STATO DEL DOCUMENTO

REVISIONE	PARAGRAFO	DESCRIZIONE	DATA
00		Emissione documento	01/12/17
01	Tutto il piano	Aggiornamento documento	19/01/2018
02	Tutto il piano	Aggiornamento documento	24/08/2018
03	Tutto il piano	Aggiornamento documento e aggiunta dell'Appendice	10/10/2018
REDATTO E VERIFICATO DA: Silvia Misseri		APPROVATO DA: Gian Domenico Volpi	

PARTE A - PIANO DI CONTINUITA' OPERATIVA

1. FINALITA' E AMBITO DI APPLICAZIONE – ATTIVITA' DI CUSTOMER SUPPORT

Nell'ambito delle attività svolte da PA&Mercato, quella di customer support si distingue per le sue peculiarità da cui consegue la necessità di garantire una continuità nell'erogazione della stessa a favore del cliente. Per questa ragione la Società si è dotata di una BIA allegata nell'appendice al presente documento e di un Piano di Continuità Operativa (BCP) e Disaster Recovery (DR) al fine di disporre di procedure atte a gestire e superare condizioni di emergenza e di disastro che impediscono la normale erogazione del servizio medesimo.

In particolare, al verificarsi di un'emergenza e/o disastro, deve essere garantito:

1. Accessibilità delle sedi operative;
2. Disponibilità del personale essenziale all'erogazione del servizio;
3. Funzionamento dei servizi infrastrutturali;
4. Accesso ai dati necessari per svolgere il servizio e conservazione degli stessi;
5. Funzionamento del sistema informativo.

Il presente Piano di Continuità Operativa documentato (BCP) racchiude tutte le informazioni e procedure necessarie per la gestione di eventi straordinari che compromettano l'ordinaria attività lavorativa della Società. Il BCP prevede al suo interno una sezione appositamente dedicata del Piano di Disaster Recovery (DR) che definisce i possibili disastri e gli scenari di rischio, individua i processi critici e le figure di riferimento, interne ed esterne alla Società, in caso di gravi problemi oltre che le modalità di risoluzione degli stessi.

Tutti i dipendenti sono a conoscenza delle procedure da mettere in atto per affrontare la condizione di disastro e/o emergenza in modo che possano continuare a fornire i servizi di customer support in caso di evento disastroso.

Il presente documento è finalizzato a illustrare le modalità tecnico/organizzative a cui la Società deve attenersi per garantire l'operatività dei propri servizi, rispettando un predeterminato periodo di tempo, a seguito di disastro o grave evento dannoso.

Nella redazione del Piano di Continuità Operativa la Società ha cercato di analizzare e ridurre le cause di rischio e ha aumentato i livelli di sicurezza delle proprie strutture. Il Piano in oggetto racchiude quindi tutte le informazioni legate all'organizzazione logistica della Società, dalla dichiarazione dell'emergenza al rientro alla normalità fino alle metodologie atte a riconoscere una situazione di crisi e far così fronte alla stessa. Tale Piano include i processi di gestione della crisi e del disaster recovery cioè le procedure riferite alle modalità di ripristino delle attività per garantire la prosecuzione dell'erogazione dei servizi.

Il presente Piano permette di stabilire quali siano le procedure alternative da attuare in caso di disastro per garantire l'operatività di PA&M garantendo, attraverso i test periodici, l'efficacia delle procedure di ripristino.

Il servizio di customer support erogato dalla nostra Società, per le sue implicazioni nei confronti dei clienti, è catalogato come "critico", in quanto in caso di carenza di parte degli elementi necessari per il suo svolgimento (es. personale, attrezzature informatiche, servizi TLC) risulta impossibile eseguirlo con gravi ripercussioni sulla qualità del servizio.

Il Piano di Continuità Operativa valuta la criticità del servizio prevedendo le strategie di ripristino: sito alternativo, metodologie per il backup, apparecchiature per il backup, ruoli e responsabilità delle figure coinvolte. Particolare attenzione viene data all'interno del BCP alla definizione degli scenari di disastro in quanto il non tempestivo riconoscimento della gravità della situazione venutasi a creare può determinare un ritardo irrecuperabile nella dichiarazione di emergenza e quindi nella gestione della stessa.

Il personale addetto al servizio ha, di norma, il compito di rilevare le condizioni di emergenza e di comunicarle alla *struttura aziendale dedicata alla gestione delle crisi (Comitato Gestione Crisi)* che si attiverà nei tempi e nelle modalità previste dal presente Piano.

La Società dispone di due sedi operative:

- primaria: Via Sandro Pertini, 5 – loc. Antella, Bagno a Ripoli (FI)

- secondaria: Via Chiantigiana 103-103/a – loc. Ponte a Ema, Bagno a Ripoli (FI)

1.1. RUOLI E RESPONSABILITÀ

In questa sezione vengono elencate le figure facenti parte del Comitato di Gestione Crisi, cui competono le responsabilità nel processo decisionale durante l'emergenza.

Il Comitato di Gestione Crisi è l'organismo di vertice nella gestione delle crisi a cui spettano le principali decisioni e la supervisione delle attività delle risorse coinvolte. È l'organo di direzione strategica dell'intera struttura in occasione dell'apertura della crisi e, inoltre, ha la responsabilità di garanzia e controllo nell'attuazione del Piano BC e DR.

Le decisioni del Comitato saranno documentate in apposita relazione nel momento in cui sarà conclusa l'emergenza e controfirmate dal Responsabile o dal Vice-responsabile Continuità Operativa. La relazione dovrà recare tutte le informazioni relative all'attivazione del processo di continuità operativa, alla dichiarazione di rientro dall'emergenza, compito spettante al Comitato di Gestione Crisi, che dovrà riunirsi per valutare l'emergenza e prendere le necessarie decisioni per provvedere al rientro dall'emergenza.

Il Comitato di Gestione Crisi della Società è composto dalle seguenti figure:

- Responsabile Continuità Operativa (RCO) e Responsabile Customer Support: Silvia Misseri; mail. silvia.misseri@pamercato.it – cell. 393.8909862
- Vice- responsabile Continuità Operativa e Responsabile dei servizi telematici –Elena Aiazzi: mail. elena.aiazzi@pamercato.it - cell. 328.7694243
- Legale rappresentante della Società: Gian Domenico Volpi – mail. giandomenico.volpi@pamercato.it – cell. 335.8014670

In caso di dichiarazione di disastro/emergenza, il RCO provvede a contattare tutte le figure facenti parte del Comitato di Gestione Crisi ai riferimenti sopra indicati.

Il Comitato di Gestione Crisi si occupa di:

- Definizione, approvazione e aggiornamento del Piano di Continuità Operativa;
- Valutazione delle situazioni di emergenza e dichiarazione dello stato di crisi;
- Avvio delle attività di recupero e controllo del loro svolgimento;
- Rapporti con l'esterno e comunicazioni ai dipendenti;
- Avvio delle attività di rientro alle condizioni normali e controllo del loro svolgimento;
- Dichiarazione di rientro;
- Gestione di tutte le situazioni non contemplate ma necessarie per la corretta attuazione del BCP;
- Promozione e coordinamento delle attività di formazione e sensibilizzazione sul tema della continuità operativa.

In condizioni di incidente disastroso, il Comitato assume il controllo di tutte le operazioni e la responsabilità sulle decisioni per affrontare l'emergenza, ridurne l'impatto e soprattutto ripristinare le condizioni preesistenti.
In condizioni di incidente grave, il Responsabile del Comitato di Crisi può decidere di lasciare il coordinamento delle operazioni al Comitato di Crisi stesso oppure di gestirlo in autonomia.

Il Comitato deve essere supportato dalle altre figure presenti in azienda e dal personale stesso, ove necessario, per garantire il funzionamento del BCP in relazione alle seguenti attività:

- supporto negli eventuali spostamenti;
- per garantire il funzionamento e l'accesso a tutte le infrastrutture informatiche e di telecomunicazioni predisposte;
- aggiornamenti relativi alle notizie provenienti dai canali pubblici di comunicazione;
- esame di tutti gli aspetti di sicurezza, in particolare per quanto riguarda la verifica del grado di sicurezza offerto dalle configurazioni adottate per l'emergenza e la protezione dei dati, o tramite il riesame delle soluzioni adottate per il ripristino dei sistemi e per il rientro alla normalità.

Il Responsabile della Continuità Operativa (RCO), ha il compito di contattare tutte le figure del Comitato di Gestione Crisi per le riunioni periodiche e provvedere agli aggiornamenti dei piani. Le riunioni periodiche sono fissate a cadenza semestrale; sono fatte salve le convocazioni straordinarie

ogniqualvolta il RCO ritiene necessario procedere alla revisione del Piano. Durante le riunioni saranno redatti appositi verbali sottoscritti e conservati in archivio cartaceo presso i locali della Società. La validità delle soluzioni e delle azioni presenti nel Piano di Continuità Operativa e nel Piano di Disaster Recovery saranno valutate periodicamente e ne verrà dato atto nei verbali delle riunioni del Comitato di Gestione Crisi.

In caso di dichiarazione di disastro/emergenza il RCO provvede inoltre a redigere una relazione che illustri le fasi e l'evoluzione dell'emergenza che sarà archiviata nell'archivio informatico della Società e che sarà inviata, qualora fosse richiesto, al cliente/clienti che sono stati interessati dall'attivazione del Piano BC e DR.

2. TLC

Gli strumenti TLC utilizzati dalla nostra Società comprendono: pc, telefoni collegati alla rete fissa, telefoni collegati alla rete mobile, collegamento internet 20 mega con 512 K garantiti. È presente in un inventario dettagliato delle infrastrutture TLC della Società al punto 6 dell'appendice al presente Piano.

La sede principale è dotata di un impianto elettrico in cui i pc, i telefoni fissi e i componenti Hardware Centralizzati sono alimentati da un gruppo di continuità UPS che ne garantisce la funzionalità in caso di abbassamenti, innalzamenti o assenza di tensione, per circa 30 minuti.

Nello specifico, la nostra sede dispone complessivamente di 4 canali di Fonia Telecom Italia (Linee telefoniche) ripartite in 2 diversi collegamenti BRI ISDN 2 canali ciascuno e due account Voip Timenet con 5 canali ciascuno il tutto gestito da un Sistema Centralizzato VOIP con alta affidabilità data da due Hardware fisici con le stesse capacità in grado di sostituirsi a vicenda. Il servizio di Back-up del sistema VOIP, attivabile per tutte le tipologie di linea VOIP (linea singola o GNR), garantisce la continua raggiungibilità dell'utente anche nel caso in cui il collegamento Internet non funzioni. È sufficiente indicare un numero, fisso o cellulare, ed il sistema dirotterà le chiamate che non sono in grado di raggiungere il numero VOIP verso la numerazione di back-up.

In questo modo saremo in grado di operare su più tecnologie e neutralizzare eventuali disservizi dati da assenza di Linee degli Operatori, in quanto fruiremo dei canali di Fonia e Dati in tre diverse modalità: con tecnologia tradizionale di Telecom Italia, da rete Voip da Timenet e infine da rete Mobile UMTS da Vodafone. Nella nostra sede sono inoltre predisposte due linee di collegamento internet: un ADSL Telecom Italia e un xDSL TimeNet di backup.

Gli addetti al customer support dispongono ciascuno di un computer fisso o portatile collegato alla rete aziendale per erogare il servizio. Ogni computer è dotato di un accesso in locale alle caselle e-mail dedicate al servizio per ciascun ente/piattaforma da supportare, con relativa archiviazione.

In caso di evento dannoso, la continuità operativa del servizio è garantita nel seguente modo:

- Nel momento immediatamente successivo al verificarsi di un malfunzionamento, nella sede principale:
    - Linee telefoniche: data la diversità delle due tecnologie di rete fissa qualora si verifichi un malfunzionamento su Telecom è possibile contare sulla telefonia Timenet e viceversa, inoltre la telefonia Timenet permette, attraverso una semplice procedura online, di deviare le chiamate su qualunque apparecchio telefonico anche in caso di guasto del router. Gli addetti al customer support inoltre dispongono di cellulari di servizio da utilizzare in caso di indisponibilità totale della rete fissa.
    - Linea internet: in caso di indisponibilità di collegamento Telecom, gli operatori sono istruiti sul cambiamento manuale dell'indirizzo IP per passare al router Timenet da effettuare su ogni pc e sono dotati inoltre di router portatili per collegarsi a internet in UMTS e continuare a erogare il servizio. In caso di assenza di internet non è possibile gestire il programma del centralino da remoto, ma ogni addetto è a conoscenza della procedura manuale per attivare e disattivare i telefoni.
    - Computer: nella sede principale sono disponibili pc portatili, in dotazione agli addetti al servizio, programmati con i software e gli accessi necessari (es. piattaforme, posta, software per erogare l'attività di customer support) per garantire l'operatività del servizio tramite una pronta sostituzione dei pc fissi qualora manchi la corrente elettrica, garantendo un'autonomia di circa 2 ore per pc. A tale scopo, le batterie dei pc portatili sono verificate sistematicamente, a cadenza settimanale e, ove necessario, ricaricate.
- In un secondo momento, trasferendosi nella sede secondaria:
    - Linee telefoniche fisse: la sede è dotata di una propria rete telefonica fissa, sulla quale dirottare le telefonate in entrata di Stazioni Appaltanti ed Operatori Economici.
    - Linea internet: la sede è dotata di una rete internet 20 mega che garantisce l'erogazione del servizio da parte degli addetti al customer support. Inoltre si specifica che i router portatili sopra indicati possono essere trasferiti nella sede secondaria ove necessario.
    - Pc portatili: in caso di trasferimento nella sede secondaria gli addetti porteranno con sé i pc portatili sopra descritti, con la possibilità di ricaricarli alla rete elettrica (se disponibile) e potranno inoltre usufruire di altri pc portatili che troveranno direttamente in loco.

3. SERVIZIO DI ARCHIVIAZIONE E ATTIVITA' DI RECUPERO DATI

Tutti i dati acquisiti durante lo svolgimento del servizio di *customer support*, unitamente agli altri dati prodotti/acquisiti dalla Società, sono archiviati in tempo reale su uno "Storage", dotato di backup

automatico e in cloud. Il salvataggio dei dati viene altresì replicato quotidianamente, sempre in modalità automatica, in ulteriore Hardware (PC fissi, Hard-disk USB, storage secondario).

Lo storage contiene lo storico dei salvataggi di una settimana: questo garantisce che in caso di perdita accidentale dei dati salvati all'interno dello stesso, sia possibile recuperarli accedendo all'ultimo salvataggio effettuato.

Il servizio offerto da Dropbox consente il salvataggio dei dati in cloud con un adeguato livello di sicurezza dal momento che il trasferimento dei dati avviene criptandoli come descritto dallo stesso fornitore di servizi.

È inoltre attivo un ulteriore storage di backup dedicato alla ridondanza dei dati contenuti in quello principale posizionato nella sede secondaria. Anche lo storage secondario è sincronizzato al cloud, che garantisce un back up automatico in tempo reale di tutti i dati contenuti al suo interno.

Ogni pc utilizzato dalla Società è dotato di un firewall software. Per garantire un maggior grado di sicurezza dei dati, è stato installato anche un firewall hardware.

4. TEMPI ENTRO I QUALI I SERVIZI DEVONO ESSERE RECUPERATI (RTO)

L'RTO, acronimo inglese di Recovery Time Objective, rappresenta il tempo massimo accettabile per operare il ripristino dei servizi di *customer support* senza determinare un disservizio altrimenti non recuperabile in termini qualitativi.

Il RTO è fissato in 60 minuti, rilevato come il lasso di tempo necessario per ripristinare l'operatività del servizio attraverso la riattivazione delle TLC, come indicato al precedente par. 2.

