Piano della Sicurezza Informatica di A.S.S.E.MI.

(art. 4, c. 3, lett. C, DPCM 03 dicembre 2013 Art.12, DPCM 13 novembre 2014)

1 Il piano di sicurezza informatica

1.1 Definizione

Il ricorso alle tecnologie dell'informazione e della comunicazione intrapreso da A.S.S.E.MI. - Azienda Sociale Sud Est Milano per lo snellimento, l'ottimizzazione e una maggiore efficienza dei procedimenti amministrativi, comporta una serie di rischi che, se non adeguatamente affrontati, potrebbero comportare gravi conseguenze sull'affidabilità dei dati e dei servizi. Tali rischi sono imputabili a due fattori caratteristici della tecnologia in questione: la non garanzia di corretto funzionamento sia nelle componenti hardware che in quelle software e l'esposizione alle intrusioni informatiche. In termini più operativi è bene intendere la sicurezza del Sistema Informativo non solo come "protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali". ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause" attraverso un'analisi dei rischi e delle misure implementate per l'eliminazione o la loro attenuazione in funzione della gravità e probabilità di un evento..

Si evidenzia che la sicurezza del Sistema Informativo non dipende solo da aspetti tecnici ma anche, se non principalmente, da quelli organizzativi, sociali e legali. La sicurezza del Sistema Informativo è pertanto vista come caratteristica "globale", in grado di fornire dinamicamente, con l'evolversi temporale delle necessità e delle tecnologie, il desiderato livello di disponibilità, integrità e confidenzialità delle informazioni e dei servizi erogati.

Il presente Piano descrive le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, nel rispetto di quanto disposto e ancora applicabile dal D. Lgs 196/2003, "Codice in materia di protezione dei dati personali" e del relativo Allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" e quanto già previsto o in corso di implementazione per l'aggiornamento delle misure tecniche come indicato nell'art.32 del REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO (in seguito GDPR) del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Sono elencate le strategie ed i controlli adottati per assicurare al Sistema Informativo di A.S.S.E.MI. un adeguato livello di sicurezza.

1.2 Obiettivi

Scopo del presente documento è descrivere la strategia che A.S.S.E.MI. intende adottare per poter soddisfare i seguenti requisiti di sicurezza:

- *Confidenzialità*: l'accesso e la divulgazione delle informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, deve poter essere effettuato solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, la probabilità che un'informazione riservata sia resa pubblica.
- *Integrità*: la modifica o la distruzione di informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, devono poter essere effettuate solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, le probabilità che l'informazione sia in qualche modo modificata. Devono essere altresì garantiti sia l'origine del dato (non ripudiabilità) che la sua conformità all'originale (autenticità).
- *Disponibilità*: l'accesso all'informazione e ai sistemi deve essere sempre affidabile e tempestivo. Una perdita di disponibilità si verifica quando a fronte di un'intrusione un sistema diventa non più accessibile da parte degli utenti.
- *Accountability* (Tracciabilità): tutte le azioni che un'entità compie nell'ambito del sistema sono memorizzate in modo tale da poter essere, in tempi successivi, ricondotte in maniera inequivocabile all'entità stessa.

L'adozione di idonee e preventive misure di sicurezza garantisce che il trattamento dei dati personali comuni identificativi, sensibili e/o giudiziari venga effettuato in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Il Piano per la sicurezza informatica si basa sull'analisi dei rischi a cui è esposto il sistema informatico, i relativi dati e documenti in esso contenuti e sulle direttive strategiche stabilite dal vertice di A.S.S.E.M.I..

Il presente Piano è soggetto a revisione, in funzione dell'estensione del sistema, dell'evoluzione tecnologica, della variazione degli obiettivi dell'organizzazione e del manifestarsi di nuovi o mutati rischi per la sicurezza. In caso di eventi straordinari il Piano è soggetto ad una revisione estemporanea.

1.3 Responsabilità (figure coinvolte)

L'Ente predispone il Piano per la sicurezza informatica ai sensi dell'art.12 del DPCM 13 novembre 2014. Tale piano risulta essere comprensivo di quanto richiesto all'art. 4 del DPCM 3 dicembre 2013, relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici, è predisposto dal Responsabile della gestione documentale nel rispetto del D.Lgs 196/2003 e del relativo Allegato B, Responsabile del trattamento dei dati personali, Direttore Generale di A.S.S.E.MI. e per quanto ancora applicabile in accordo all'art.32 del GDPR.

2 Il sistema informativo A.S.S.E.MI.

2.1 Tipologia di servizi offerti

Il Sistema Informativo di A.S.S.E.MI. è rivolto a soddisfare tutte le esigenze di carattere informativo-informatico dal punto di vista delle esigenze "interne" gestendo direttamente i dati dell'utenza della popolazione residente che riceve o dalle persone o dai Comuni appartenenti alla rete.

2.2 Servizio informativo

2.2.1 Organizzazione

Nel contesto del Sistema Informativo ogni dipendente di A.S.S.E.MI. deve collaborare, secondo le proprie specifiche funzioni, alla gestione del Sistema Informativo e alla gestione generale della sicurezza.

Tipologia Utenti	Compiti/Responsabilità	Note
Addetti società assistenza hardware e software	Attuazione e messa in opera delle politiche di sicurezza informatica (sistemi antivirus, firewalling, backup, politiche relative alle utenze, …). Verifiche sull'attuazione delle politiche	
Dipendenti A.S.S.E.MI. (generici)	Rispetto delle norme relative alla Sicurezza Informatica; rispetto delle norme inerenti il trattamento dati	Vedi incarichi specifici a Responsabile o incaricato del trattamento nei settori specifici

2.2.2 Addetti

Nel contesto del Sistema Informativo ogni dipendente di A.S.S.E.MI. è, in varia misura e con compiti diversi, corresponsabile del Sistema Informativo nel suo complesso. Per quanto concerne la gestione vera e propria della progettazione ed implementazione delle politiche di sicurezza informatica è stata incaricata una società esterna specializzata in tale settore la quale svolge anche attività di assistenza hardware e software.

