulazioni (c.d. "*stress test*") aventi riguardo ai processi ed ai servizi critici come sopra individuati, per valutare l'affidabilità e l'efficacia del piano di continuità aziendale. Qualora l'Internal Audit rilevasse carenze ed individuasse le relative correzioni e/o possibili ottimizzazioni, ne da nota al Capo della Struttura Esecutiva per procedere, se del caso, all'adeguamento del piano di continuità, che comunque sarà oggetto di revisione a seguito di nuove minacce ed anche di modifiche organizzative, normative o tecnologiche rilevanti.

4. FORMAZIONE DEL PERSONALE

Il personale tutto, a cui è stato fornito il presente piano di continuità aziendale, è periodicamente aggiornato a mezzo di specifici corsi di formazione.

5. STRUTTURA DI GESTIONE DELL'EMERGENZA

- Capo della Struttura Esecutiva, responsabile attivazione del piano di continuità aziendale;
- team di crisi (composto dai responsabili delle funzioni specificatamente interessate: Sala Operativa, Amministrazione, IT, Personale, Commerciale, Segreteria, Compliance, Internal Audit), gestione del piano di continuità aziendale;
- tutto il personale interessato, esecuzione delle procedure secondo le istruzioni fornite dal piano di continuità aziendale e dal team di crisi.

6. CONTATTI DI EMERGENZA

- Gendarmeria: 112 o 113
- Polizia Civile/Vigili del Fuoco: 115 - 0549 887776/887769 - antincendio@poliziacivile.smi
- Protezione Civile: 0549 887088 – protezione.civile@pa.sm
- Centrale Operativa Interforze h24: 112/113/115 - 0549 888888 - centraleoperativainterforze@pa.sm
- emergenza sanitaria: 118
- Banca Centrale della Repubblica di San Marino: 0549 981010 – fax 0549/981019 - info@bcsm.sm

- Onit Sistemi: 0547 635888/313110 – ns. referente Francesco Salvadorini fsalvadorini@onitsistemi.it
- Arcoba (Iridis): 030 7777841 – info@arcoba.it
- Azienda Autonoma di Stato per i Servizi Pubblici AASS: 0549 999102 (pronto intervento)
- TIM San Marino: 0549 886303 (segnalazione guasti) – WhatsApp 0549 886303