Il raggiungimento del RTO prevede degli step intermedi che corrispondono a recuperi parziali di operatività per riuscire a far fronte, anche se parzialmente, alle richieste dei clienti. Questi step intermedi sono:

- Entro 20 minuti dall'evento *disruptive*: utilizzo di router portatili per garantire connessione internet e continuare a utilizzare i pc (fissi o portatili, a seconda del fatto che sia o meno disponibile l'energia elettrica anche attraverso l'attivazione dell'UPS) per fornire supporto ai clienti;
- Entro 40 minuti dall'evento *disruptive*: raggiungimento della sede secondaria, disponibilità di collegamento internet e telefonico e di energia elettrica per alimentare i pc;
- Entro 60 minuti dall'evento *disruptive* (RTO): ripristino dell'operatività degli addetti al servizio dalla sede secondaria.

5. LIVELLI DI RECUPERO NECESSARIO PER OGNI SERVIZIO (RPO)

L'RPO, acronimo inglese di Recovery Point Objective, rappresenta la massima perdita di dati tollerata: è quindi il valore che descrive la differenza tra il momento in cui il dato viene prodotto e la sua messa in sicurezza attraverso opportune procedure di backup e/o copia sul sito di DR.

I dati prodotti dagli addetti al customer support e gestiti sono delle seguenti tipologie:

- Telefonate: il numero delle telefonate, la loro durata, l'oggetto (articolato in categorie predefinite dal cliente), la tipologia di utente (buyer/seller) vengono registrati quotidianamente dagli addetti su un file messo a disposizione da parte del cliente. Ciascun addetto salva in tempo reale il proprio file all'interno della cartella relativa alla singola giornata di lavoro contenuta sul Server.
- E-mail: sono archiviate in locale sui singoli pc degli addetti e in cloud in maniera istantanea al loro invio/ricezione. La registrazione delle mail avviene in modalità analoga a quanto sopra descritto per le telefonate sempre attraverso l'ausilio del file messo a disposizione dal cliente.
- Settimanalmente viene altresì redatto un report complessivo contenente tutti i dati relativi al supporto erogato che viene archiviato su storage.
- Altri documenti prodotti/gestiti durante lo svolgimento del servizio di customer support (così come tutti gli altri dati prodotti e gestiti dalla Società nello svolgimento di altri servizi), sono realizzati e/o archiviati operando direttamente sulle cartelle di file dello storage con back-up automatico sul cloud DropBox.

Come descritto al precedente articolo 3, il back up su storage e sul cloud avviene in tempo reale e automaticamente. Questo permette di avere dati costantemente archiviati e aggiornati sia in locale che in cloud.

6. CONDIZIONI LIMITE CHE PORTANO ALL'ATTUAZIONE DEL PIANO – SCENARI DI CRISI

Le condizioni per le quali è necessario ricorrere alla continuità operativa sono:

1. Indisponibilità della sede primaria per eventi atmosferici, allagamenti, incendi, etc.;
2. Indisponibilità della sede primaria per:
    a. Indisponibilità o assenza prolungata dell'energia elettrica;
    b. Indisponibilità o assenza prolungata della rete per il trasferimento dei dati (internet);
    c. Indisponibilità o assenza prolungata della rete per la telefonia fissa.
3. Indisponibilità di personale essenziale: Mancanza massiva di personale dovuta, a titolo esemplificativo, a epidemia influenzale o strade bloccate.
4. Perdita documentazione

Ogni dipendente che riscontri un problema e/o un disservizio che impedisca il normale svolgimento dell'attività lavorativa, sia esso logistico o informatico o legato al personale, deve informare il proprio Responsabile.

Il Responsabile valuterà la situazione sottoposta dal dipendente; nel caso in cui il problema non sia risolvibile con gli ordinari mezzi di intervento attiverà il *Comitato per la gestione delle crisi* (vedi successivo par. 8, Parte A).

In particolare, il Responsabile del Customer Support è tenuto ad utilizzare la "Tabella di classificazione degli incidenti", di cui al successivo par. 7 Parte A, per determinare il grado di severità dell'incidente ed eventualmente notificare al *Comitato per la gestione delle crisi/RCO* l'evento incidentale se ritenuto di categoria "Grave" o "Disastroso".

In base al livello di gravità delle condizioni riscontrate, si potranno/dovranno prendere le seguenti decisioni:

1. Indisponibilità della sede primaria per eventi atmosferici, allagamenti, incendi, etc. Se l'indisponibilità si protrae oltre 15 minuti, il RCO attiva le procedure transitorie di cui al precedente par. 2 e contemporaneamente attua il trasferimento nella sede secondaria con ripristino dell'operatività del servizio da questa sede.

2. Indisponibilità della sede primaria per:
   a. Indisponibilità o assenza prolungata della corrente elettrica;
   b. Indisponibilità o assenza prolungata della rete per il trasferimento dei dati (internet);
   c. Indisponibilità o assenza prolungata della rete per la telefonia fissa.

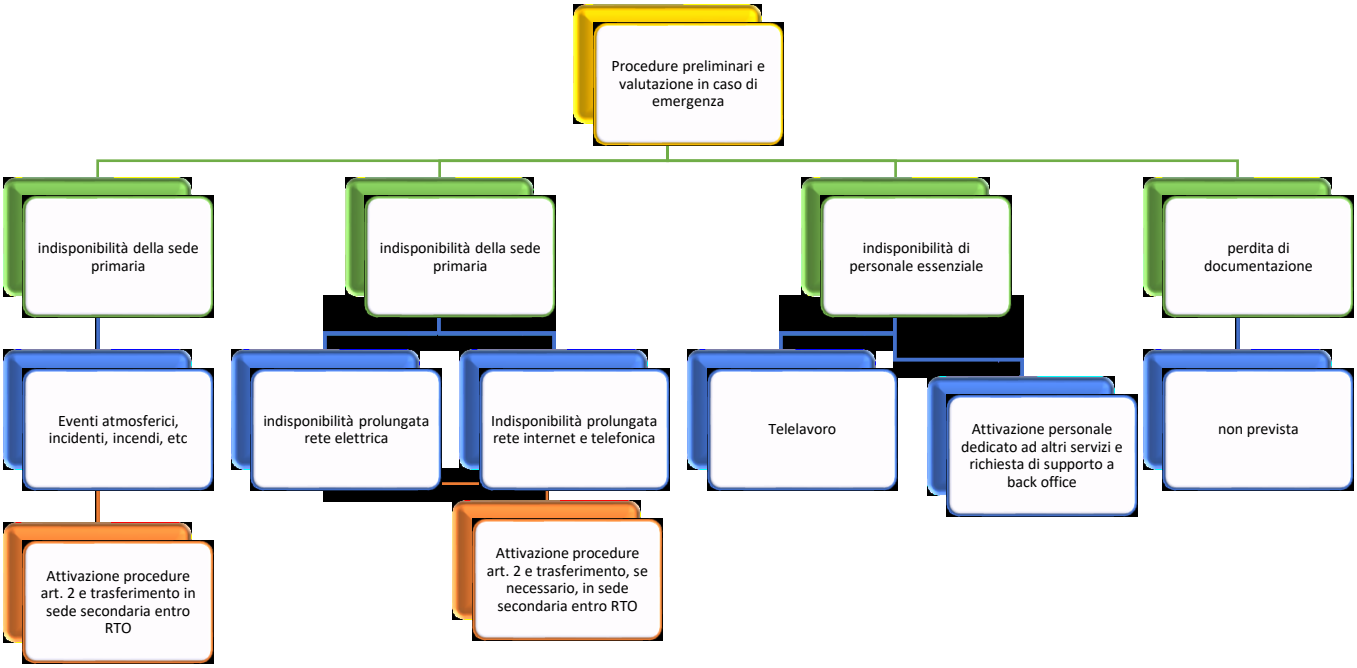
   Se l'indisponibilità si protrae oltre 15 minuti, il RCO attiva le procedure transitorie di cui al precedente par. 2 e se lo reputa necessario attua il trasferimento nella sede secondaria con ripristino dell'operatività del servizio da questa sede.

3. Indisponibilità di personale essenziale: mancanza massiva di personale. Questa è la casistica di più complessa gestione, in quanto il personale dedicato al *customer support* è specializzato per l'erogazione del suddetto servizio essendo in possesso di competenze e conoscenze specifiche. Per questa ragione, la Società ha attivato un numero di operatori del CS in numero tale da garantire la costante presenza di più addetti, ognuno con conoscenze trasversali su tutti i clienti gestiti, per garantire la sostituibilità tra gli stessi in caso di ferie, malattie, etc. Il Responsabile del Customer Support è affiancato nella sua attività da due vice-responsabili in grado di subentrare nelle funzioni del responsabile in caso di sua assenza.
   In caso di eventi eccezionali (es. pandemie influenzali, blocchi delle strade di accesso alla sede prolungati) che comportano l'assenza massiva di operatori di customer support, le contromisure che il RCO può prendere sono le seguenti:
   - *Ricorso al restante personale dipendente della Società:* questo personale per le sue caratteristiche professionali, pur non occupandosi di *customer support*, ha conoscenze in materia sia di piattaforme di e-procurement che di appalti pubblici, e può quindi supplire temporaneamente alla carenza degli addetti del *customer* fornendo un primo supporto. In seconda istanza può scalare al secondo livello di supporto;

- *Ricorso al back office del fornitore della piattaforma su cui viene erogato il servizio di customer support*.
- *Ricorso al telelavoro*: per una corretta erogazione del servizio sono sufficienti agli addetti un pc e un telefono. Molti degli addetti sono dotati di cellulare aziendale, in ogni caso tutti dispongono di un pc e di una connessione internet nella propria abitazione e sono autorizzati e istruiti, in caso di evento straordinario, a erogare il servizio con i propri mezzi e autenticarsi con le proprie credenziali ai software on line per svolgere il supporto, mantenendosi sempre in contatto con il Responsabile.

4. Perdita di documentazione: archiviando tutti i dati e i documenti in cloud, questo scenario non è ritenuto plausibile.

Di seguito viene riportato il Diagramma di Flusso che schematizza le decisioni da prendere in base alla valutazione delle condizioni della sede principale e di mancanza massiva di personale.



7. TABELLA DI CLASSIFICAZIONE DEGLI INCIDENTI

Il Responsabile del Customer Support è tenuto a utilizzare la seguente tabella per determinare il grado di severità dell'incidente ed eventualmente notificare al Responsabile della Continuità operativa o al Comitato Gestione Crisi l'evento incidentale se ritenuto di categoria "Grave" o "Disastroso", come meglio descritto nella seguente tabella.

Livello	Classe incidente	Descrizione	Responsabilità

1	ORDINARIO	L'incidente non provoca disservizi significativi e l'impatto sull'operatività della Società non è rilevante. L'evento è risolvibile con mezzi di intervento ordinari	Responsabile del servizio o suo delegato
2	SIGNIFICATIVO	Degrado o interruzione di una percentuale minoritaria (< 25%) del servizio per cui lo stesso continua ad essere erogato anche se in modalità rallentata	Responsabile del servizio o suo Delegato
3	GRAVE	Degrado o interruzione di una percentuale da media a elevata (26% < x < 55%) del servizio per cui lo stesso continua ad essere erogato ma causando gravi disservizi	A cura del responsabile della Continuità Operativa
4	DISASTROSO	Incidente che causa l'interruzione di una percentuale da elevata a completa del servizio (56% < x < 100%)	Comitato di Crisi

8. MODALITA' DI ATTIVAZIONE, GESTIONE E MANUTENZIONE del BCP

La dichiarazione dello stato di crisi e l'attivazione del presente Piano di BC è compito del Responsabile della Continuità Operativa, che assicura anche la gestione delle fasi successive di recovery descritte nei capitoli a seguire.

Le modalità per cui si deve attivare il piano di continuità operativa sono regolamentate in questa sezione. Vengono di seguito elencati i casi limite in cui deve essere attivato il piano in modo che i dipendenti della Società e le figure facenti parte del Comitato di Gestione Crisi sappiano valutare immediatamente il livello del disservizio.

Risulta infatti decisiva la corretta valutazione della gravità dell'evento in modo da attuare subito il piano idoneo ad arginare l'emergenza.

A tal proposito tutti i dipendenti della Società, le figure del Comitato di Gestione Crisi e i fornitori con cui la Società ha stipulato contratti di assistenza hardware e software, hanno conoscenza del Piano BC e il Piano di DR.

Il piano include:

1. Modalità di mobilitazione delle persone interessate;
2. Punti di ritrovo;
3. Circostanze in cui l'organizzazione ritiene che l'attivazione del BCP non sia necessaria;
4. Modalità di gestione, manutenzione, verifica e test del BCP;
5. Piano di Disaster Recovery;
6. Modalità di rientro dall'emergenza.

I punti sopra elencati sono sviluppati nei prossimi paragrafi.

8.1 Modalità di mobilitazione delle persone interessate

I componenti del Comitato di Gestione Crisi e le altre figure interessate nell'attivazione del Piano di Continuità Operativa e di Disaster Recovery, interni ed esterni alla Società, devono essere contattati attraverso i riferimenti riportati al successivo articolo 4, parte B.

Di seguito si riporta la tabella con ruoli e responsabilità del team di ripristino della BC:

FASE	ATTIVITA'	RESPONSABILE	DOCUMENTO DI RIFERIMENTO	COMPOSIZIONE DEL TEAM
Fase di recovery	Attivazione dei piani	Comitato di gestione crisi	Piano di Continuità Operativa	Comitato di gestione crisi
	Supervisione, supporto e coordinamento delle operazioni di ripristino	Responsabile Continuità Operativa	Piano di Continuità Operativa	Responsabile Continuità Operativa e Responsabile Servizi telematici
	Coordinamento delle operazioni di recovery dei processi	Servizi telematici e Responsabile Customer Support	Piano di Disaster Recovery	Responsabile Servizi telematici, Responsabile Customer Support, assistenza hardware e software
	Coordinamento delle operazioni di recovery delle tecnologie (applicazioni e sistemi)	Responsabile servizi telematici	Piano di Disaster Recovery	Responsabile Servizi telematici, assistenza hardware e software
Gestione presso sede secondaria	Gestione dei servizi critici ristabiliti presso la sede di DR	Responsabile Continuità Operativa e Customer Support	Piano di Continuità Operativa	Responsabile Servizi telematici, Responsabile Customer Support, assistenza hardware e software

Rientro e chiusura della crisi	Ordine di rientro alla sede primaria	Comitato di gestione crisi	Piano di Continuità Operativa	Comitato di gestione crisi
	Coordinamento delle operazioni di rientro del servizio	Responsabile Continuità Operativa	Piano di Disaster Recovery	Responsabile Continuità Operativa e Responsabile servizi telematici
	Coordinamento delle operazioni di rientro alle postazioni di lavoro abituali	Responsabile servizi telematici e Responsabile Customer Support	Piano di Disaster Recovery	Responsabile Continuità Operativa e Responsabile servizi telematici, assistenza hardware e software

8.2 Punti di ritrovo

Il punto di ritrovo principale è la sede primaria sita in Via Sandro Pertini 5, loc. Antella, Bagno a Ripoli (FI).
Nel caso in cui non sia possibile operare presso il sito primario, il Comitato di Gestione Crisi dichiarerà e organizzerà lo spostamento del personale e delle infrastrutture trasportabili presso la sede secondaria, sita in Via Chiantigiana 103-103/a, Bagno a Ripoli (FI).

8.3 Circostanze in cui l'organizzazione ritiene che l'attivazione del BCP non sia necessaria

Nei casi in cui l'interruzione parziale e temporanea del servizio non comporti perdite di dati o disservizi rilevanti (vedi Tabella di classificazione degli incidenti) non sarà necessario attivare il Piano di Continuità Operativa.