2.3 Infrastruttura tecnologica

2.3.1 Generalità

L'Infrastruttura Tecnologica di A.S.S.E.MI. è schematizzata come segue:

<table>
<tr><th colspan="2">Apparati Server interni</th></tr>
<tr><th>Tipologia di apparati</th><th>Descrizione e Luogo</th></tr>
<tr><td>1 Server marca IBM mod. x3650 M2
Sistema operativo
Windows Server 2008 R2 Standard</td><td>Server proprietà A.S.S.E.MI. dislocato presso la Sala Server A.S.S.E.MI. situato a San Donato Milanese, via Sergnano n.2
Funzioni svolte:
Active Directory e Domain Services
File server
DHCP and DNS server
Gestione e database per programma gestionale CieloNext-archivio storico</td></tr>
<tr><td></td><td>E' stata valutata possibilità di installare un server di proprietà A.S.S.E.MI. a San Giuliano Milanese, si è proceduto all'acquisto, a cui seguirà installazione e configurazione (vedi allegato n.1)</td></tr>
<tr><td colspan="2">apparati Server Esterni

Il sistema contabile di A.S.S.E.MI Ad Hoc Revolution, integrato con il software Fatel per la fatturazione elettronica e comunicazioni IVA, è gestito tramite applicativi web collocati in server farm con contratto di hosting con fornitore esterno Zucchetti S.p.A. e Zucchetti Informatica, vedi all. n.4 "SLA Data Center di Zucchetti S.p.A."

Il servizio di posta elettronica, il sito web aziendale e la cartella sociale distrettuale sono gestiti tramite fornitore esterno Progetti di Impresa s.r.l., vedi paragrafo 2.3.2 - Struttura fisica.

Il servizio di rilevazione presenze delle risorse umane, è configurato e gestito con applicativo software INAZ Human Energy, su server esterno INAZ il quale con certificazione standard internazionale ISO 27001 garantisce la sicurezza e la riservatezza dei dati trattati, vedi all.5 " Guida rapida Inaz IFKTalk ''</td></tr>
</table>

Apparati di Rete	
1 switch gestito marca 3com mod.baseline 2928 1 router 1 Access Point Lynksys mod.WRT54GL 1 Access Point Zyxel mod WAP3205	**RETE DI SAN DONATO MILANESE, via Sergnano n.2**
1 router/ap wireless marca Aethra 1 switch 24 p. non gestito a marca Intellinet	**RETE DI MELEGNANO, via Marsala n.6 – 3° Polo**
	RETE DI SAN GIULIANO MILANESE, via Giolitti n. 11 – 1° Polo Gli apparati di rete sono attualmente di proprietà e in carico al Comune di San Giuliano Milanese.
<u>Apparati Storage, di Backup e Sicurezza</u>	
2 HD esterni USB utilizzati per backup 1 Firewall Hardware marca Checkpoint mod Checkpoint600 1 UPS marca APC mod.smart-ups sc1000	**Sede di San Donato Milanese**
NAS Marca Buffalo mod. LS-WXL7C5	Di proprietà A.S.S.E.MI situato presso **la sede di Melegnano** utilizzato come archivio condiviso dai pc connessi in rete locale, si è proceduto all'acquisto, a cui seguirà installazione e configurazione di un sistema incrementale di Backup online (vedi allegato n.2)

Infrastruttura di Comunicazione	
1 Armadio rack situato in sala server al 1 piano 1 Armadio rack situato in locale tecnico presso gli uffici della sede in oggetto	SAN DONATO MILANESE MELEGNANO SAN GIULIANO MILANESE Proprietà e in carico al Comune di San Giuliano Milanese
Apparati Client	
15 PC desktop, 1 PC desktop presso domicilio lavoratore dipendente in telelavoro, 8 Notebook utilizzati in mobilità da personale vario	SAN DONATO MILANESE
8 PC desktop, 1 Notebook utilizzato in mobilità da personale vario	MELEGNANO
PC desktop di proprietà e in carico al Comune di San Giuliano Milanese	SAN GIULIANO MILANESE

2.3.2 Struttura fisica

Il sistema informatico dell'Ente è così costituito:

SEDE SAN DONATO MILANESE

Server "Windows 2008" con funzioni di domain controller, file server, DNS e DHCP; tale server accoglie anche l'installazione del software gestionale "CieloNext" e relativa repository costituita da un database in formato SQL.

Tutte le principali funzioni così come i servizi connessi con le attività svolte in sede si poggiano unicamente sul server.

Sono presenti 15 pc desktop facenti parte del dominio assemi.local: sulla maggior parte di essi è installato un sistema operativo Windows 7 pro, solo alcuni dei pc di recente acquisizione possiedono licenza Windows 10 pro.

E' presente un 1 PC desktop presso il domicilio di lavoratore dipendente con progetto di telelavoro per handicap, con multifunzione scanner, stampante, fotocopiatrice Brother protetto con software antivirus e collegamento a linea telefonica dati privata.

2 Stampanti di rete HP

2 Access Point dislocati tra il pian terreno ed il primo piano consentono l'accesso in wireless alla rete aziendale

Nell rete locale sono presenti anche 1 scanner di rete a marca Brother, uno scanner USB a marca HP ed un Fax.
Sono presenti n.8 Notebook utilizzati in mobilità da personale vario, con sistema operativo Windows 7 pro, solo alcuni di recente acquisizione possiedono licenza Windows 10 pro.

Attualmente il sistema informatico della sede principale non è connesso in nessun modo con le sedi distaccate

3° POLO MELEGNANO

Un NAS storage a marca Buffalo assolve all'unico compito di fileserver condiviso con gli 8 pc desktop della sede.

Degli 8 pc presenti 5 sono forniti di OS windows 7 pro e 3 di Win10 pro, è presente n.1 Notebook utilizzati in mobilità da personale vario, con sistema operativo Windows 7 pro.

Nell rete locale sono presenti anche 1 scanner di rete a marca Brother, uno scanner USB a marca HP una stampante HP di rete ed un Fax.

L'infrastruttura di Melegnano non fa parte del dominio A.S.S.E.MI. e non c'è collegamento remoto con la sede di San Donato Milanese.

1° POLO SAN GIULIANO MILANESE

Attualmente la sede in oggetto è sprovvista di un proprio sistema informatico; tutti i pc in uso così come gli apparati di rete, stampanti e quant'altro sono di proprietà del Comune di San Giuliano Milanese, ad esclusione di uno scanner Brother collegato ad un pc desktop, di proprietà A.S.S.E.MI.