8.4 Modalità di gestione, manutenzione, verifica e test del Piano BC e DR

Il Piano BC e DR sarà aggiornato periodicamente secondo necessità (a titolo esemplificativo e non esaustivo: modifica delle condizioni di erogazione del servizio, etc.) e sottoposto ad approvazione da parte del Comitato di Gestione Crisi nel corso delle riunioni periodiche indette dal Responsabile della Continuità Operativa.
In ogni caso, il Piano di Continuità Operativa dovrà essere aggiornato almeno una volta ogni due anni e dovrà essere vagliato ed approvato dal Comitato di Gestione Crisi.

Sulla base dei dati raccolti durante i test, previsti al successivo par. 9, Parte B, il Comitato di Gestione Crisi valuta il Piano e ne dichiara la conformità o procede ad aggiornarlo, dandone evidenza nella Tabella delle revisioni e notificandolo a tutte le figure interessate nelle procedure di BC e di DR.

Qualsiasi modifica apportata al Piano di Continuità Operativa e/o al Piano di Disaster Recovery costituisce revisione del Piano stesso e pertanto deve essere approvata ed archiviata. Ciascuna versione del Piano dovrà avere un numero identificativo della data e della versione del piano.

Le copia del Piano di Continuità Operativa e del Piano di Disaster Recovery della Società, costantemente aggiornati, saranno depositate presso gli uffici della Società, oltre che salvate in maniera digitale sullo storage e notificate alle figure coinvolte nei piani stessi ad opera del Responsabile della CO.

Il Responsabile della CO:

- aggiorna periodicamente il Comitato di Gestione Crisi sullo stato complessivo delle operazioni di recovery e ripristino del servizio.
- è tenuto a verificare l'aggiornamento periodico dei piani e degli allegati, la formazione del personale citato nei documenti, test ed esercitazioni.
- Verifica che il Responsabile dei servizi telematici abbia provveduto ai controlli sulla funzionalità e aggiornamento di tutte le TLC e della strumentazione informatica utilizzata per erogare il servizio.

Il Servizio di assistenza software e quello di assistenza hardware e TLC sono tenuti a segnalare preventivamente al RCO e al Responsabile dei servizi telematici ogni cambiamento tecnologico che possa rendere inapplicabile il presente documento, in modo da consentire di modificare i piani e le soluzioni tecnologiche ivi contenute.

8.5 Piano di Disaster Recovery (PDR)

Il PDR è contenuto all'interno del presente Piano di Continuità operativa e ne costituisce la Parte B.

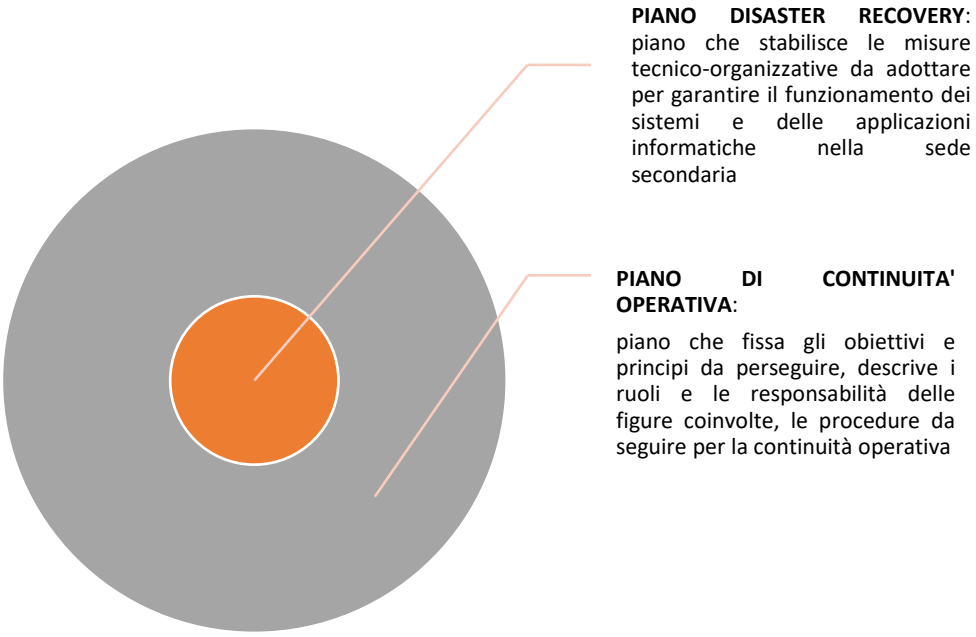
8.6 Modalità di rientro dall'emergenza

Il ritorno allo svolgimento della normale attività lavorativa è la condizione in cui non risulta necessario prolungare l'adozione del Piano e di conseguenza la fine dell'emergenza. Il rientro dall'emergenza è deciso dal Comitato di Gestione Crisi che si riunisce per la valutazione del disastro, per la dichiarazione dell'emergenza, per prendere le decisioni durante tutto l'arco temporale della stessa e al termine della stessa per decidere sul rientro, dopo aver valutato le condizioni di ripristino del servizio.

La dichiarazione di rientro dall'emergenza viene effettuata nel momento in cui l'erogazione del servizio raggiunga nuovamente la piena operatività con il conseguente rientro alla sede principale.

PARTE B - PIANO DI DISASTER RECOVERY

Il Piano di Disaster Recovery, che fa parte integrante del BCP, è l'insieme delle azioni e dei sistemi con i quali la Società provvede al ripristino delle funzionalità tecnologiche e organizzative della propria struttura. Esso contiene la descrizione delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione del servizio di customer support a fronte di gravi emergenze che ne intacchino la regolare attività.



Oltre alle modalità di archiviazione dei suddetti dati anche in locale (come descritto al precedente articolo 3, parte A), questi sono replicati/contenuti anche in soluzioni di cloud computing che garantiscono, in proprio, la conservazione e il ripristino dei dati. Sono quindi esclusi dalla procedura interna di disaster recovery.

1. FINALITÀ E CONTENUTI DEL PIANO DI DISASTER RECOVERY

Il Piano di Disaster Recovery, ha la funzione di spiegare nel dettaglio le fasi necessarie per il ripristino delle risorse hardware e software utilizzate per l'erogazione del servizio da parte degli operatori del customer support.

Nel piano di DR vengono altresì dettagliate le procedure operative necessarie per effettuare una corretta valutazione della situazione di emergenza/disastro che non consenta la normale erogazione

dei servizi da parte della Società. Nel presente documento vengono inoltre descritte le varie fasi per provvedere al ripristino del sistema di telecomunicazione, ovvero del recupero dei dati e la configurazione delle procedure per arginare l'emergenza e avviare il successivo rientro alle normali condizioni operative. Sono inoltre descritte le procedure per l'attivazione del sito di DR (sede secondaria) nel caso non sia accessibile e utilizzabile il sito primario.

La Società ha anche provveduto all'analisi delle minacce possibili e dei relativi rischi che possono derivare sia da una non corretta gestione dell'infrastruttura informatica, sia dall'integrità delle apparecchiature elettroniche e informatiche. La sicurezza e l'integrità dei dati, in termini di protezione degli stessi da varie tipologie di cause, esterne e interne alla Società, permette di raggiungere livelli di sicurezza che garantiscono una drastica diminuzione delle probabilità di rischio.

L'integrità fisica dei sistemi informatici e di telecomunicazione, dettagliata nei paragrafi successivi, può infatti essere intaccata o distrutta da:

- calamità naturali (alluvioni, terremoti, fulmini, etc.)
- cause accidentali (incidenti, allagamenti, distruzione dell'edificio, distruzione di personal computer, server o altri elaboratori elettronici in cui siano custoditi i dati trattati)
- cause esterne (sommosse, rivolte, devastazioni, atti vandalici, eventi socio-politici, furti)

L'integrità fisica delle infrastrutture, dettagliata nei paragrafi successivi, necessaria per il funzionamento dei sistemi e per poter consentire una normale attività lavorativa agli operatori della Società, deve essere assicurata dalla continua presenza dell'elettricità nello stabile. Per sopperire a mancanze temporanee di energia elettrica e cali di tensione, è prevista la disponibilità di Dispositivi UPS (Gruppi di Continuità), in grado di subentrare in caso di guasti di varia natura, che garantiscono un'autonomia operativa di 30 minuti, come specificato al precedente articolo 2, parte A.

L'integrità fisica delle infrastrutture è altresì garantita dal fatto che le sedi della società (sia primaria che secondaria), sotto il profilo prevenzionistico, sono conformi alle vigenti disposizioni in materia di igiene e sicurezza sul lavoro (D.Lgs. 81/2008) e di prevenzione incendi (DPR 157/2011 – D.M. 10/03/98).

L'integrità dei dati, indispensabile per lo svolgimento del servizio, deve sempre essere garantita e potrebbe essere compromessa da semplici errori umani del personale, da guasti dell'hardware, dal non funzionamento della connessione internet, da furto di dati o di credenziali di accesso al sistema, da azioni di *hacking*.

Per limitare la perdita dei dati o l'alterazione degli stessi è necessario predisporre minimi livelli di sicurezza e garantire un corretto e costante backup dei dati trattati, come meglio dettagliato nel paragrafo rubricato "Politiche di sicurezza e salvaguardia dei dati".

2. DESCRIZIONE DELLA SOLUZIONE DI DISASTER RECOVERY

In questa sezione viene descritta la soluzione di disaster recovery adottata dalla Società per assicurare la continuità di funzionamento del sistema informatico e telematico a fronte di eventi dannosi che comportino un'indisponibilità del servizio oltre la soglia di tolleranza indicata al precedente par. 7, Parte A.

La scelta di dotarsi di un sito di DR su "Cloud", è stata dettata da condizioni operative che permettono di sfruttare una soluzione con rapporto costi/benefici ottimali, tenendo conto dei seguenti elementi:

- Volume medio-basso di dati da mantenere sul sito Cloud
- Variazione giornaliera dei dati che permette la trasmissione attraverso le linee internet a disposizione della Società

In merito al Disaster Recovery, la soluzione "Cloud Computing" è stata adottata per le seguenti attività:

- Posta elettronica Outlook: la nostra Società ha attivato delle licenze Microsoft per i propri dipendenti, che comprendono anche la posta elettronica Outlook. La posta è installata su tutti i pc dei dipendenti della Società. La posta è costantemente aggiornata e archiviata on line sul cloud Microsoft e consultabile da internet, accedendo con le credenziali dei vari profili.
- Dropbox: i dati archiviati nello storage sono costantemente sincronizzati con DropBox, su cui disponiamo di uno spazio di archiviazione di 1TB. Lo spazio è ampiamente sufficiente per le nostre esigenze ma, nel caso in cui risulti necessario ampliarlo, sarà acquistato ulteriore spazio necessario per garantire il back-up in cloud di tutti i dati gestiti dalla Società (sia per il servizio di customer support che per gli altri erogati). DropBox consente il recupero dei file entro 30 giorni (cioè la possibilità recuperare file precedenti entro 30 giorni) e di avere più utenze collegate alla Società.

I piani DR dei software attivati con licenza Microsoft e di Dropbox sono ritenuti pienamente idonei e in linea con il presente Piano al fine di garantire la continuità operativa del servizio.

Per quanto riguarda invece i programmi utilizzati per erogare il servizio di customer support (es. software per il tracking delle segnalazioni, software per il recupero delle password degli utenti iscritti, etc.) e le piattaforme telematiche interessate dal servizio, sono raggiungibili on-line, essendo applicazioni che lavorano su internet il cui accesso è regolato tramite utilizzo di credenziali che ci sono state rilasciate dai proprietari dei programmi/piattaforme. Anche per i dati gestiti sui suddetti programmi e piattaforme, l'attività di disaster recovery è garantita dalle aziende proprietarie e/o fornitrici dei servizi.
Nel caso in cui le piattaforme telematiche messe a disposizione dal cliente per erogare il servizio subiscano dei malfunzionamenti o dei rallentamenti questi influiranno direttamente sulla capacità di PA&M di erogare correttamente il servizio di CS. Il RCO comunicherà tempestivamente al cliente, con le modalità di cui al punto 4.1 del piano di DR, la necessità di rimessa in pristino delle suddette piattaforme affinché venga garantita la continuità operativa del servizio e si informerà altresì delle

tempistiche di risoluzione nonché delle eventuali modalità alternative per erogare il servizio agli utenti.

La criticità legata al piano di Disaster Recovery della Società è quindi basato prevalentemente sulla disponibilità e qualità del collegamento internet per accedere agli archivi/software di tipo cloud e di quello telefonico.

Per questa ragione, la Società:

- per garantire e migliorare il proprio sistema informatico, ha provveduto a stipulare un contratto di manutenzione e assistenza tecnica software con la ditta ABC Technology S.n.c. che prevede un supporto sia programmato che on demand che garantisce un intervento in caso di evento bloccante entro 2 ore lavorative dalla richiesta, tramite e-mail, telefono e/o con la presenza in loco dei propri tecnici qualora la problematica non sia risolvibile da remoto.
- ha attivato un contratto di assistenza tecnica per la parte hardware degli apparati di telecomunicazione, con la ditta Teleinformatica Italiana di Leonardo Pieri che garantisce il ripristino dell'efficienza dei sistemi con tempistiche di intervento di due ore lavorative dalla richiesta, in caso di guasto di tipo bloccante, sia con interventi da remoto che on-site dei propri tecnici qualora necessario.

L'attivazione del piano di DR consiste quindi nel ripristinare l'accesso a internet e alla linea telefonica, condizioni necessarie per l'erogazione del servizio di *customer support* che sarà comunque garantito anche in caso di non fruibilità della linea fissa, nelle modalità indicate al precedente articolo 2, parte A.

3. PERIMETRO DI RIFERIMENTO DEL PIANO

3.1 Descrizione del sistema informativo primario

La Società ha una sede primaria, sita in Via Sandro Pertini 5, Bagno a Ripoli (FI) e una secondaria sita in Via Chiantigiana 103-103/a, Bagno a Ripoli (FI).

La Società possiede un proprio sistema informativo, ubicato all'interno della sede principale, costituito da: storage, router, computer, centralino, canali fonia e dati, telefoni VOIP.

Tutti i pc dei dipendenti della Società possiedono un sistema antivirus e firewall software.

La società si è dotata di un firewall hardware.

3.2 Fattori critici e di rischio, descrizione dei casi di disastro/indisponibilità prolungata che si intendono affrontare con la soluzione di DR

3.2.1 Fattori critici e di rischio: elenco dei possibili rischi

In questa sezione vengono dettagliati i rischi possibili e probabili a cui possono essere sottoposte le infrastrutture, fisiche e tecnologiche della Società, e i dati trattati.
Per i dati trattati devono essere garantite le seguenti qualità fondamentali:
a) la **disponibilità:** assicura che l'accesso ai dati sia disponibile quando necessario. Per garantire questo, l'accesso alle informazioni o alle risorse informatiche è negato a chi non possiede l'autorizzazione;
b) l'**integrità:** garantisce l'accuratezza e completezza dei dati e delle informazioni custodite all'interno degli hardware ovvero nello storage. Per garantire questa "qualità" si rende necessario codificare ed adottare delle corrette procedure per il backup dei dati e nel contempo evitare che le informazioni correttamente salvate possano formare oggetto di modifica o di accesso senza autorizzazione;
c) la **riservatezza:** garantisce che i dati e le informazioni siano conosciute e accessibili solo ed esclusivamente al personale autorizzato. Il rispetto della citata "qualità" si ottiene negando l'accesso alle informazioni a tutti i soggetti, interni ovvero esterni alla Società, che non siano legittimati al trattamento e alla conoscenza degli stessi dati.
Per garantire il rispetto di queste qualità è necessario conoscere ed analizzare le minacce che potrebbero incidere sulle stesse.