Caratteristiche sedi operative

Sede	**A.S.S.E.MI. San Donato**	**A.S.S.E.MI. Melegnano**	**A.S.S.E.MI. San Giuliano Milanese**
Collegamento tra sedi	No	No	No
Video sorveglianza	No	No	No
Allarme	si	si	
Anticendio	Estintori	Estintori	Estintori
VPN	No	No	No

Caratteristiche uffici

Ufficio			
Denominazione	A.S.S.E.MI.	3° Polo	1° Polo
Sede	San Donato Milanese	Melegnano	San Giuliano Milanese
Estintori	/	/	/
Accesso	Ingresso sede	Porta chiusa a chiave	Porta chiusa a chiave
Armadi chiusi a chiave	/	/	/
Allarme	vedi sede	vedi sede	vedi sede
Cassaforte	si	no	si
Video sorveglianza	no	no	no

Caratteristiche armadio di rete

Armadio di rete		
Denominazione	Armadio Rete San Donato Milanese	Armadio Rete Melegnano

Ubicazione	/primo piano (sala server)	Primo piano (loc.tecnico)
Dimensioni	/	/
Accesso	Chiuso a chiave	Liberamente accessibile
Collegamento tra armadi	nn	nn
UPS	si	nn
Raffreddamento	nn	nn
Ignifugo	nn	nn
Posizione (terra, appeso, ecc)	terra	appeso

Caratteristiche connettività

Connettività	**San Donato**	**Melegnano**	**San Giuliano**
Denominazione	Alice Ready 20M		nn
Tipologia	ADSL		nn
DL	17 Mbps	nn	nn
UL	0,70 Mbps	nn	nn
Minimo garantito	nn	nn	nn
Gestore	Telecom	Fastweb	Telecom
Ip statico	nn	nn	nn
Voip	nn	nn	nn
Note	nn	nn	nn

Caratteristiche apparati di rete sede San Donato Mil.

Apparati di rete	Access Point	Access Point	Firewall	Switch
Denominazione	nn	nn	nn	nn
Tipologia apparato	AP	AP	Firewall	Switch
Marca e modello	Lynksys WRT54GL v1.1	Zyxel WAP3205 v2	Checkpoint 600	3COM Baseline 2928-SFP Plus
Numero porte	1x 10/100 WAN, 4x 10/100 Switched LAN	2 x 10/100 Mbps Ethernet RJ-45 ports with auto MDI/MDIX support	8 x 1 GbE LAN, 1 x 1 GbE DMZ, 1 x 1 GbE WAN Interface	24 × 10/100/1000B ase-T autosensing Ethernet ports + 4 GE SFP interfaces
Velocità porte	10/100	10/100	10/100/1000	10/100/1000
Ubicazione	1°piano/armadio rack- San Donato	Pianterreno-sala riunioni- San Donato	1piano/armadio rack San Donato	1piano/armadio rack San Donato
VPN	nn	nn	nn	nn
Vlan	nn	nn	nn	nn
DMZ	nn	nn	nn	nn

Moduli attivi	nn	nn	nn	nn
Regole e porte configurate	nn	nn	nn	nn
UPS	nn	nn	nn	nn
Gestione esterna	nn	nn	nn	nn
Bilanciamento	nn	nn	nn	nn
Failover	nn	nn	nn	nn

Apparati di rete	Router/Access Point	Switch
Denominazione	nn	nn
Tipologia apparato	Router/Access Point	switch
Marca e modello	Aethra	Intellinet
Numero porte	nn	24
Velocità porte	nn	nn
Ubicazione	1 piano locale tecnico-San Donato Mil.	1 piano locale tecnico-San Donato Mil.
VPN	nn	nn
Vlan	nn	nn
DMZ	nn	nn
Moduli attivi	nn	nn
Regole e porte configurate	nn	nn
UPS	nn	nn
Gestione esterna	nn	nn
Bilanciamento	nn	nn
Failover	nn	nn

Caratteristiche gruppo di continuità

Gruppo di continuità	UPS
Denominazione	UPS
Ubicazione	Armadio rack 1 piano San Donato Milanese
Apparati collegati	serverassemi /
Potenza	600Watts
Periodicità test e controllo	nn
Gruppo elettrogeno	nn
Montaggio	Base armadio

Caratteristiche storage 3° Polo-Melegnano

Storage	
Denominazione	Nas 3 polo
Tipologia	NAS
Marca e modello	Buffalo LS-WXL7C5
Numero dischi	2
Raid	1
Capacità totale/libero	500 GB /
Tipologia dischi	2*500 GB Sata
Ubicazione	Melegnano 3polo
Montaggio	Armadio rack
Numero porte di rete	1
Velocità porte	10/100
Modalità aggiornamento	Manuale
Periodicità aggiornamento	Annuale
UPS	nn
Gestione esterna	nn

Caratteristiche server SEDE SAN DONATO MIL.SE

Server	
Denominazione	serverA.S.S.E.MI.
Tipologia	Server Fisico
Marca e modello	IBM system x3650 M2
Ubicazione	Sala server San Donato 1°piano
Processori	Intel Xeon E5520 2,27 GHz
Ram	6 GB
Spazio disco totale	C: 78 GB, D:1,46 GB F:198 GB,G 278 GB
Programmi installati	Gestionale CieloNext
Schede di rete e velocità	10/100
Sistema operativo	Windows 2008 Standard x32
Numero alimentatori	1
Funzioni	DC, File server, DHCP, DNS, Gestionale CieloNext
Assistenza	Adelante Dolmen
UPS	si

Caratteristiche elaboratori

Elaboratori			
Denominazione	Assemi-San Donato Milanese	Melegnano 3° Polo	San Giuliano Milanese 1° Polo
Quantità	16	8	nn
Sistema operativo	12 Windows 7 pro 4 Windows 10 pro	5 Windows 7 pro 3 Windows 10 pro	nn
UPS	nn	nn	nn
Note	nn	nn	nn

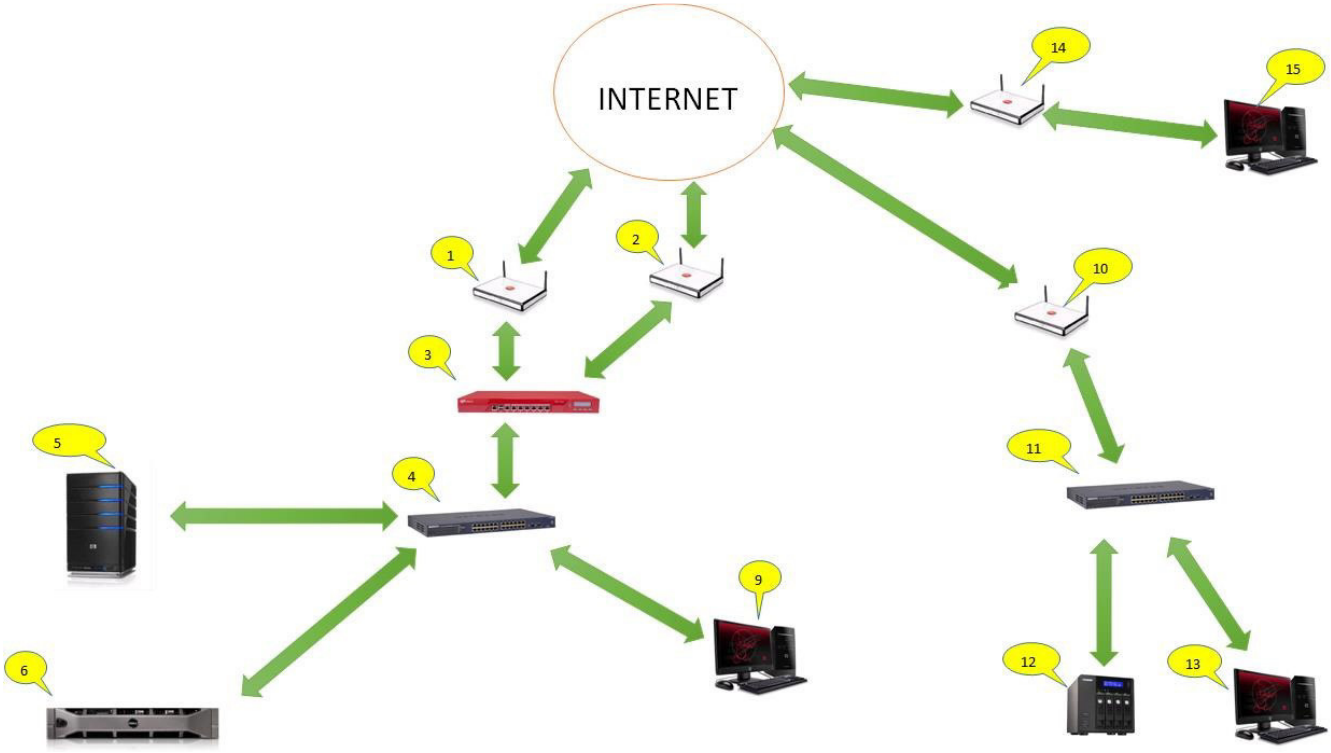
Caratteristiche linee analogiche

Linee Analogiche	
Denominazione	Borchia 1
Tipo linee	Analogica
Ubicazione	A.S.S.E.MI. 1
Gestore	Telecom

Caratteristiche centralino

Tipologia	Centralino
Marca e modello	Alcatel
Linee	4 linee fonico + 1 fax
Ubicazione	Ufficio Apparati Sede 2
Montaggio	A parete
UPS	no

Descrizione grafica dell'infrastruttura A.S.S.E.MI.



1	Router 3
2	//////
3	//////////
4	/////////
5	//////////
6	//////////
9	//////////////
10	//////////////
11	//////////////
12	//////////
13	//////////////
14	//////////////
15	//////////////////////

Tutti i servizi facenti capo alla sede di San Donato Milanese sono installati sull'unico server e viene fatto un backup giornaliero su dischi Usb che vengono ruotati settimanalmente (i 2 dischi vengono alternativamente collocati nella cassaforte situata in ufficio amministrazione di San Donato Milanese). La connettività è gestita tramite firewall Watchguard. A San Donato è disponibile anche

una connessione wireless ad uso esclusivo interno. Il servizio di posta elettronica è gestito da fornitore esterno Progetti di Impresa s.r.l. Le due sedi distaccate, il terzo polo di Melegnano e l'ufficio minori del comune di San Giuliano Milanese sono forniti di connettività propria ed indipendente: per quanto riguarda gli uffici di San Giuliano la connettività è fornita direttamente dal Comune che la gestisce tramite il personale IT interno. Ad eccezione della sede principale di San Donato Milanese le reti di Melegnano e San Giuliano non sono protette da sistemi perimetrali di difesa (Firewall Hardware)

2.3.2.1 PEC

Per quanto concerne la PEC si rimanda alle indicazioni contenute nel Manuale di Gestione del Protocollo Informatico agli art.3.3 - Ricezione dei documenti su casella istituzionale (PEC) e art.3.4 – Altre caselle di posta elettronica certificata.

2.3.3 Architettura applicativa

Nel presente paragrafo descriviamo i principali software applicativi ed utilità in uso presso A.S.S.E.MI. esplicitandone le caratteristiche salienti.

Dal punto di vista della architettura applicativa possiamo distinguere le seguenti categorie:

a) Software centralizzati: trattasi di applicativi in uso a livello A.S.S.E.MI. installati in unica posizione, su server presso la sala server A.S.S.E.MI., in uno degli ambienti virtuali di cui al precedente paragrafo, oppure resi disponibili da enti esterni e usufruibili da A.S.S.E.MI. via Web. Quasi sempre la architettura elaborativa è a 3 livelli, composta da un database server, da un application (e web) server con accesso dei client via Web tramite la Intranet A.S.S.E.MI..
b) Software stand-alone: in questa categoria intendiamo software installati localmente sulle postazioni di lavoro, essenzialmente ai fini della produttività personale.

2.3.4 Sistema di Conservazione

Per quanto concerne il sistema di conservazione si fa rimando a quanto dettagliato nel Manuale di Gestione all'art.10.2 – Conservazione dei documenti informatici del protocollo Informatico e gestione documentale.

Si specifica che i documenti contabili, fatture elettroniche verso la PA, generati tramite applicativo informatico Fatel di Zucchetti S.p.A. e le fatture elettroniche ricevute dai fornitori tramite SDI sono conservate digitalmente a norma con il sistema di conservazione sostitutiva Infinity di Zucchetti

S.p.A., con caricamento manuale sul portale Zucchetti all'indirizzo hpttps://conservazionedigitale.zucchetti.it, come dettagliato nell'allegato manuale (all.n.3).

3 Politiche organizzative della sicurezza

3.1 Generalità

La definizione e l'applicazione delle politiche di sicurezza all'interno di A.S.S.E.MI. richiedono l'individuazione di un insieme di regole che fanno riferimento alle tecnologie usate, alle metodologie, alle procedure d'implementazione e ad altri elementi specifici dell'ambiente e del sistema informativo.

L'applicazione delle politiche di sicurezza all'interno di A.S.S.E.MI. richiede, inoltre, la definizione di processi che descrivano gli specifici passi operativi che le persone devono seguire per raggiungere gli obiettivi che sono stati stabiliti. I processi sono indispensabili per la gestione di tutti gli oggetti legati alla sicurezza.

Attualmente, l'individuazione della politica di sicurezza A.S.S.E.MI. determina il modello logico della sicurezza fissandone gli obiettivi. L'individuazione degli obiettivi di sicurezza si traduce in obiettivi del sistema informativo, sostanziandosi con la formalizzazione di norme organizzative e standard di riferimento. Inoltre, la sicurezza viene considerata da tutto il personale, una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione. Un sistema di sicurezza, per poter raggiungere i migliori risultati funzionali, va visto globalmente, negli aspetti fisici, logici e organizzativi, come un insieme di misure e strumenti hardware, software, organizzativi e procedurali integrati fra loro, volti a ridurre la probabilità di danni a un livello accettabilmente basso e ad un costo ragionevole.