Analisi di dettaglio degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali trattati

Gli eventi in grado di determinare dei danni e, conseguentemente, in grado di rappresentare un rischio per la sicurezza dei dati trattati dall'Ente, possono essere ricondotti a 3 macro-categorie:

A. EVENTI RICONDUCIBILI AL COMPORTAMENTO UMANO
B. EVENTI RICONDUCIBILI AGLI STRUMENTI INFORMATICI
C. EVENTI RICONDUCIBILI AL CONTESTO FISICO-AMBIENTALE-INFRASTRUTTURALE

A. EVENTI RICONDUCIBILI AL COMPORTAMENTO UMANO

A.01 Accesso non autorizzato ai dati personali trattati mediante il cosiddetto "impersonamento informatico".

Nelle ipotesi di accesso non autorizzato ai dati personali trattati dalla Società mediante "impersonamento Informatico", un soggetto non autorizzato (interno o esterno alla Società stessa), può accedere ai dati con le credenziali di autenticazione attribuite all'incaricato legittimato all'accesso, sostituendosi in tutto e per tutto al soggetto titolare delle stesse.
La concreta possibilità che si verifichi un'ipotesi di accesso non autorizzato a dati trattati su supporto informatico si può avvenire nelle seguenti situazioni:

I. distrazione o negligenza di un incaricato del servizio di customer support il quale, per esempio, lascia incustodita la propria postazione di lavoro collegata ovvero non custodisce diligentemente le proprie credenziali di autenticazione
II. scambio delle Password tra gli Incaricati
III. carenza nel sistema e nelle procedure di attribuzione e gestione dei profili di autenticazione e di autorizzazione degli utenti.

L'accesso non autorizzato ai dati trattati dalla Società espone a ulteriori rischi di modifica non autorizzata, di danneggiamento, di mancanza di congruità, di perdita e di esportazione illegittima dei dati stessi.

Per ridurre i suddetti rischi, la Società:

- In riferimento al punto I) e II), ha sensibilizzato i propri operatori, con appositi ordini di servizio, oltre che con la diffusione del proprio codice disciplinare interno, a custodire e non diffondere le proprie credenziali di accesso sia ai computer che agli applicativi utilizzati, oltre che a non lasciare incustodita la propria postazione di lavoro se prima non ha provveduto alla disconnessione della propria utenza.
- In riferimento al punto III), sono stati creati gruppi di utenza abilitati alle singole aree informatiche/di archiviazione di competenza. Per quanto riguarda l'accesso ai software per erogare il servizio di customer support e alle piattaforme telematiche oggetto del servizio di supporto, le password sono state rilasciate dai proprietari e/o gestori delle stesse, devono contenere caratteri alfanumerici e speciali e devono essere aggiornate periodicamente.

A.02 Insufficiente conoscenza del sistema informatico o dell'applicazione

In alcuni casi, l'operatore può involontariamente compiere azioni che causano un danno semplicemente perché non è perfettamente a conoscenza delle conseguenze del suo operato a causa di una non perfetta conoscenza del sistema, dello strumento informatico ovvero dell'applicazione.
Il danno che può essere provocato varia a seconda del comportamento posto in essere e può determinare:
i. Un blocco momentaneo della stazione di lavoro
ii. Un blocco che può coinvolgere anche altri utenti della Rete
iii. L'inserimento, la modifica o la cancellazione (e dunque la perdita) non voluta di informazioni e dati
iv. L'invio di dati a soggetti non autorizzati
v. La visione di dati a soggetti non autorizzati

Questa casistica è alquanto improbabile dal momento che gli operatori del customer support sono specializzati nello svolgimento della suddetta attività. I nuovi operatori sono adeguatamente formati e affiancati da operatori esperti. Sono inoltre coordinati da un Responsabile che interviene in caso di necessità. In occasione del rilascio di nuove funzionalità delle piattaforme, gli operatori del customer support possono contattare direttamente il back office del fornitore della piattaforma stessa per avere indicazioni su come utilizzare le nuove funzionalità in questione.

A.03 Insufficiente conoscenza dei rischi e delle misure di sicurezza

Una non puntuale conoscenza dei gravi rischi che possono determinarsi quale conseguenza di una condotta non improntata al rispetto delle norme tecniche dettate dal D.Lgs. 196/03 e dal Regolamento UE 2016/679 può comportare i seguenti rischi:
i. La diffusione nell'ambito dell'Ufficio, tra colleghi, delle credenziali di accesso
ii. La negligente custodia delle credenziali di autenticazione da parte del singolo operatore

iii. La circostanza che venga lasciata la propria stazione di lavoro accesa e collegata quando ci si allontana per qualsiasi ragione
iv. La circostanza che vengano lasciate, liberamente fruibili, stampe e tabulati contenenti dati riservati

Il danno che può essere determinato nelle ipotesi considerate è quello di accesso non autorizzato ai dati trattati, di modifica e di esportazione illegittima degli stessi e, nei casi più gravi, di distruzione.

In merito a tale comportamento la Società ha sensibilizzato i propri operatori, con appositi ordini di servizio oltre che con la diffusione del proprio codice disciplinare interno, a custodire e non diffondere le proprie credenziali di accesso sia ai computer che agli applicativi utilizzati, oltre che a non lasciare incustodita la propria postazione di lavoro se prima non ha provveduto a scollegare la propria utenza. Per maggiore sicurezza ogni pc richiede la password di accesso dopo 15 minuti di inattività.

A.04 Distrazione e Negligenza
La distrazione e la negligenza possono essere di tipo "fisico" o "logico".
La distrazione/negligenza di tipo *fisico*, in genere, comporta direttamente danni alla strumentazione e alle attrezzature (es. rottura, danneggiamento, etc.) e, in alcuni casi, causa indirettamente danni ai dati.

La distrazione/negligenza di tipo *logico* invece, determina in genere esclusivamente danni ai dati trattati (a titolo esemplificativo e non esaustivo: durante la sessione di lavoro l'operatore viene distratto e dimentica di salvare il documento su cui stava lavorando, preme inavvertitamente dei tasti che provocano l'esecuzione di un comando non voluto, stacca inavvertitamente il cavo del pc, versa acqua inavvertitamente sul pc, ecc).
Il danno che tale evento può determinare è quello di alterazione, corruzione, cancellazione e, nei casi più gravi, perdita dei dati.

In merito a tale evenienza, la Società cerca di garantire un ambiente lavorativo ordinato (per ridurre il rischio fisico) e tranquillo, evitando il coinvolgimento degli operatori di customer support in attività diverse da quelle che stanno svolgendo (per limitare il rischio logico).

A.05 Atto doloso
È senza dubbio il più grave e pericoloso degli eventi dannosi legati al fattore umano in quanto presuppone una precisa volontà indirizzata alla manomissione ovvero alla distruzione delle strumentazioni o dei dati trattati.
Potrebbe verificarsi che, con comportamento consapevole, derivante potenzialmente da vari fattori (es. risentimento verso la Società o perseguimento di fini personali), gli operatori del *customer support* compiano operazioni illecite durante l'erogazione del servizio.

Per ridurre questa tipologia di rischio, la Società si impegna a mantenere con tutti i propri dipendenti un rapporto di leale collaborazione, garantendo il rispetto dei diritti dei lavoratori e il mantenimento di un ambiente di lavoro sereno.

B. EVENTI RICONDUCIBILI AGLI STRUMENTI INFORMATICI

B.01 Azione di Virus Informatici ovvero di programmi suscettibili di recare danno

Esistono dei virus informatici programmati per cancellare o danneggiare i dati, o per causare la paralisi dei servizi erogati mediante gli strumenti informatici.
L'azione di questi agenti dannosi è generalmente innescata dal download di programmi di varia natura che vengono diffusi per posta elettronica sotto forma di allegati, oppure provengono da siti che, ingannando l'utente, lo inducono a salvare questi file sulla propria postazione di lavoro.

In merito a tale minaccia la Società ha impostato un sistema di antivirus e di firewall software per ogni pc. È stato anche attivato un firewall hardware.

B.02 Spamming o tecniche di sabotaggio

In riferimento ad azioni di sabotaggio compiute da terzi tramite programmi che sfruttando difetti del software utilizzato per la gestione della posta elettronica o di altri servizi informatici e saturano il servizio di richieste fino alla paralisi parziale o totale dello stesso. Questa azione determina l'indisponibilità temporanea dei dati gestiti dal servizio che forma oggetto di attacco.
In merito a tale minaccia la Società si avvale del Filtro Antispam del Client di posta elettronica e della protezione del Firewall hardware centrale.

B.03 Obsolescenza degli strumenti Hardware

L'obsolescenza delle attrezzature, che nel campo informatico è particolarmente rapida, oltre a rappresentare un fattore di rischio "attivo", può impedire l'attivazione e l'implementazione di misure di sicurezza fisiche o logiche che si rendano opportune per eliminare o ridurre alcuni rischi.
L'esempio che può essere fatto è quello che si riferisce all'impossibilità tecnica di installare su un vecchio pc un sistema di cifratura dei dati che richiede processori di una certa potenza e sufficiente memoria.

In merito al suddetto rischio, la Società, anche grazie agli incaricati dell'assistenza informatica e a quelli sugli apparecchi di telecomunicazione, provvede a monitorare il grado di obsolescenza delle proprie apparecchiature informatiche e a sostituirle con versioni più recenti in caso di necessità.

B.04 Malfunzionamento/indisponibilità degli strumenti Hardware

Come tutte le macchine, anche le strumentazioni informatiche sono soggette ad avarie che possono renderle inutilizzabili per periodi più o meno lunghi.
A seconda del tipo di guasto si può avere solo il blocco dell'attività della postazione di lavoro oppure anche il danneggiamento o la perdita dei dati (si pensi al caso di avaria che interessi l'hard disk).

Per far fronte a questa evenienza, la Società ha stipulato i contratti di assistenza con interventi "on demand" come specificato al precedente articolo 2, parte B.

B.05 Malfunzionamento Software e obsolescenza derivante da mancato aggiornamento

In questo punto si fa riferimento alla possibilità, insita in ogni software, di rivelare difetti di funzionamento inizialmente non presenti o non evidenti. Tale possibilità esiste sempre in quanto ogni programma dipende da altri prodotti software (primo fra tutti il sistema operativo) e hardware (le apparecchiature di rete) che devono essere sostituiti o aggiornati nel tempo. Il risultato di tale evento può essere l'indisponibilità temporanea o addirittura permanente di dati nel caso più grave, in cui cioè non sia più possibile ristabilire la situazione originaria.

Anche per tale evento sono stati stipulati opportuni contratti di Aggiornamento Software con le aziende produttrici o intermediarie.

B.06 Accessi esterni non autorizzati

Questo è il caso in cui vi siano intrusioni via rete, avvenute senza furto di credenziali di autenticazione ma semplicemente mediante lo sfruttamento di difetti del software, per effettuare accessi non autorizzati ai dati.

Ogni pc è dotato di un firewall software. È stato anche installato un firewall hardware centralizzato di alta affidabilità che oltre ad impedire accessi dall'esterno ne traccia anche i tentativi. In ogni caso l'azienda si è dotata di norme di comportamento in caso di rilevamento di *data breach*.

C. EVENTI RICONDUCIBILI AL CONTESTO FISICO-AMBIENTALE-INFRASTRUTTURALE

C.01 Ingressi non autorizzati ad aree/locali ad accesso ristretto

In questo caso viene in rilievo la concreta possibilità che soggetti non legittimati possano materialmente introdursi all'interno dei locali e degli Uffici in cui sono posizionati gli apparati e gli elaboratori informatici ospitanti i dati gestiti per l'erogazione del servizio. In casi di questo tipo, il danno che può derivare non è solo quello, di per sé già molto grave, di accesso di soggetto non autorizzato alle banche dati trattate dagli operatori, ma si possono verificare anche ipotesi di modifica, di distruzione e conseguente perdita, di esportazione illegittima delle Banche Dati oggetto dell'evento dannoso considerato.

In relazione a tale possibilità la Società ha provveduto alla protezione dei locali con apposite serrature le cui chiavi di accesso sono consegnate solo al personale dipendente È altresì presente un sistema di allarme con sensori di movimento presenti in ogni stanza e agli accessi con batterie tampone della durata di 24 ore.

C.02 Sottrazione/Furto di strumenti contenenti dati personali

Ci si riferisce all'ipotesi di furto di una postazione di lavoro (workstation) ovvero di uno *storage* con conseguente perdita di tutti i dati ospitati nello strumento informatico oggetto di sottrazione.
Nell'ipotesi considerata, il danno provocato deriva da un soggetto non legittimato che accede alle banche dati ospitate all'interno dello strumento informatico con la conseguenza che la Società perda la disponibilità delle stesse.

In relazione a tale possibilità la Società ha provveduto alla protezione dei locali con apposite serrature le cui chiavi di accesso sono consegnate solo al personale dipendente. È altresì presente un sistema di allarme con sensori di movimento presenti in ogni stanza e agli accessi con batterie tampone della durata di 24 ore.
Si sottolinea inoltre che tutti i dati gestiti sono costantemente archiviati su storage che effettua una sincronizzazione automatica su cloud, quindi il furto del supporto hardware non comporta la perdita dei dati che possono sempre essere recuperati sull'archivio on-line.

C.03 Guasto a sistemi complementari (Impianto elettrico)
Ci si riferisce a tutti quegli eventi che riguardano sistemi e impianti esterni ma complementari agli strumenti informatici e che vanno ad impattare sugli stessi inficiandone la funzionalità. Il tipico esempio di guasto a sistema complementare è quello che riguarda l'impianto elettrico.
Il rischio correlato a tale tipologia di evento è quello di danneggiamento dei dati e di indisponibilità temporanea, ovvero nei casi più gravi, permanente degli stessi.

In relazione a tali guasti la Società è dotata di un sistema di UPS (Gruppi di Continuità) per poter continuare transitoriamente il lavoro durante l'eventuale Black-out e attivare il piano di CO, come specificato al precedente articolo 2, parte A.

C.04 Eventi distruttivi, naturali o artificiali accidentali o dovuti ad incuria
Include tutti gli eventi di effetto distruttivo sui supporti fisici contenenti i dati o sulle apparecchiature informatiche, indipendentemente dalla loro natura, qualora non siano già inclusi nelle casistiche precedenti.
Il rischio che si può determinare sui dati è quello di danneggiamento, indisponibilità temporanea o perdita parziale o totale degli stessi.
Gli eventi in questione comprendono:

- Incendio parziale o diffuso
- Scariche atmosferiche
- Allagamenti
- Condizioni ambientali estreme

Fermo restando il fatto che le sedi della Società sono in regola con le normative antincendio e con quelle sulla sicurezza nei luoghi di lavoro, qualora si verifichino eventi che danneggino i supporti fisici di archiviazione questo non comporta la perdita dei dati in essi contenuti in quanto sono sincronizzati automaticamente con uno storage di tipo cloud.

C.05 Errori umani nella gestione della sicurezza fisica
Ci si riferisce a ogni evento determinato da un errore umano nella gestione della sicurezza negli ambienti fisici ospitanti gli apparati e gli strumenti informatici. In questa categoria sono ricomprese, a mero titolo esemplificativo, sia le ipotesi di non cura delle basilari norme di comportamento atte a

garantire il non accesso di personale non autorizzato. Il rischio correlato a tale tipologia di evento va dall'accesso non autorizzato ai dati fino alla perdita e alla distruzione degli stessi.

Per ridurre questa tipologia di rischio, la Società sensibilizza periodicamente i propri dipendenti nell'osservanza delle regole di normale diligenza da utilizzare per garantire il corretto accesso ai locali.

3.3.2 Sicurezza Informatica

L'accesso al sistema informatico della Società e alle caselle di posta elettronica viene garantito attraverso la fornitura di apposite credenziali costituite da un codice identificativo (User ID) e da una password personali, attribuite in via esclusiva a ciascun dipendente e aggiornate ogni tre mesi a seguito di un'impostazione automatica; lo storage conserva tutte le informazioni sulle utenze e sui permessi di accesso alle risorse disponibili.
Ogni utente risulta inserito in un Gruppo (relativo all'attività di propria competenza) al fine di avere accesso a una serie di dati e cartelle riservate.
La Società ha quindi provveduto ad attribuire a tutti i dipendenti, ciascuno per le attività di propria competenza, una credenziale di autenticazione costituita da una User-Id e da una Password.
La forma di protezione adottata per contrastare gli eventuali sbalzi di tensione elettrica, come già menzionato al precedente par. 3, Parte A, è rappresentata da gruppi di continuità collegati, in locale, ai computer della Società, allo storage e agli apparati di rete.

Come già anticipato nella sezione corrispondente, per la protezione da software dannosi, virus e malware, intrusioni dall'esterno, oltre all'installazione di antivirus e firewall software in tutti i Client di Rete (protezione locale), è stato installato un Firewall hardware centrale.

3.3.3 Descrizione dei casi di disastro/indisponibilità.

Casi in cui sarà attivata la soluzione di DR, rischi considerati:

- Mancanza di erogazione del servizio dovuta all'impossibilità di accedere ai dati e alle banche dati;
- Distruzione delle infrastrutture IT;
- Impossibilità di accedere ai locali destinati nei quali sono stati collocati: storage, apparati di rete e di backup;
- Indisponibilità dei servizi pubblici (esempio: rete elettrica, rete fonia, internet etc.).

4. ORGANIZZAZIONE E PERSONALE

Organizzazione, ruoli e responsabilità, strutture e personale coinvolto nelle attività

In questa sezione vengono elencate tutte le persone e le figure con i relativi incarichi, dati anagrafici e contatti per le comunicazioni, che sono coinvolte nella gestione dell'emergenza e della soluzione di DR, comprensivo delle figure facenti parte del Comitato di Gestione Crisi.
Viene inoltre descritta la struttura di riferimento per la gestione della soluzione di DR con i rispettivi compiti e competenze.

Responsabile Continuità Operativa: provvede a contattare tutte le figure del Comitato di Gestione Crisi con i contatti indicati nella tabella sottostante. Provvede a redigere, qualora fosse richiesta, la relazione da inviare al cliente coinvolto nell'evento dannoso nei casi in cui sopraggiunga un disastro e sia necessario attivare la continuità operativa e il disaster recovery.
Responsabile Customer Support: viene contattato dal RCO quale responsabile che provvede ad avvisare gli operatori del servizio relativamente all'attivazione della continuità operativa e di tutte le successive decisioni che il Comitato di Gestione Crisi prenderà relativamente all'emergenza. Provvede inoltre a informare il Comitato di Gestione Crisi relativamente ai problemi e/o esigenze legate al proprio settore. In sua assenza, subentrano i vice-responsabili del Customer Support.
Attualmente la figura di RCO e Responsabile Customer Support coincidono.
Vice-responsabile Continuità Operativa: supporta il RCO e lo sostituisce in caso di assenza.
Legale rappresentante della Società: viene contattato dal RCO per informarlo della situazione di crisi e sulle modalità di gestione della stessa.
Servizio di assistenza software: viene contattato dal RCO e si riunisce con il Comitato di Gestione Crisi per valutare l'entità dell'evento disastroso dichiarato; in seguito provvede al ripristino del sistema nella sede secondaria individuata.
Servizio di assistenza hardware e telecomunicazioni: viene contattato dal RCO e provvede alla configurazione delle apparecchiature hardware (telefoni, collegamento internet, ecc.), per garantire la continuazione dell'erogazione dei servizi e la ripresa di una normale attività lavorativa.

N.B. Il RCO è esentato dall'obbligo di applicare parzialmente o totalmente il presente piano di ripristino nel caso ravvisi l'insorgere di condizioni di rischio o di aggravamento del rischio per il personale della Società legato alla messa in opera del Piano di DR.

Il personale trasferito presso l'eventuale sede temporanea di recovery è tenuto a rispettare le usuali condizioni di lavoro, in particolare per l'orario.

Nella tabella che segue vengono mostrate le responsabilità per la soluzione di disaster recovery, secondo i livelli attuativi e di ripristino dei vari sistemi e delle apparecchiature.

Nome e cognome	Ruolo	Cellulare	Posta elettronica
Silvia Misseri	RCO e Responsabile Customer Support	393.8909862	silvia.misseri@pamercato.it
Elena Aiazzi	Vice-responsabile RCO e Responsabile servizi telematici	328.7694243	elena.aiazzi@pamercato.it
Gian Domenico Volpi	Legale rappresentante	335.8014670	giandomenico.volpi@pamercato.it
ABC Technology	Servizio di assistenza software	055.701162; Simone Aiazzi : 338.4612503 Roberto Bianchi: 338.6599667	info@abctech.it
Teleinformatica Italiana	Servizio di assistenza hardware e telecomunicazioni	055.6531401; Leonardo Pieri: 348.2864526 Roberto Capanni: 349.4377345	info@teleinformaticaitaliana.it

4.1 COMUNICAZIONI VERSO L'ESTERNO

Per le comunicazioni verso l'esterno il Comitato di Gestione di Crisi/RCO adotta le seguenti modalità:

- per segnalare ai propri clienti un'interruzione anche parziale del servizio o un suo rallentamento, il RCO invia una comunicazione tramite email al referente indicato nella "Scheda Cliente" (vedi punto 2 in Appendice) spiegando la natura del problema, le misure prese per risolverlo, il tempo stimato per tornare del tutto operativi uscendo dall'emergenza ed eventuali danni già in essere (es: perdita di dati, perdita consistente di infrastrutture, reclami ecc). All'invio della e-mail seguirà una telefonata allo stesso referente per anticipare verbalmente il contenuto della stessa. Lo stesso iter procedurale

sarà seguito dal RCO anche per segnalare il ripristino del servizio ai propri clienti e confermando la fine dello stato di emergenza.

- per segnalare problemi alle infrastrutture telefoniche e/o informatiche il Responsabile delle Telecomunicazioni contatterà telefonicamente tramite altra linea il fornitore delle apparecchiature o i gestori dei servizi a seconda del tipo di problema rilevato (vedi "Vademecum" punto 4 in Appendice). Nella chiamata il RTL evidenzierà le problematiche riscontrate, lo stato attuale delle infrastrutture, il tipo di disservizio e gli eventuali tentativi di ripristino effettuati nella sede e sottolineerà l'emergenza del ripristino del disservizio.

- per segnalare problemi sulle piattaforme telematiche fornite dai clienti il RCO invia una comunicazione tramite email al referente indicato nella "Scheda Cliente" (vedi punto 2 in Appendice) spiegando la natura del problema e gli eventuali reclami ricevuti. All'invio della e-mail seguirà una telefonata allo stesso referente per anticipare verbalmente il contenuto della stessa.

- per segnalare eventuali informazioni utili all'erogazione del servizio, ad esempio il piano ferie, il RCO invia una comunicazione tramite email al referente indicato nella "Scheda Cliente" (vedi punto 2 in Appendice).

4.2 COMUNICAZIONI VERSO L'INTERNO

Per le comunicazioni verso l'interno il Comitato di Gestione di Crisi/RCO adotta le seguenti modalità:

- Il RCO redige ordini di servizio da inviare via email ai dipendenti della Società per informarli di eventuali giornate di formazione riguardanti il piano BC e DR e delle relative simulazioni degli scenari di crisi; per informarli di importanti modifiche al piano in via preventiva alle giornate di formazione; per comunicare la presenza di nuovi documenti da visionare nella cartella condivisa; per qualunque altro tipo di comunicazione ufficiale;

- Gli addetti al Customer Support comunicano verbalmente al RCO o al RTL problemi riscontrati nell'erogare il servizio non appena rilevano il malfunzionamento/rallentamento.

- Gli addetti al Customer Support nel caso di ricorso al telelavoro comunicano telefonicamente e tramite posta elettronica tra di loro e con il RCO per informarsi a vicenda dello stato del servizio. Il RCO informa gli addetti al servizio, con le stesse modalità di cui sopra circa il recupero della sede primaria, l'eventuale aggravarsi delle problematiche e relativamente a qualunque altro tipo di comunicazione necessaria al corretto svolgimento del lavoro e del servizio stesso.

5. POLITICA DI SICUREZZA E DI SALVAGUARDIA DEI DATI

In questa sezione vengono descritte le procedure di backup e archiviazione dei dati poste in essere dalla Società per evitare una qualsiasi perdita dei dati e di salvaguardia degli stessi attraverso la copia custodita in cloud.

Il backup è un punto fondamentale nelle procedure di disaster recovery e per garantire maggiori livelli di sicurezza è necessario che le copie di sicurezza dei dati siano collocate anche all'esterno della sede della Società, ovvero in cloud.
La Società, come meglio descritto in precedenza, per provvedere alla conservazione dei propri dati si è dotato di un'infrastruttura hardware, coadiuvata da specifico ambiente software e da servizi cloud, come di seguito organizzata:

- Uno storage collocato nella sede primaria e uno di ridondanza collocato nella sede secondaria che sono tra loro sincronizzati tramite Dropbox. Il server primario è sempre sincronizzato istantaneamente con il cloud DropBox che copia i dati immediatamente anche nel server secondario
- gli operatori del *customer support* gestiscono i dati direttamente sulle cartelle collegate in linea con lo storage e i dati sono salvati direttamente sullo stesso
- Quotidianamente viene attuato in automatico il back-up dei dati contenuti nello storage anche su altro hardware.
- In tempo reale, avviene la sincronizzazione di tutti i dati contenuti nello storage sul cloud. Come indicato in narrativa, il cloud utilizzato dalla Società è DropBox.
- Per quanto riguarda le e-mail, sono gestite e conservate nel cloud Microsoft, oltre che in locale sui pc degli utenti.
- In relazione ai dati gestiti tramite piattaforme telematiche per le quali viene svolto il servizio di customer support e/o attraverso software gestionali che ci sono stati messi a disposizione dai nostri clienti per l'erogazione del servizio stesso, questi sono archiviati e gestiti dai fornitori/proprietari delle stesse.

6. FASI DELLA SOLUZIONE DI DISASTER RECOVERY

Di seguito sono riepilogate le fasi della soluzione di disaster recovery individuata dalla Società:

- Valutazione della situazione di crisi/disastro/indisponibilità sito primario
- Dichiarazione del Disatro a opera del RCO
  - Le modalità di comunicazione dello stato di disastro sia all'esterno, verso i clienti e le ulteriori parti interessati (es. soggetti che erogano i servizi di TLC), sia all'interno sono dettagliate ai paragrafi 4.1 e 4.2 del presente Piano di DR.
- Notifica e attivazione delle strutture e del personale coinvolto nelle attività connesse alla dichiarazione di Disastro
- Attivazione del piano DR secondo gli scenari presenti al punto 3 dell'Appendice
- Attivazione del sito di DR e verifica del funzionamento del sistema informativo
- Gestione del sistema informativo presso il sito di DR
- Ripristino della sede primaria con la formale "Dichiarazione di fine emergenza" da parte del Comitato Gestione Crisi

7. GESTIONE E AGGIORNAMENTO DEL PIANO DR

Di primaria importanza è l'aggiornamento/revisione del piano di DR affinché sia sempre adeguato all'attività e all'organizzazione della Società. Ciò è garantito da una verifica periodica dell'adeguatezza della soluzione di DR ad opera del Responsabile della Continuità Operativa, che è altresì tenuto a verificare l'aggiornamento periodico dei piani e degli allegati, la formazione del personale citato nei documenti, l'effettuazione di *testing* ed esercitazioni.

I servizi di assistenza software e di assistenza hardware e TLC sono tenuti a segnalare preventivamente al Responsabile della Continuità Operativa ogni cambiamento tecnologico che possa rendere inapplicabile il presente documento, variazioni rilevanti nelle criticità dei processi gestiti e in particolare nel RTO, in modo da modificare strategia, piani e soluzioni tecnologiche contenute nel piano stesso per adeguarli alla nuova situazione.

8. COLLEGAMENTI/EVENTUALI INTERAZIONI CON GLI ALTRI DOCUMENTI DELLA SOCIETA'

Sistema di Gestione della Qualità Aziendale, in vigore da gennaio 2017 certificato da DNV GL, certificato n° 237485-2017-AQ-ITA-ACCREDIA

9. PROCEDURE DI TEST

La Società provvede all'esecuzione di test periodici e operativi in modo che sia garantito l'aggiornamento e il controllo dei piani. I test sono programmati almeno ogni sei mesi e comunque ogniqualvolta il Piano sia modificato.

Le modifiche del piano di Disaster Recovery saranno effettuate ogni qualvolta venga acquistata una nuova apparecchiatura per l'adeguamento del sistema informatico che vada a impattare sull'attuazione della soluzione tecnologica. Oltre all'adeguamento tecnologico del sistema informatico, si dovrà provvedere all'aggiornamento del Piano di DR anche nel caso in cui sia modificata la metodologia utilizzata per il disaster recovery.

I test periodici dovranno essere relazionati e inseriti nel Piano.

Possono comunque verificarsi condizioni che richiedono specifiche procedure di manutenzione straordinaria per cui si dovrà provvedere ad un adeguamento del Piano, a titolo esemplificativo e non esaustivo:

- modifiche delle figure facenti parte del Comitato di Gestione Crisi;
- modifiche dei Responsabili delle Aree/Servizi;
- modifiche legate ai gestionali utilizzati dalla Società e/o dal fornitore;
- modifica del fornitore dei servizi di assistenza hardware;
- modifica del fornitore dei servizi di assistenza software;

- modifiche dei contatti di qualsiasi figura interessata nelle procedure di CO e di DR o comunque sopra elencata.

I test consistono nelle seguenti simulazioni sul sito di DR:

- Il Responsabile della CO, esegue Comunicazione del Test di DR ai Responsabili di Area.
- Il Responsabile della CO attiva il Piano di DR nelle modalità operative simulate. Viene controllato l'effettivo aggiornamento dei dati estraendone una serie significativa a campione. Esempio:
    - Controllo delle e-mail archiviate in locale e sul cloud;
    - Controllo della data e della consistenza degli ultimi Documenti creati sullo storage e replicati su Google Drive.
- Il Responsabile del Customer Support esegue una serie di operazioni standard per verificare l'efficienza e l'aggiornamento del sito di DR.

Alla conclusione delle procedure di test deve essere redatta una relazione, a cura del Responsabile della Continuità Operativa e conservata agli atti, la quale deve essere fornita in copia alle figure che compongono il Comitato di Gestione Crisi.

La suddetta relazione deve descrivere i procedimenti effettuati per il test del *disaster recovery* e deve evidenziare gli eventuali discostamenti dal corretto andamento delle procedure.

Si procede alla descrizione nel dettaglio delle fasi del test di *disaster recovery*:

SCENARIO A: PERDITA SITO PRIMARIO

La simulazione consiste in:

- interruzione della sincronizzazione dello storage primario e riallineamento dei dati dello storage secondario rispetto a quanto contenuto nel cloud;
- procedure di collegamento al cloud (sul sito di DR);
- procedura di avvio del singolo servizio o dei servizi;
- procedure di ripristino della soluzione di disaster recovery.

SCENARIO B: INTERRUZIONE CORRENTE ELETTRICA E COLLEGAMENTO INTERNET

La simulazione consiste in:

- attivazione dei pc portatili di emergenza;
- attivazione del servizio telefonico tramite utilizzo di cellulari;
- collegamento internet UMTS tramite utilizzo di router portatili;
- trasferimento nel sito secondario se necessario;
- procedura di avvio dei servizi dalla sede secondaria;
- procedura di verifica dell'accesso ai dati anche dalla sede secondaria;
- procedure di ripristino della soluzione di disaster recovery.