3.1.1 Backup

SEDE DI SAN DONATO MILANESE

I principali dati elaborati dall'ente presso la sede in oggetto sono salvati nella memoria centrale del server (serverassemi); l'intero contenuto degli HD del server stesso è criptato tramite servizio proprietario Microsoft (bitlocker) e ad ogni riavvio del server è necessaria la pen drive USB sulla

quale è contenuta l'apposita chiave di decriptazione del contenuto degli HD per poter accedere al server ed al suo contenuto. Il processo di backup avviene tramite Windows Server Backup 2008 e la destinazione dei backup sono 2 dischi USB utilizzati alternativamente a rotazione (il disco non utilizzato viene messo in cassaforte situata nell'ufficio dell'amministrazione). La rotazione dei dischi è affidata al personale amministrativo della sede.

SEDE DI MELEGNANO – 3° Polo

I dati utilizzati e condivisi della sede in oggetto risiedono unicamente sul NAS utilizzato come File server: ad oggi la sede è ancora sprovvista di un servizio di backup specificatamente predisposto. Si è proceduto all'acquisto, a cui seguirà installazione e configurazione di un sistema incrementale di Backup online (vedi allegato n.2).

UFFICI DI SAN GIULIANO MILANESE – 1° Polo

Non essendo gli uffici dotati di un sistema informatico proprio né di nessuna attrezzatura informatica di proprietà non esistono attualmente backup in rete locale ne tantomeno un archivio condiviso per i dati che risiedono esclusivamente sui singoli pc utilizzati dagli operatori. E' stata valutata la possibilità di installare un server di proprietà A.S.S.E.MI. a San Giuliano Milanese, si è proceduto all'acquisto, a cui seguirà installazione e configurazione (vedi allegato n.1).

3.2 Sicurezza logica

3.2.1 Introduzione

La sicurezza logica si occupa della protezione dell'informazione, dei dati, dei documenti, delle applicazioni, dei sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. La realizzazione della sicurezza logica è pensata in termini architetturali e ciò comporta l'individuazione di tutti i sistemi hardware e software che implementano le attività dei vari servizi aziendali, in modo tale da garantirne la fruibilità nel tempo, che deve essere nel contempo aperta a tutti gli operatori necessari, ma limitata alle funzioni ad essi attribuite in un determinato momento.

3.2.2 Sistema di autenticazione

La credenziale di autenticazione consiste in un codice per l'identificazione dell'Incaricato (utente), associato a una parola chiave riservata e conosciuta solamente dal medesimo. **La parola chiave è composta da almeno otto caratteri (numeri e lettere) e non contiene riferimenti agevolmente riconducibili all'Incaricato, il quale provvederà a modificarla al primo utilizzo**. Le credenziali di autenticazione sono affidate al controllo del ***Server "Windows 2008"*** che garantisce l'applicazione delle politiche di protezione e sicurezza in forma centralizzata ed automatizzata. La politica di centralizzazione del sistema informativo si appoggia al sistema integrato di *active directory* ("insieme di servizi di rete - *account* utente, *account computer*, cartelle condivise, stampanti, *etc*. - adottati dai sistemi operativi organizzati in modo da consentirne la condivisione da parte dei *client*") tramite apposita profilazione degli utenti (gestione dei profili di autorizzazione). Ad integrare la protezione sul sistema informativo, i *software* dell'Ente e gli applicativi *web* sono dotati di apposite procedure di accesso tramite *username* ("nome con il quale l'utente viene riconosciuto da un *computer*, da un programma o da un *server*") e *password* ("sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa informatica"). Lo *username* è un identificativo che, insieme alla *password*, rappresenta le credenziali per accedere alle risorse informatiche o ad un sistema.

Per tutti gli applicativi allocati su server esterni vengono seguite le medesime procedure di autentificazione sopra indicate.

3.2.3 Antivirus e similari

Il sistema informatico dell'Ente e i dati personali da esso custoditi sono protetti contro il rischio di intrusione e contro l'azione di programmi di cui all'Articolo 615-*quinquies* del Codice Penale ("*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*"), mediante l'attivazione:

- *software antivirus "Webroot SecureAnywhere"* per il *Server "Windows 2008"* e i singoli elaboratori, inclusa la sede di Melegnano.

I sistemi operativi degli elaboratori sono periodicamente aggiornati automaticamente mediante *Windows Update* con le opportune *patch* di sicurezza ("programma o parte di programma che aggiorna e corregge un *software*"); Il Server di San Donato Milanese viene invece aggiornato manualmente dall'azienda incaricata – Ad Adelante Dolmen s.c.s. - di fornire l'assistenza tecnica, la procedura viene effettuata o da remoto o durante le uscite in assistenza.

Gli aggiornamenti dei programmi per elaboratore volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne difetti sono stati correttamente installati. I programmi sono stati impostati in modo da scaricare e aggiornare automaticamente le loro funzionalità garantendone quindi sempre la massima efficacia di funzionamento.

Al fine di prevenire intrusioni dall'esterno è stato installato e configurato presso San Donato Milanese un *firewall hardware "Checkpoint 600"* e su ciascun elaboratore è attivato il *firewall software* integrato nel sistema operativo *"Windows"*. Attualmente l'efficacia della protezione offerta dal Firewall è però limitata dal fatto che per la maggior parte dei servizi aggiuntivi configurabili non è attivo un canone/abbonamento per i pacchetti di protezione aggiuntiva (Antivirus Firewall, Application Control, url filtering , anti bot, anti spam). E' in corso la valutazione della migliore soluzione di aggiornamento del sistema firewall.

4 Documenti e Banche dati

4.1 Sistema di gestione informatica dei documenti

Il DPR 445/2000, all'art. 1, comma 1, lett. r) definisce il Sistema di Gestione Informatica dei Documenti come *"l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti"*. Tale sistema è attivato da A.S.S.E.MI. su tutte le postazioni di lavoro degli uffici afferenti all'AOO e le abilitazioni all'utilizzo delle sue funzionalità sono stabilite e aggiornate a cura del Responsabile – Direttore Generale di A.S.S.E.MI., unico dirigente dell'organizzazione, della gestione documentale e dei sistemi informativi. Per quanto concerne i software attraverso i quali viene registrato e gestito il patrimonio documentale dell'ente si fa riferimento alle indicazioni contenute nel manuale di gestione così come anche per i seguenti argomenti:

- Protocollo informatico;
- Formazione dei documenti;
- Formati adottati;
- Sottoscrizioni;
- Validazione temporale;
- Metadati;
- Trasmissione dei documenti;
- Conservazione.