SCENARIO C: DATA RECOVERY

La simulazione della perdita dei dati, consiste in:

- interruzione della sincronizzazione in cloud e del riallineamento dei dati effettuate presso la sede di DR;
- procedure di collegamento al cloud;
- procedure di recupero o di acquisizione di nuove apparecchiature elettroniche se necessario;
- procedure di ripristino della soluzione di disaster recovery.

10. FORMAZIONE SUL PIANO BC E DR

La Società provvede all'erogazione di formazione a favore degli addetti al servizio interessato dal presente Piano, a cadenza annuale e comunque ogniqualvolta lo stesso sia modificato.

La formazione è organizzata e svolta a cura del RCO e/o del suo vice.

APPENDICE

1. NUMERI UTILI

1. COMITATO DI GESTIONE CRISI			
Nome e cognome	Ruolo	Cellulare	Posta elettronica
Silvia Misseri	RCO e Responsabile Customer Support	393.8909862	silvia.misseri@pamercato.it
Elena Aiazzi	Vice-responsabile RCO e Responsabile servizi telematici	328.7694243	elena.aiazzi@pamercato.it
Gian Domenico Volpi	Legale rappresentante	335.8014670	giandomenico.volpi@pamercato.it

ASSISTENZA			
Nome e cognome	Ruolo	Cellulare	Posta elettronica
ABC Technology	Servizio di assistenza software	055.701162; Simone Aiazzi: 338.4612503 Roberto Bianchi: 338.6599667	info@abctech.it
Teleinformatica Italiana	Servizio di assistenza hardware e telecomunicazioni	055.6531401; Leonardo Pieri: 348.2864526 Roberto Capanni: 349.4377345	info@teleinformaticaitaliana.it

FORNITORI			
Nome e cognome	Ruolo	Telefono	Posta elettronica
Tim impresa semplice	Gestore linea fissa e internet	Call Center 191 Segnalazione guasti 800018914	
TimeNet	Gestore linea fissa e internet	0571 1738000	assistenza@timenet.it
Vodafone	Gestore linee mobili	Andrea Bini 3482246046 Servizio Business 800227755	andrea.bini@gruppoaura.com
ENEGAN	Gestore rete elettrica	Numero verde aziende 800978883 Informazioni su distacchi Da fisso 800978883 Da cell. 0550978883	

NUMERI TELEFONICI SU CUI DEVIARE LE CHIAMATE IN CASO DI EMERGENZA			
Nome e cognome	Ruolo	Telefono	Posta elettronica
SEDE SECONDARIA	Sede di via Chiantigiana 103-103/a, Bagno a Ripoli	055.640009	
SILVIA MISSERI	RCO e Responsabile Customer Support	393.8909862	silvia.misseri@pamercato.it
SARA STINGHI	Vice-referente customer support	360.1094944	sara.stinghi@pamercato.it
FRANCESCA TOGNOCCHI	Vice-referente customer support	337.1298316	francesca.tognocchi@pamercato.it
ELEONORA PERRINO	Addetta customer support	331.6872277	eleonora.perrino@pamercato.it
CELLULARE DI SERVIZIO	Cellulare di emergenza	370.3154392	

2. SCHEDE CLIENTI

SCHEDA N. 1°

NOMINATIVO:	i-Faber S.p.A
SEDE:	Via M. Quadrio, 17, 20154 Milano MI
REFERENTE:	Marco Sampaolesi marco.sampaolesi@accenture.com 3489781290
REQUISITI RICHIESTI AL CUSTOMER SUPPORT	RTO (Recovery Time Objective): 60 minuti RPO (Recovery Point Objective) : non richiesto

COMITATO GESTIONE CRISI PA&M	
RESPONSABILE CONTINUITÀ OPERATIVA (RCO) E RESPONSABILE CUSTOMER SUPPORT	SILVIA MISSERI silvia.misseri@pamercato.it cell. 393.8909862
VICE-RESPONSABILE CONTINUITÀ OPERATIVA E RESPONSABILE DEI SERVIZI TELEMATICI	ELENA AIAZZI elena.aiazzi@pamercato.it cell. 328.7694243
LEGALE RAPPRESENTATE DELLA SOCIETÀ	GIAN DOMENICO VOLPI giandomenico.volpi@pamercato.it cell. 3358014670

3. SIMULAZIONE SCENARI

SCENARIO A1: PERDITA SITO PRIMARIO – INDISPONIBILITÀ RETE INTERNET E RETE TELEFONICA

La simulazione coinvolge il RCO, il RTLC e 3 addetti al customer support e consiste in:

- Il RCO valuta la situazione di crisi e dichiara lo stato di Disastro
- Il RCO comunica la crisi al RTLC
- Il RTLC fa una verifica interna dello stato dei telefoni e di internet, stacca lo switch per provare a ripristinare le linee
- Se il problema persiste il RTLC chiama il fornitore della linea telefonica e di internet per capire se il problema è esterno alla sede aziendale
- Se il problema è esterno segnala il guasto al fornitore che garantisce per contratto di risolvere il problema entro 24 ore
- Prima di trasferirsi alla sede secondaria il RTLC accende i router di emergenza e se necessario opera un reindirizzamento manuale sul router di backup per ogni pc del Customer support; allo stesso tempo il RCO comunica al cliente la necessità di deviare le chiamate sui numeri di emergenza. Il RTLC a seconda della linea telefonica non funzionante ha la possibilità di deviare direttamente le chiamate in entrata delle linee Timenet
- Il trasferimento alla sede secondaria deve rappresentare un caso limite e deve avvenire solo nel caso di indisponibilità di tutte le linee telefoniche e dei tre sistemi di connessione internet
- Qualora si rendesse necessario il RCO può decidere di optare per il trasferimento nella sede secondaria.
- In trenta minuti dalla segnalazione della necessità di trasferimento il personale essenziale e il RCO raggiungono la sede secondaria e tornano operativi tramite i pc di emergenza portati dalla sede primaria e con quelli già presenti nella sede secondaria, collegandosi alla rete internet e recuperando i dati archiviati nel cloud.
- L'operatività deve essere ripristinata in un tempo massimo di 60 minuti (RTO)
- Il RTLC rimane in entrambi i casi alla sede primaria per verificare la risoluzione del problema e si tiene in contatto tramite cellulare aziendale con il RCO per aggiornalo degli sviluppi.
- Una volta rientrato il problema il RTLC avviserà il RCO che la sede primaria è tornata operativa e che il personale essenziale diviso in due gruppi può rientrare dalla sede secondaria.
- Il RCO comunica ai propri clienti che la crisi è stata risolta

SCENARIO A2: PERDITA SITO PRIMARIO – EVENTO ATMOSFERICO, ALLAGAMENTO, INCENDIO ETC..

La simulazione coinvolge il RCO, il RTLC e 3 addetti al customer support e consiste in:

- Il RCO valuta la situazione di crisi e dichiara lo stato di Disastro
- Il RCO comunica la crisi al RTLC e a tutto il personale presente
- Il RCO fa evacuare la sede primaria e chiama i soccorsi se necessario
- Il RCO avvisa il personale del Customer Support della necessità del trasferimento e, solo se possibile in condizioni di sicurezza, si reca nel punto di DR per reperire i pc portatili di emergenza.
- Il RCO comunica ai propri clienti di deviare le chiamate alla sede secondaria ed ai cellulari aziendali.
- In trenta minuti dalla segnalazione della necessità di trasferimento il personale essenziale e il RCO raggiungono la sede secondaria e tornano operativi con i pc di emergenza già presenti in loco, collegandosi alla rete internet e recuperando i dati archiviati nel cloud o collegandosi allo Storage secondario se è stato possibile trasportarlo.
- L'operatività deve essere ripristinata in un tempo massimo di 60 minuti (RTO)
- Il lavoro viene portato avanti nella sede secondaria fino al completo ripristino della sede primaria
- Il RCO valuta quando è possibile rientrare alla sede primaria e avvisa i propri clienti che la crisi è stata risolta

SCENARIO B: INTERRUZIONE CORRENTE ELETTRICA E COLLEGAMENTO INTERNET

La simulazione coinvolge il RCO, il RTLC e 3 addetti al customer support e consiste in:

- Il RCO valuta la situazione di crisi e dichiara lo stato di Disastro
- Il RCO comunica la crisi al RTLC
- Il RCO comunica agli addetti la necessità di attivare i pc portatili di emergenza;
- Il RTLC attiva i router portatili di emergenza e se necessario comunica agli addetti di attivare i telefoni aziendali come hotspot
- Il RCO comunica ai propri clienti di trasferire le chiamate sui cellulari di servizio.
- Se entro un'ora dal guasto la crisi non è ripristinata l'RCO comunica la necessità di trasferimento nel sito secondario;
- In trenta minuti dalla segnalazione della necessità di trasferimento, il personale essenziale e il RCO raggiungono la sede secondaria e tornano operativi collegandosi alla rete internet tramite i pc di emergenza portati dalla sede primaria e con quelli già presenti nella sede secondaria e recuperando i dati archiviati nel cloud.
- L'operatività deve essere ripristinata in un tempo massimo di 60 minuti (RTO)
- Il RCO comunica ai propri clienti che è possibile deviare le chiamate anche alla sede secondaria
- Il RTLC rimane alla sede primaria per verificare la risoluzione del problema e si tiene in contatto tramite cellulare aziendale con il RCO per aggiornalo degli sviluppi.
- Una volta rientrato il problema il RTLC avviserà il RCO che la sede primaria è tornata operativa e che il personale essenziale diviso in due gruppi può rientrare dalla sede secondaria.
- Il RCO comunica ai propri clienti che la crisi è stata risolta

SCENARIO C: DATA RECOVERY

La simulazione della perdita dei dati coinvolge il RCO, il RTLC e 3 addetti al customer support e consiste in:

- Il RCO valuta la situazione di crisi e dichiara lo stato di Disastro
- Il RCO comunica la crisi al RTLC
- Nell'ipotesi che lo storage primario sia stato compromesso il RTLC lo scollega dalla rete e chiama il tecnico per farsi guidare nell'apertura dell'accesso allo storage secondario agli addetti del Customer support.
- Nel frattempo gli addetti possono accedere ai dati tramite il cloud.
- Il tecnico valuterà con il RCO e il RTLC la necessità di sostituire o riparare lo storage compromesso.
- La perdita di uno o di entrambi gli storage non compromette l'operatività del customer support, crea la necessità di sostituire o riparare l'apparecchiatura compromessa, ma i dati saranno sempre accessibili nel cloud.

4. VADEMECUM PIANO BC E DR TELECOMUNICAZIONI

4.1 SE NON FUNZIONA IL TELEFONO

PER I NUMERI TIM 055.642259 - 055.643044

- controllare che le borchie siano tutte accese (spia rossa o arancione) → se sono spente le borchie chiamare l'assistenza TIM al 191
- controllare che siano accesi:
  - "centralino generale" → se non funziona controllare che sia attaccato alla corrente e che non sia spento dal pulsante posteriore. Se è effettivamente rotto è disponibile un "centralino di Backup" da attaccare al suo posto IMPORTANTE: non possono coesistere due centralini!!! Scollegare il vecchio PRIMA di attaccare il nuovo!!!
  - "centralino 055642259-055643044" - BRI LINK 0 E BRI LINK 1 DEVONO ESSERE ENTRAMBE VERDI se non lo sono controllare che il centralino sia attaccato alla corrente.

  Se il problema non è risolto dopo queste operazioni chiamare la Teleinformatica:

  Leonardo 3482864526
  Roberto 3494377345

PER I NUMERI TIMENET 0556560174 – 0556560399

- controllare che il router TIMENET sia acceso (le linee 0556560174 – 0556560399 funzionano attraverso questo router, così come la sincronizzazione di dropbox) – LA LUCE ROSSA "internet" è REGOLARE

→ se il router timenet è spento chiamare la Teleinformatica dopo aver verificato che sia correttamente attaccato alla corrente:
Leonardo 3482864526
Roberto 3494377345

→ attivare trasferimento di chiamate sulle linee Telecom dal pannello di controllo di TimeNet per accedere al pannello di controllo:
https://timenet.it/ → area riservata → inserire credenziali →VOIPSTAR →Info e Utility Dettagli linea 0556065399 → gestisci trasferimenti → "sempre" + numero di telefono su cui trasferire le chiamate (non entreranno più di 4 chiamate perché abbiamo solo 4 canali telecom)

In ogni caso se il problema non viene risolto nei primi 20 minuti di disservizio comunicare al responsabile del Customer Sopport di far deviare le chiamate sui numeri di emergenza:

NUMERI TELEFONICI SU CUI DEVIARE LE CHIAMATE IN CASO DI EMERGENZA			
Nome e cognome	Ruolo	Telefono	Posta elettronica
SILVIA MISSERI	RCO e Responsabile Customer Support	393.8909862	silvia.misseri@pamercato.it
SARA STINGHI	Vice-referente customer support	360.1094944	sara.stinghi@pamercato.it
FRANCESCA TOGNOCCHI	Vice-referente customer support	337.1298316	francesca.tognocchi@pamercato.it
ELEONORA PERRINO	Addetta customer support	331.6872277	eleonora.perrino@pamercato.it
CELLULARE DI SERVIZIO	Cellulare di emergenza	370.3154392	
SEDE SECONDARIA	Sede di via Chiantigiana 103-103/a, Bagno a Ripoli	055.640009	

4.2 SE NON FUNZIONA INTERNET

- verificare che router TIM e firewall siano accesi eventualmente controllare che siano correttamente attaccati alla corrente → il router è una scatolina nera con due antenne sul retro e sta dietro il firewall

- Riavviare il router TIM tramite il pulsante posteriore o direttamente staccando e riattaccando l'alimentazione. Se il problema è quello nel giro di 10/15 minuti dovrebbe tornare tutto funzionante.

- Se non basta provare a staccare e riattaccare gli switch 1 e 2 direttamente staccando le prese riconoscibili tramite l'etichetta perché internet passa dai telefoni che dipendono appunto dagli switch. TENERE PRESENTE CHE STACCANDO GLI SWITCH SI INTERROMPONO LE CHIAMATE IN CORSO E SI ISOLANO I TELEFONI PER QUALCHE MINUTO

- Se ancora internet non è ripartito accendere le chiavette internet di emergenza e chiamare il servizio Alice Business 800018914
  Se i pc non riescono a connettersi in wifi alle chiavette staccare il cavo di rete tenendo presente che senza cavo di rete non si accede a server e public

- È possibile invece di accedere a internet con le chiavette di emergenza passare manualmente ogni pc sul router timenet nel caso in cui il malfunzionamento di internet non derivi dalla mancanza di corrente

PASSAGGIO A ROUTER TIMENET

- ➔ CICCARE CON IL TASTO DESTRO SUL TASTO "START" PER CERCARE IL "PANNELLO DI CONTROLLO"
- ➔ CENTRO CONNESSIONE RETE ➔ ETHERNET
- ➔ DETTAGLI :
  PRENDERE NOTA DELL' INDIRIZZO IPv4 (es: 192.168.1.100 ultime tre cifre diverse per ogni PC)
- ➔ Tornare su ETHERNET e cliccare PROPRIETÀ
- ➔ doppio clic su "PROTOCOLLO INTERNET VERSIONE 4 (TCP/IPV4)"
- ➔ UTILIZZA IL SEGUENTE INDIRIZZO IP:
  - INDIRIZZO IPv4 diverso per ogni pc
  - Subnetmask 255.255.255.0
  - Gateway predefinito da scegliere fra i seguenti:
    192.168.1.20 (Timenet)
    192.168.1.254 (Telecom)
- ➔ utilizza i seguenti indirizzi server dns:
  - Server DNS preferito: 8.8.8.8
  - Server DNS alternativo 8.8.4.4

- Se il problema non dipende dalla TIM chiamare la Teleinformatica:
  Leonardo Pieri 3482864526
  Roberto Capanni 3494377345

  Oppure ABC Tech:
  Simone Aiazzi 338.4612503
  Roberto Bianchi 338.6599667

5. BUSINESS IMPACT ANALYSIS (BIA)

Activity Details											
Key Critical Activities	Key Critical Sub - Activities	Key Dependencies	30 min.	60 min	1,01 h to 4 h	4,01 h to 12,00 h	12,01 h +	Impact	MTPD	RTO	RPO
CUSTOMER SUPPORT	1) CALL	EMPLOYEES	3	5	5	5	5	-Financial impact - Legal regulatory - Reputation media - Stake Holder - Customer	24 H.	60 MIN.	NO IMPACT
		TELEINFORMATICA ITALIANA	2	2	3	4	5		48 H.	4 H.	NO IMPACT
		TELECOM ITALIA SPA	3	4	5	5	5		48 H.	60 MIN.	NO IMPACT
		ENEGAN	2	4	5	5	5		1 WEEK	60 MIN.	NO IMPACT
		TIMENET	3	4	5	5	5		48 H.	60 MIN.	NO IMPACT
		VODAFONE	2	2	3	4	5		48 H.	60 MIN.	NO IMPACT
		ABC TECHNOLOGY	2	2	3	4	5		48 H.	4 H.	NO IMPACT
		STORAGE	1	2	3	3	3		6 DAYS	24 H.	0
		MICROSOFT	3	4	5	5	5		24 H.	60 MIN.	0
		IFABER	3	5	5	5	5		24 H.	-	0
		HEADQUARTERS	2	3	3	4	4		4 WEEK	24 H.	NO IMPACT

		SEPARATE BRANCH	1	1	2	3	4		8 WEEKS	48 H.	NO IMPACT
		ENEL ENERGIA SPA	1	1	2	3	4		8 WEEKS	48 H.	NO IMPACT
		TLC SUPERVISOR	1	1	2	2	3		4 WEEKS	2 WEEKS	NO IMPACT
		CUSTOMER SUPPORT' SUPERVISOR	1	1	2	2	3		4 WEEKS	2 WEEKS	NO IMPACT
		UNIPOL	5	5	5	5	5		24 H.	NO IMPACT	NO IMPACT
		NEXT.IT	3	4	5	5	5		24 H.	60 MIN.	0
		MANAGER	1	1	2	2	3		4 WEEKS	2 WEEKS	NO IMPACT
		FIRST LEVEL TLC	5	5	5	5	5		24 H.	60 MIN.	1 H.
		SECOND LEVEL TLC	2	2	3	4	5		48 H.	60 MIN.	1 H.
		THIRD LEVEL TLC	1	1	2	3	3		48 H.	24 H.	1 H.
		DROPBOX	1	2	3	4	5		6 DAYS	24 H.	0
	2) E-MAIL	EMPLOYEES	3	5	5	5	5	-Financial impact - Legal regulatory - Reputation	24 H.	60 MIN.	NO IMPACT
		TELEINFORMATICA ITALIANA	2	2	3	4	5		24 H.	4 H.	NO IMPACT
		TELECOM ITALIA SPA	3	4	5	5	5		24 H.	60 MIN.	NO IMPACT

		ENEGAN	2	4	5	5	5	media - Stake Holder - Customer	1 WEEK	60 MIN.	NO IMPACT
		TIMENET	3	4	5	5	5		24 H.	60 MIN.	NO IMPACT
		VODAFONE	1	1	2	3	4		24 H.	60 MIN.	NO IMPACT
		ABC TECHNOLOGY	2	2	3	4	5		24 H.	4 H.	NO IMPACT
		STORAGE	1	2	3	3	4		6 DAYS	24 H.	0
		MICROSOFT	4	4	5	5	5		24 H.	60 MIN.	0
		IFABER	2	3	4	4	5		24 H.	-	0
		HEADQUARTERS	1	2	3	3	4		1 WEEK	24 H.	NO IMPACT
		SEPARATE BRANCH	1	1	2	3	4		2 WEEKS	48 H.	NO IMPACT
		ENEL ENERGIA SPA	1	1	2	3	4		2 WEEKS	48 H.	NO IMPACT
		TLC SUPERVISOR	1	1	2	2	3		4 WEEKS	2 WEEK	NO IMPACT
		CUSTOMER SUPPORT' SUPERVISOR	1	1	2	2	3		4 WEEKS	2 WEEK	NO IMPACT
		UNIPOL	5	5	5	5	5		24 H.	NON PERTINENTE	NO IMPACT
		NEXT.IT	4	4	5	5	5		24 H.	60 MIN.	24 H.

		MANAGER	1	1	2	2	3		4 WEEKS	2 WEEK	NO IMPACT
		FIRST LEVEL TLC	5	5	5	5	5		24 H.	60 MIN.	1 H.
		SECOND LEVEL TLC	2	2	3	4	5		48 H.	60 MIN.	1 H.
		THIRD LEVEL TLC	1	1	2	3	3		48 H.	24 H.	1 H.
		DROPBOX	1	2	3	4	5		6 DAYS	24 H.	0
	3) ADMINISTRATION	READYTECH	1	1	1	1	3	-Financial impact - Legal regulatory - Reputation media - Stake Holder - Customer	30 DAYS	15 DAYS	1 WEEK
		INFOCERT	1	1	1	1	3		30 DAYS	15 DAYS	1 WEEK
		CNA SERVIZI E CONSULENZE SRL	1	1	1	1	3		30 DAYS	15 DAYS	1 WEEK
		STUDIO TRIBUTARIO E COMMERCIALE BRIENZA ALESSIO E FRANCESCO CONTICINI	1	1	1	1	3		30 DAYS	15 DAYS	1 WEEK
		RSPP FILIPPO GALLETTI	1	1	1	1	3		1 WEEK	48 H.	NO IMPACT
		ADMINISTRATIVE MANAGEMENT	1	1	1	1	3		4 WEEKS	2 WEEK	NO IMPACT

	4) PRIVACY	PRIVACY SUPERVISOR	1	1	2	2	5	-Financial impact - Legal regulatory - Reputation media - Stake Holder - Customer	4 WEEK	2 WEEK	NO IMPACT
		DPO	1	1	1	1	5		4 WEEK	2 WEEK	NO IMPACT
	5) MARKETING		1	1	1	1	1	-Financial impact - Legal regulatory - Reputation media - Stake Holder - Customer	\	\	NO IMPACT
	6) CONSULTANCY FOR PUBLIC ADMINISTRATIONS AND PRIVATE IN THE FIELD OF PUBLIC CONTRACTS		1	1	1	1	1		\	\	NO IMPACT

6. DEPENDENCIES

DEPENDENCIES - INTERNAL

#	Name of the business unit	Dependency Type	Reason for dependency	Linked to Function (Specify numbers)
1	EMPLOYEES	MANDATORY	THEY DELIVER THE SERVICE	1 TO 6
2	HEADQUARTERS	MANDATORY	THE PLACE WHERE THE SERVICE IS DELIVERED	1 TO 6
3	FIRST LEVEL TLC (SWITCHBOARD - FIREWALL - ROUTER - SWITCH1 - SWITCH2 - ANTIVIRUS)	MANDATORY	INFRASTRUCTURES TO DELIVEREDE THE SERVICE	1 TO 6
4	SECOND LEVEL TLC (PC-TELEPHONES- PORTABLE ROUTERS)	DISCRETIONARY	INFRASTRUCTURES TO DELIVEREDE THE SERVICE	1 TO 6
5	THIRD LEVEL TLC (LAPTOP-MOBILE PHONES- ACCESSPOINT)	DISCRETIONARY	INFRASTRUCTURES TO DELIVEREDE THE SERVICE	1, 2, 6
6	MANAGER	MANDATORY	THE HEAD OF THE ORGANIZATION	1 TO 6
7	SEPARATE BRANCH	DISCRETIONARY	THE PLACE WHERE THE SERVICE IS DELIVERED IN CASE OF EMERGENCY	1 AND 2
8	STORAGE	DISCRETIONARY	ARCHIVE	1 TO 6

9	TLC SUPERVISOR	MANDATORY	PART OF THE ORGANIZATION	1 TO 6
10	ADMINISTRATIVE MANAGEMENT	MANDATORY	PART OF THE ORGANIZATION	1 TO 6
11	PRIVACY SUPERVISOR	MANDATORY	PART OF THE ORGANIZATION	1 TO 6
12	CUSTOMER SUPPORT' SUPERVISOR	MANDATORY	PART OF THE ORGANIZATION	1 AND 2

DEPENDENCIES - EXTERNAL

#	Name of the agency	Reason for dependency	Linked to Function (Specify number)	Impact if the organization stops providing service	Does the agency have BCM implemented?
1	TELEINFORMATICA ITALIANA	TLC	1 TO 6	H	Not Sure
2	ABC TECHNOLOGY	TLC	1 TO 6	H	No
3	ZONA ZERO	WEB AGENCY	3 TO 6	M	No
4	ENEGAN	ENERGY PROVIDER	1 TO 6	H	Not Sure
5	VODAFONE	TLC	1 TO 6	M	Not Sure
6	TELECOM ITALIA SPA	TLC	1 TO 6	H	Not Sure
7	TIMENET SRL	TLC	1 TO 6	H	Not Sure
8	IFABER	SUPPLIER AND CLIENT	1,2,6	H	Yes

9	READYTECH	ACCOUNTING	3	L	No
10	MICROSOFT IRELAND OPERATIONS LTD	TLC	1 TO 6	H	Not Sure
11	DROPBOX	TLC	1 TO 6	H	No
12	NEXT.IT	TLC	1 TO 6	H	No
13	DPO FLAVIO CORSINOVI	DATA PROTECTION	4	L	Not Applicable
14	STUDIO TRIBUTARIO E COMMERCIALE BRIENZA ALESSIO E FRANCESCO CONTICINI	ACCOUNTING CONSULTATION	3	L	Not Applicable
15	CNA SERVIZI E CONSULENZE SRL	LABOUR CONSULTANT	3	M	Not Sure
16	UNIPOL SAI ASSICURAZIONE SPA	INSURANCE	1 TO 6	H	Not Applicable
17	RSPP FILIPPO GALLETTI	SECURITY ADVISOR	1 TO 6	L	Not Applicable
18	INFOCERT SPA	ACCOUNTING	3	L	Not Sure
19	ENEL ENERGIA	ENERGY PROVIDER	1,2	M	Not Sure

Impacts
Financial Impact
Legal regulatory
Reputation Media
Stake Holder
Customer
Other

Impact	Impact Rating		
Minor or no impact	**1**		Insignificant
Impact can be tolerated/Tolerable Financial Loss	**2**		Minor
Significant impact/Legal Warning/ Some Financial Loss	**3**		Moderate
Serious Impact/Legal Warning/Financial Loss	**4**		Major
Critical Impact/Legal Implications/Huge Financial Loss/ Reputation Loss to some Extent/	**5**		Critical

REV 00 DEL 8 OTTOBRE 2018

7. INVENTARIO INFRASTRUTTURE TLC

STANZA	NOME/ DIPENDENTE	TLC	DESCRIZIONI AGGIUNTIVE	MARCA	DATA INGRESSO	PERIODO DI VITA PRESUNTO	DATA PRESUNTA SOSTITUZIONE
A	ELENA	SIM	3287694243	VODAFONE	dic-17	-	-
		TELEFONO FISSO-A1	253 ELENA	SANGOMA	giu-17	5 ANNI	**giu-22**
		PC - A1	ANTIVIRUS KASPERSKY	KASPERSKY	11/01/2018	1 ANNO	**11/01/2019**
			MOUSE PC - A1	DELL	ott-16	4 ANNI	**ott-20**
			TASTIERAPC - A1	DELL	ott-16	4 ANNI	**ott-20**
			MONITORPC - A1	DELL	ott-16	6 ANNI	**ott-22**
			DESKTOP-F1UASF9	DELL	ott-16	3 ANNI	**ott-19**
			CASSE PC - A1	LOGITECH	feb-17	6 ANNI	**feb-23**
	SILVIA	Cell. 1	GALAXY S8 PLUS 64GB BLACK E RID	SAMSUNG	dic-17	3 ANNI	**dic-20**
		SIM	3938909862	VODAFONE	dic-17	-	-

		CUFFIE TELEFONO - A2	2 CUFFIE	JABRA	apr-18	3 ANNI	**apr-21**
		TELEFONO FISSO- A2	225 SILVIA	YEALINK	giu-16	5 ANNI	**giu-21**
		PC-A2	ANTIVIRUS KASPERSKY	KASPERSKY	10/04/2018	1 ANNO	**11/04/2019**
			MOUSE PC-A2	DELL	apr-18	4 ANNI	**apr-22**
			TASTIERAPC-A2	DELL	apr-18	4 ANNI	**apr-22**
			MONITOR PC-A2	SAMSUNG	apr-18	6 ANNI	**apr-24**
			DESKTOP-R4KF4OR	DELL	apr-18	3 ANNI	**apr-21**
	ELEONORA	Cell. 2	GALAXY J3 ED 2016 4G BLACK STD	SAMSUNG	dic-17	3 ANNI	**dic-20**
		SIM	3316872277	VODAFONE	dic-17	-	**-**
		CUFFIE TELEFONO - A3	1 CUFFIA	YEALINK	giu-17	3 ANNI	**giu-20**
		TELEFONO FISSO- A3	251 ELEONORA	SANGOMA	giu-17	5 ANNI	**giu-22**
		PC - A3	ANTIVIRUS KASPERSKY	KASPERSKY	10/04/2018	1 ANNO	**11/04/2019**
			MOUSE PC - A3	DELL	apr-18	4 ANNI	**apr-22**
			TASTIERA PC - A3	DELL	apr-18	4 ANNI	**apr-22**
			MONITOR PC - A3	SAMSUNG	apr-18	6 ANNI	**apr-24**
			DESKTOP-PSICC0R	DELL	apr-18	3 ANNI	**apr-21**

	MILKO	NAS CHIANTI - A4	echiantinas	QNAP	mag-18	3 ANNI	**mag-21**
		TELEFONO FISSO-A4	222 MILKO	YEALINK	giu-17	5 ANNI	**giu-22**
		MONITOR1 - A4	MILKO MONITOR	SAMSUNG	set-18	6 ANNI	**set-24**
B	TLC DI SERVIZIO	SIM	3703154392	VODAFONE	dic-17	-	-
		Cell. 3	WINDOWS PHONE LUMIA 640	MICROSOFT	ott-15	3 ANNI	**ott-18**
		CENTRALINO	211	YEALINK	giu-16	5 ANNI	**giu-21**
	FRANCI T	Cell.4	GALAXY J3 ED 2016 4G BLACK STD	SAMSUNG	dic-17	3 ANNI	**dic-20**
		SIM	3371298316	VODAFONE	dic-17	-	-
		CUFFIE GN200 - B1	2 CUFFIE	GN200	set-17	3 ANNI	**set-20**
		TELEFONO FISSO - B1	214 FRANCESCA T.	YEALINK	giu-18	5 ANNI	**giu-23**
		PC - B1	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			MOUSE PC - B1	ASUS	lug-17	4 ANNI	**lug-21**
			TASTIERA PC - B1	ASUS	lug-17	4 ANNI	**lug-21**
			MONITOR PC - B1	PHILIPS	lug-17	6 ANNI	**lug-23**
			DESKTOP-03ODCN8	ASUS PRO	lug-17	3 ANNI	**lug-20**
	FRANCI R	TELEFONO FISSO - B2	224 FRANCESCA R.	YEALINK	giu-16	5 ANNI	**giu-21**
		CUFFIE JABRA - B2	1 CUFFIA	JABRA	set-17	3 ANNI	**set-20**