Si specifica che il sistema contabile di A.S.S.E.MI Ad Hoc Revolution, integrato con il software Fatel per la fatturazione elettronica e comunicazioni IVA, è gestito tramite applicativi web collocati in server farm con contratto di hosting con fornitore esterno Zucchetti S.p.A. e Zucchetti Informatica, vedi all. n.4 "SLA Data Center di Zucchetti S.p.A."

Il servizio di posta elettronica, il sito web aziendale e la cartella sociale distrettuale sono gestiti tramite fornitore esterno Progetti di Impresa s.r.l., vedi paragrafo 2.3.2 - Struttura fisica.

Il servizio di rilevazione presenze delle risorse umane, è configurato e gestito con applicativo software INAZ Human Energy, su server esterno INAZ il quale con certificazione standard internazionale ISO 27001 garantisce la sicurezza e la riservatezza dei dati trattati, vedi all.5 "" Guida rapida Inaz IFKTalk ''

5 Trattamento dei dati personali - Analisi dei rischi

Per quanto concerne le politiche inerenti il trattamento dei dati personali e l'analisi dei rischi incombenti sui dati ed i documenti si fa esplicito rimando alle disposizioni aziendali sulla Privacy e politiche di sicurezza, vedi determinazione direttoriale n. 126 del 18/05/2018 con oggetto "Adeguamento disposizioni normative Privacy GDPR 679/16".

ALLEGATO N.1

A.S.S.E.MI.- Prot. N. 2886 del 22/05/18

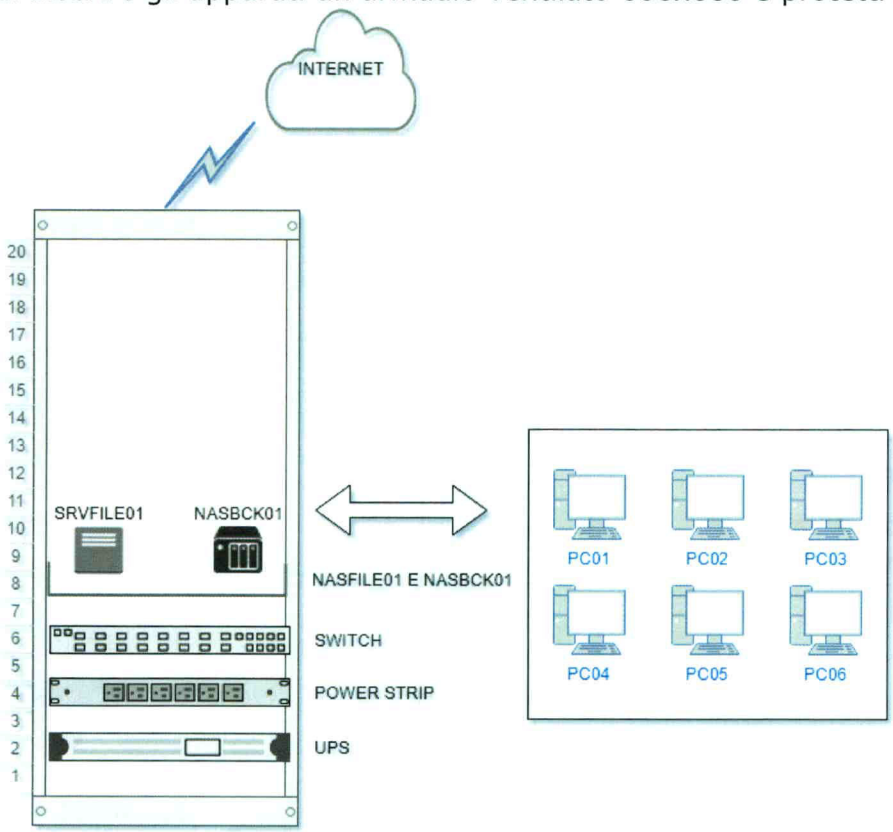
ADELANTE DOLMEN
SOLUZIONI INFORMATICHE A MISURA D'UOMO

Milano 18/05/2018

Spett.le A.S.S.E.M.I.
Via Sergnano,2
20097 San Donato Milanese
Milano

OGGETTO: vendita HW e SW per la sede di San Giuliano

La presente proposta commerciale è relativa alla rete informatica del Centro minori di San Giuliano. In questa sede sono presenti 10 PC attualmente non collegati alla rete comunale.
Vi presentiamo questa proposta per la migliore organizzazione e messa in sicurezza della rete locale, in modo da predisporre il sistema per il rispetto delle norme della Privacy.
Vista la difficoltà di connessione con la sede e considerando la limitazione della banda, che da test si aggira intorno a 1,5 Mbps, si propone un sistema per le autenticazioni in locale, con la creazione di un nuovo dominio "centrominori.local".
Il sistema si basa su un Server HP con Windows Server 2016 Standard che gestirà la rete e servirà da archivio, il NAS sarà utilizzato per il backup.
La sicurezza viene garantita cifrando il server con tecnologia BitLocker e Pendrive USB che contiene la chiave, come già in uso nella sede principale.
Sul server sarà installata la gestione Antivirus.
Si propone di inserire gli apparati un armadio ventilato 600x600 e protetti da UPS.



Adelante Dolmen scs ONLUS
Via Lombardini 13 20143 Milano
Tel 02.30328229 – 02.32167001 Fax 02 3032 8230
Codice fiscale – P. Iva – Registro Imprese di Milano 12237260158
www.adcoop.it

ADELANTE DOLMEN
SOLUZIONI INFORMATICHE A MISURA D'UOMO

Descrizione	Codice	Q.tà	P. u.	P. Tot.
HPE MICROSEVER GEN10 X3216	873830-421/PRO	1	462,00 €	462,00 €
HP 1TB 6G SATA 3.5IN NHP MDL	801882-B21	2	184,50 €	369,00 €
HP TPM MODULE 2.0 KIT	745823-B21	1	35,10 €	35,10 €
Transcend USB KEY 4GB	TS4GJF370	2	7,28 €	14,55 €
NAS QNAP TS-231P	TS-231P	1	226,91 €	226,91 €
HDD WD 2TB RED	WD20EFRX	2	102,00 €	204,00 €
RIELLO UPS IDR600 4min USB	IDR600	1	270,00 €	270,00 €
SWITCH - ZYXGS-1900-8	ZYXGS-1900-8	1	99,00 €	99,00 €
Cavo Ethernet CAT5 2 mt server e nas	ROS1402	4	3,30 €	13,20 €
Cavo Ethernet CAT5 3 mt - uplink	NX090501111	1	4,02 €	4,02 €
Armadio Rack 19" 600x600 15U	I-CASE AV-2115BKTY	1	330,00 €	330,00 €
Multipresa 8 Posti da Rack 19" Connettore C14	I-CASE STRIP-81V	1	26,85 €	26,85 €
Windows Svr Std 2016 64Bit Italian DVD 10 Clt	P73-07074	1	1.994,63 €	1.994,63 €
Iperius Backup Essential		1	103,50 €	103,50 €
HPE 3Y FC NBD Microserver Gen10 SVC	H7LF8E	1	118,47 €	118,47 €
Ore montaggio e installazione		4	0	0,00 €
Ore configurazione e test		4	0	0,00 €
TOTALE UNA TANTUM				**4.271,22 €**
CANONE ANNUALE				
Antivirus Webroot SecureAnyware	Webroot	11	18,90 €	**207,90 €**

Importo totale fornitura in opera(U.T.).....euro 4.271,22
Canone annuale antivirus.....euro 207,90

L'importo U.T. è fatturato alla consegna del materiale.
Il Canone annuale è fatturato con cadenza annuale anticipata.
Le ore di montaggio, installazione, configurazione e test sono state valorizzate a 0 in quanto rientranti nel contratto di manutenzione.
Pagamenti: 30gg data fattura

Tutti gli importi sono IVA esclusa.

La presente offerta si completa delle Condizioni generali di Contratto scaricabili dal sito www.adcoop.it

FIRMA E TIMBRO CLIENTE PER ACCETTAZIONE

AZIENDA SOCIALE SUD EST MILANO ★ A.S.S.E.M.I.

Adelante Dolmen scs ONLUS
Via Lombardini 13 20143 Milano
Tel 02.30328229 – 02.32167001 Fax 02 3032 8230
Codice fiscale – P. Iva – Registro Imprese di Milano 12237260158
www.adcoop.it

ALLEGATO N.2

A.S.S.E.MI.- Prot. N. 3473 del 14/06/18

ADELANTE DOLMEN
SOLUZIONI INFORMATICHE A MISURA D'UOMO

Milano 30/05/2018

Spett.le A.S.S.E.M.I.
Via Sergnano,2
20097 San Donato Milanese
Milano

OGGETTO: Offerta commerciale per servizio backup sede di Melegnano

Attualmente la sede del Terzo Polo di Melegnano è sprovvista di backup.
Per facilitare ed automatizzare la procedura di backup dei dati si propone una soluzione con archiviazione fino a 100 GB, che prevede un costo d'attivazione e un abbonamento annuale.

SCHEDA Iperius Backup Desktop

Il software economico e potente per mettere in sicurezza i tuoi dati

- Backup incrementale su NAS e dischi esterni USB
- Backup automatico e copia dei file aperti (VSS)
- Drive Image, Sincronizzazione, Backup FTP e Cloud
- Backup su Google Drive, Amazon S3, Azure Storage, OneDrive, Dropbox
- Compatibile con Windows XP, Vista, Windows 7 e Windows 8/8.1/10
- Licenza perpetua con supporto e aggiornamenti inclusi

Semplice e affidabile

Configurare un backup online dei file è estremamente semplice con Iperius. Ti basterà creare una operazione di backup (con esecuzione automatica), selezionare le cartelle e i file da trasferire, impostare il tuo account Online Storage, e decidere quante copie mantenere. Potrai inoltre ricevere notifiche email per controllare il risultato dei backup e accedere ai file in qualsiasi momento e da qualsiasi postazione o FTP Client.

Protezione estesa

Fare un backup online dei dati consente di avere una sicurezza in più nella protezione del proprio lavoro, di documenti o immagini importanti. Un backup remoto mette infatti al riparo i file da rotture hardware, disastri ambientali, e attacchi di virus di tipo ransomware (cryptolocker, teslacrypt, ecc). Grazie alla connessione sicura FTPS e alla criptazione AES 256 bit integrata, potrai avere più copie, anche incrementali, sempre al sicuro e sempre accessibili.

Adelante Dolmen scs ONLUS
Via Lombardini 13 20143 Milano
Tel 02.30328229 - 02.32167001 Fax 02 3032 8230
Codice fiscale - P. Iva - Registro Imprese di Milano 12237260158
www.adcoop.it

Descrizione	Q.tà	Costo iva esclusa
Importo U.T. (attivazione)	1	Euro 58,00
Canone annuo	1	Euro 99,00
Installazione configurazione	1	

L'importo U.T. è fatturato all'accettazione della presente proposta.
Il canone annuale è fatturato anticipatamente con cadenza annuale.
Pagamenti: 30gg data fattura

Tutti gli importi sono IVA esclusa.

La presente offerta si completa delle Condizioni generali di Contratto scaricabili dal sito www.adcoop.it

FIRMA E TIMBRO CLIENTE PER ACCETTAZIONE

AZIENDA SOCIALE SUD EST MILANO
A.S.S.E.M.I.

Adelante Dolmen scs ONLUS
Via Lombardini 13 20143 Milano
Tel 02.30328229 – 02.32167001 Fax 02 3032 8230
Codice fiscale – P. Iva – Registro Imprese di Milano 12237260158
www.adcoop.it

ALLEGATO N.3

CONSERVAZIONE INFINITY

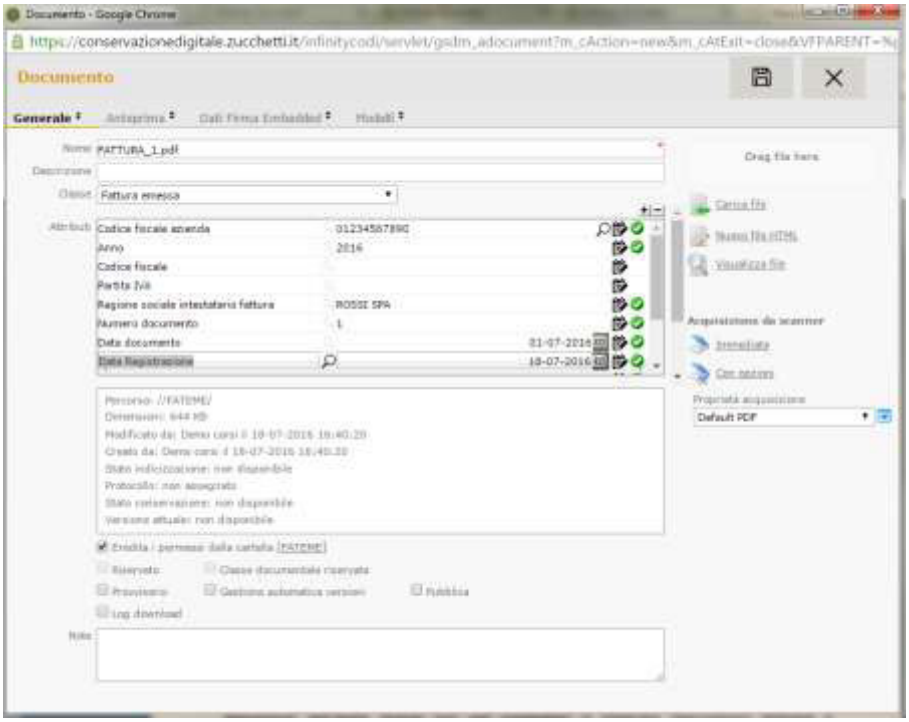
Manuale Utente

INFINITY PROJECT

ZUCCHETTI
IL SOFTWARE CHE CREA SUCCESSO

Assistenza tecnica Conservazione Digitale
sosinfinity.assistenza@zucchetti.it

Sommario



L'inserimento dei metadati avviene successivamente al caricamento nella sezione "Attributi".