		PC - B2	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			MOUSE PC - B2	FUJITSU	set-17	4 ANNI	**set-21**
			TASTIERA PC - B2	FUJITSU	set-17	4 ANNI	**set-21**
			MONITOR PC - B2	PHILIPS	set-17	6 ANNI	**set-23**
			PAM2	FUJITSU	set-17	3 ANNI	**set-20**
	SARA	Cell. 5	GRAND PRIME	SAMSUNG	ott-15	3 ANNI	**ott-18**
		SIM	3601094944	VODAFONE	dic-17	-	**-**
		CUFFIE GN200 - B3	2 CUFFIE	GN200	set-17	3 ANNI	**set-20**
		TELEFONO FISSO - B3	212 SARA	YEALINK	giu-17	5 ANNI	**giu-22**
		PC - B3	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			MOUSE PC - B3	ASUS	lug-17	4 ANNI	**lug-21**
			TASTIERA PC - B3	ASUS	lug-17	4 ANNI	**lug-21**
			MONITOR PC - B3	PHILIPS	lug-17	6 ANNI	**lug-23**
			DESKTOP-3ID406B	ASUS PRO	lug-17	3 ANNI	**lug-20**
	DUCCIO	TELEFONO FISSO - B4	252 DUCCIO	SANGOMA	giu-17	5 ANNI	**giu-22**
		CUFFIE JABRA - B4	2 CUFFIE	JABRA	set-17	3 ANNI	**set-20**
		PC - B4	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			MOUSE PC - B4	FUJITSU	set-17	4 ANNI	**set-21**
			TASTIERA PC - B4	FUJITSU	set-17	4 ANNI	**set-21**

			MONITOR PC - B4	PHILIPS	set-17	6 ANNI	**set-23**
			PAM1	FUJITSU	set-17	3 ANNI	**set-20**
	BEATRICE	TELEFONO FISSO - B5	254 BEATRICE	SANGOMA	giu-17	5 ANNI	**giu-22**
		CUFFIE JABRA - B5	2 CUFFIE	JABRA	set-17	3 ANNI	**set-20**
		PC - B5	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			MOUSE PC - B5	FUJITSU	set-17	4 ANNI	**set-21**
			TASTIERA PC - B5	FUJITSU	set-17	4 ANNI	**set-21**
			MONITOR PC - B5	PHILIPS	set-17	6 ANNI	**set-23**
			PAM3	FUJITSU	set-17	3 ANNI	**set-20**
C	SABRINA	TELEFONO FISSO - C1	218 SABRINA	YEALINK	giu-16	5 ANNI	**giu-21**
		PC -C1	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			MOUSE PC -C1	TRUST	lug-15	4 ANNI	**lug-19**
			LAPTOP-24ICGEMV	ACER	lug-17	3 ANNI	**lug-20**
	GABRIELE	TELEFONO FISSO - C2	230 GABRIELE	GRAND STREAM	set-17	5 ANNI	**set-22**
		PC - C2	MOUSE PC - C2	TRUST	lug-15	4 ANNI	**lug-19**
			ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			PCw7	PACKERBELL	mag-16	3 ANNI	**mag-19**
	IRENE	Cell. 6	SAMSUNG S3 - GT - I9300	SAMSUNG	ott-15	3 ANNI	**ott-18**

		SIM	3351225654	VODAFONE	dic-17	-	-
		TELEFONO FISSO - C3	213 IRENE	YEALINK	giu-16	5 ANNI	**giu-21**
		PC - C3	MOUSE PC - C3	TRUST	lug-15	4 ANNI	**lug-19**
			ANTIVIRUS KASPERSKY	KASPERSKY	10/04/2018	1 ANNO	**11/04/2019**
			irenepc	DELL	apr-18	3 ANNI	**apr-21**
D	**GIANNI**	TELEFONO FISSO - D1	227 LISA	YEALINK	giu-16	5 ANNI	**giu-21**
		Cell. 7	GALAXY S8 PLUS 64GB BLACK E RID	SAMSUNG	dic-17	3 ANNI	**dic-20**
		SIM	3358014670	VODAFONE	dic-17	-	-
		PROIETTORE		EPSON	giu-16	6ANNI	**giu-22**
		MONITORD1		SHARP	2015	6 ANNI	**2021**
		TELEFONO SOSTITUTIVO		YEALINK	giu-16	5 ANNI	**giu-21**
		TELEFONO FISSO - D2	223 GIANNI	YEALINK	giu-16	5 ANNI	**giu-21**
		PC - D2	ANTIVIRUS KASPERSKY	KASPERSKY	10/04/2018	1 ANNO	**11/04/2019**
			GIANNIPC	DELL	apr-18	3 ANNI	**apr-21**
	FABIOLA	Cell. 8	GALAXY S8 PLUS 64GB BLACK E RID	SAMSUNG	dic-17	3 ANNI	**dic-20**

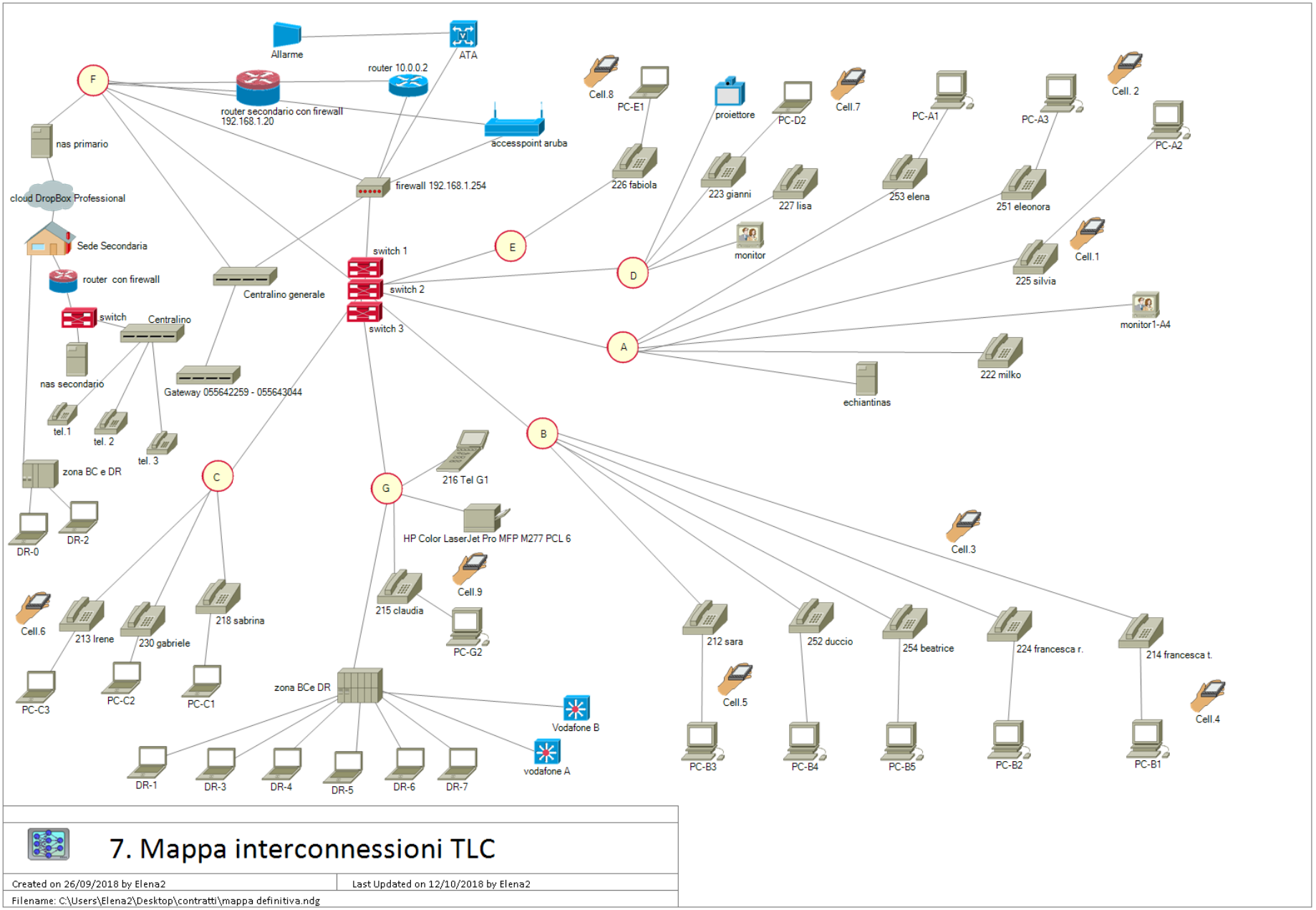
E		SIM	3282346719	VODAFONE	dic-17	-	-
		TELEFONO FISSO - E1	226 FABIOLA	YEALINK	giu-16	5 ANNI	**giu-21**
		PC - E1	TASTIERA PC - E1	TRUST	feb-16	4 ANNI	**feb-20**
			ANTIVIRUS KASPERSKY	KASPERSKY	10/04/2018	1 ANNO	**11/04/2019**
			fabiolainspiron	DELL	apr-18	3 ANNI	**apr-21**
F	ARMADIO	SERVER	winserver2016	DELL	apr-18	5 ANNI	**apr-23**
		NAS PRIMARIO	pamercato	qnap	ott-17	3 ANNI	**ott-20**
		HARD DISK	BACK UP DEL NAS	Vulteck	dic-17	5 ANNI	**dic-22**
		FIREWALL	Zyxell usg20-vpn	Zyxell	feb-17	5 ANNI	**feb-22**
		ACCESS POINT		ARUBA	apr-18	5 ANNI	**apr-23**
		GATEWAY	TELECOM	PATTON	giu-16	3 ANNI	**giu-19**
		CENTRALINO DI BACKUP	NETBOXV16	NETHESIS	giu-16	3 ANNI	**giu-19**
		CENTRALINO PRINCIPALE	NETBOXV16	NETHESIS	giu-16	3 ANNI	**giu-19**
		ATA	allarme	Grandstream	giu-16	5 ANNI	**giu-21**
		UPS1	PRESE ROSSE	RIELLO	giu-16	5 ANNI	**giu-21**
		UPS2	ARMADIO	RIELLO	giu-16	5 ANNI	**giu-21**
		Switch3	switch di back up	Edge	giu-16	5 ANNI	**giu-21**
		Switch2	NETGEAR PROSAVE	NETGEAR	giu-16	5 ANNI	**giu-21**
		Switch1	HPPROCURVE	HP	giu-16	5 ANNI	**giu-21**

		router1	TELECOM	NETGEAR	giu-17	5 ANNI	**giu-22**
		router2	TIMENET	Zyxell	lug-18	5 ANNI	**lug-23**
G	CLAUDIA	Cell. 9	GALAXY J5 ED 2017 BLACK STD	SAMSUNG	dic-17	3 ANNI	**dic-20**
		SIM	3288763738	VODAFONE	dic-17	-	-
		TELEFONO CORDLESS - G1	216	GIGASET	feb-18	5 ANNI	**feb-23**
		TELEFONO FISSO - G2	215 CLAUDIA	YEALINK	giu-16	5 ANNI	**giu-21**
		PC - G2	MOUSE PC - G2	TRUST	ott-16	4 ANNI	**ott-20**
			ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			TASTIERA PC - G2	DELL	ott-16	4 ANNI	**ott-20**
			MONITOR PC - G2	DELL	ott-16	6 ANNI	**ott-22**
			DESKTOP-NKC9PJS	DELL	ott-16	3 ANNI	**ott-19**
		STAMPANTE	HP Color LaserJet Pro MFP M277 PCL 6	HP	giu-17	5 ANNI	**giu-22**
	ZONA DI DR	DR6	Lenovo2 SOLO INTERNET	LENOVO	2016	3 ANNI	**2019**
			ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
		DR MOUSE1		TRUST	ott-16	4 ANNI	**ott-20**
		DR MOUSE2		Dell	ott-16	4 ANNI	**ott-20**
		DR1	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			DELL1	DELL	2015	3 ANNI	**2018**

		DR 3	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			PACKERBELL1	PACKERBELL	2015	3 ANNI	**2018**
		DR4	ANTIVIRUS KASPERSKY	KASPERSKY	16/01/2018	1 ANNO	**17/01/2019**
			ACER	ACER	2015	3 ANNI	**2018**
		DR 5	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			DELL2	DELL	2015	3 ANNI	**2018**
		DR 6	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			LENOVO 2	LENOVO	2016	3 ANNI	**2019**
		DR 7	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			DELL SILVIA	DELL	2015	3 ANNI	**2018**
		vodafoneA	R216 LTE WHITE STD	HUAWEI	dic-17	5 ANNI	**dic-22**
		vodafoneB	R216 LTE WHITE STD	HUAWEI	dic-17	5 ANNI	**dic-22**
2° SEDE		NAS SECONDARIO		qnap	dic-17	3 ANNI	**dic-20**
	ZONA DI DR	DR-0	ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
			LENOVO1 SOLO INTERNET	LENOVO	2016	3 ANNI	**2019**
			ANTIVIRUS KASPERSKY	KASPERSKY	10/01/2018	1 ANNO	**11/01/2019**
		DR-2	PACKERBELL2	PACKERBELL	2015	3 ANNI	**2018**

SOFTWARE E LICENZE	365 OFFICE ESSENTIAL BUSINESS	19 LICENZE	MICROSOFT	16/12/2017	1 ANNO	**16/12/2018**
	365 OFFICE BUSINESS PREMIUM	6 LICENZE	MICROSOFT	16/12/2017	1 ANNO	**16/12/2018**
	GAMMA EVOLUTION	GESTIONALE DI FATTURAZIONE	READYTECH	15/05/2018	-	**-**
	DROP BOX PROFESSIONAL	CLOUD ON LINE	DROP BOX	4/5/2018	-	4/5/2019
	DROP BOX BASIC	SOLO CARTELLA SUPPORTO	DROP BOX	-	-	-

LEGENDA SCADENZE	2024	apparecchiatura appena entrata in azienda oppure con lunga durata
	2023	
	2022	
	2021	apparecchiatura da iniziare a tenere sotto controllo con maggiore frequenza oppure con breve durata
	2019	
	2018	La società prende atto della possibile necessità di sostituzione delle apparecchiature e procede ove necessario alla sostituzione di eventuali parti del dispositivo


Allarme
ATA
F
router 10.0.0.2
router secondario con firewall
192.168.1.20
accesspoint aruba
nas primario
firewall 192.168.1.254
cloud DropBox Professional
Sede Secondaria
router con firewall
switch
Centralino
nas secondario
Gateway 055642259 - 055643044
Centralino generale
switch 1
switch 2
switch 3
E
D
A
B
C
G
Cell.8
PC-E1
226 fabiola
proiettore
PC-D2
Cell.7
223 gianni
227 lisa
PC-A1
253 elena
PC-A3
251 eleonora
Cell. 2
PC-A2
monitor
225 silvia
Cell.1
monitor1-A4
222 milko
echiantinas
tel.1
tel. 2
tel. 3
zona BC e DR
DR-0
DR-2
216 Tel G1
HP Color LaserJet Pro MFP M277 PCL 6
Cell.9
215 claudia
PC-G2
Cell.3
Cell.6
213 Irene
230 gabriele
218 sabrina
PC-C3
PC-C2
PC-C1
zona BCe DR
Vodafone B
vodafone A
DR-1
DR-3
DR-4
DR-5
DR-6
DR-7
212 sara
Cell.5
PC-B3
252 duccio
PC-B4
254 beatrice
PC-B5
224 francesca r.
PC-B2
214 francesca t.
Cell.4
PC-B1
7. Mappa interconnessioni TLC
Created on 26/09/2018 by Elena2
Last Updated on 12/10/2018 by Elena2
Filename: C:\Users\Elena2\Desktop\contratti\mappa definitiva.ndg