Una volta inseriti i dati necessari, è possibile salvare il record.

2.2.3-Massiva

Al fine di importare massivamente i documenti è possibile procedere dal seguente punto di menù: *Area pre-ingest > Acquisizione > Massiva*. Nella finestra cui si accede è necessario selezionare la classe; tramite il pulsante "Aggiungi file" è possibile selezionare i documenti che si intendono importare.

Una volta selezionati, premendo il tasto "Upload" il programma importerà i documenti nel sistema di conservazione.

Glossario

Area documentale o pre-ingest	Area che non fa parte del sistema di conservazione. Si tratta di un insieme di funzionalità che consente al Produttore di predisporre i propri documenti informatici da inviare al sistema di conservazione
Chiusura del pacchetto di archiviazione o Chiusura della conservazione	Operazione consistente nella sottoscrizione del pacchetto di archiviazione con firma digitale apposta da un Firmatario Delegato di Zucchetti S.p.a. e apposizione di una validazione temporale con marca temporale alla relativa impronta
Classe documentale	Un insieme di oggetti e/o documenti informatici che condividono una o più proprietà quali ad esempio la tipologia, i metadati, ecc.
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Marca temporale	Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale; la marca temporale prova l'esistenza in un certo momento di una determinata informazione, sotto forma di struttura dati firmata da una Time Stamping Authority
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche e le modalità riportate nel presente Manuale di conservazione
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	Pacchetto informativo inviato dal Produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale di conservazione
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, documenti amministrativi informatici, documenti informatici rilevanti ai fini tributari, fascicoli informatici, aggregazioni documentali

	informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici
Processo schedulato	Esecuzione di un processo informatico programmato che non necessita di intervento umano. Si tratta di processi ripetitivi che iniziano in relazione a determinate modalità.
Responsabile del Servizio di conservazione	È Zucchetti S.p.a. che opera attraverso uno o più persone fisiche formalmente incaricate all'esecuzione dell'insieme delle attività finalizzate alla conservazione a norma dei documenti informatici nell'ambito della fornitura del servizio di conservazione erogato ai propri clienti

1-Introduzione

Obiettivo del presente manuale è fornire le indicazioni necessarie alla fruizione, nelle sue principali funzionalità, del sistema di Conservazione Digitale realizzato con tecnologia Infinity Zucchetti.

1.1-Gestione del servizio

Il processo di conservazione prevede delle chiusure con cadenza regolare tramite un processo di schedulazione automatico; di conseguenza, i documenti trasmessi, anche in virtù della firma digitale apposta, si intendono definitivi. È consigliabile, quindi, effettuare gli eventuali controlli di congruità contestualmente all'acquisizione dei documenti nel sistema di conservazione.

Il servizio dispone, comunque, di funzioni di ricerca, estrazione, report e cancellazione che consentono l'operatività in totale autonomia.

N.B. Eventuali eliminazioni di documenti, successive al processo di conservazione, non inficiano in alcun modo la conservazione degli altri documenti del medesimo Pacchetto di Archiviazione e anno contabile [Maggiori dettagli in merito al paragrafo 3.4].

1.2-Menù

Accedendo alla procedura, è possibile visualizzare in alto a destra l'azienda di lavoro e il nome dell'utente che ha effettuato l'accesso.

Il menu presenta le funzioni suddivise in **Area pre-ingest** e **Conservazione Digitale**, e alcuni link funzionali:

Mappa funzionale: per visualizzare la struttura completa del menù;

Manuale del servizio: per scaricare il manuale del servizio di conservazione di Zucchetti;

Cambio password: per effettuare la modifica della password di accesso all'applicativo;

Esci: per eseguire il logout dall'applicativo.

2-Area pre-ingest

È l'area dell'applicativo che non fa parte del sistema di conservazione; si tratta di un insieme di funzionalità che consente al Produttore di predisporre i propri documenti informatici da inviare al sistema di conservazione che provvederà ad acquisirli definitivamente tramite un processo schedulato di generazione dei Pacchetti di Versamento.

2.1-MyArea

Il servizio di conservazione mette a disposizione il pannello MyArea, dalla voce di menù *Area pre-ingest > Home Area pre-ingest*, il quale consente di monitorare la fase di acquisizione nell'ambiente di conservazione.

All'esecuzione delle suddette operazioni l'interfaccia si svuoterà segnalando "Nessun documento da lavorare", in attesa che l'utente carichi nuovi documenti.

L'interfaccia è suddivisa in diverse aree:

- Filtri : qualora nel processo di conservazione siano presenti più aziende, l'area in questione consente di selezionare (tramite ) la singola azienda sulla quale si intende operare. Con le medesime modalità, è possibile effettuare la selezione della classe documentale, quindi l'anno fiscale di competenza e, in base a quest'ultimo specificare una data limite per i documenti da considerare.

- Tree View : rappresenta la spalla sinistra della MyArea e consente di visualizzare in modo gerarchico:
  - al primo livello le Aziende che presentano documenti caricati e da conservare;
  - al secondo livello le Classi documentali delle aziende del primo livello;
  - al terzo livello gli Anni di riferimento per le classi documentali del livello precedente;
  - al quarto livello gli eventuali Sezionali gestiti nei vari anni.

- Riepilogo: rappresenta la sezione centrale della MyArea nella quale vengono esposte le informazioni relative ai documenti da processare.

La Tree View assume anche un ruolo di filtro delle informazioni visualizzate nel riepilogo; selezionando un determinato livello si otterrà, nell'area di Riepilogo, il numero di documenti aggregati per il livello successivo fino ad arrivare a visualizzare tale informazione relativamente ai singoli documenti.

2.2-Acquisizione

Il servizio di conservazione mette a disposizione le funzioni di acquisizione dei documenti dalla voce di menù *Area pre-ingest > Acquisizione*.

2.2.1-Importazione documenti

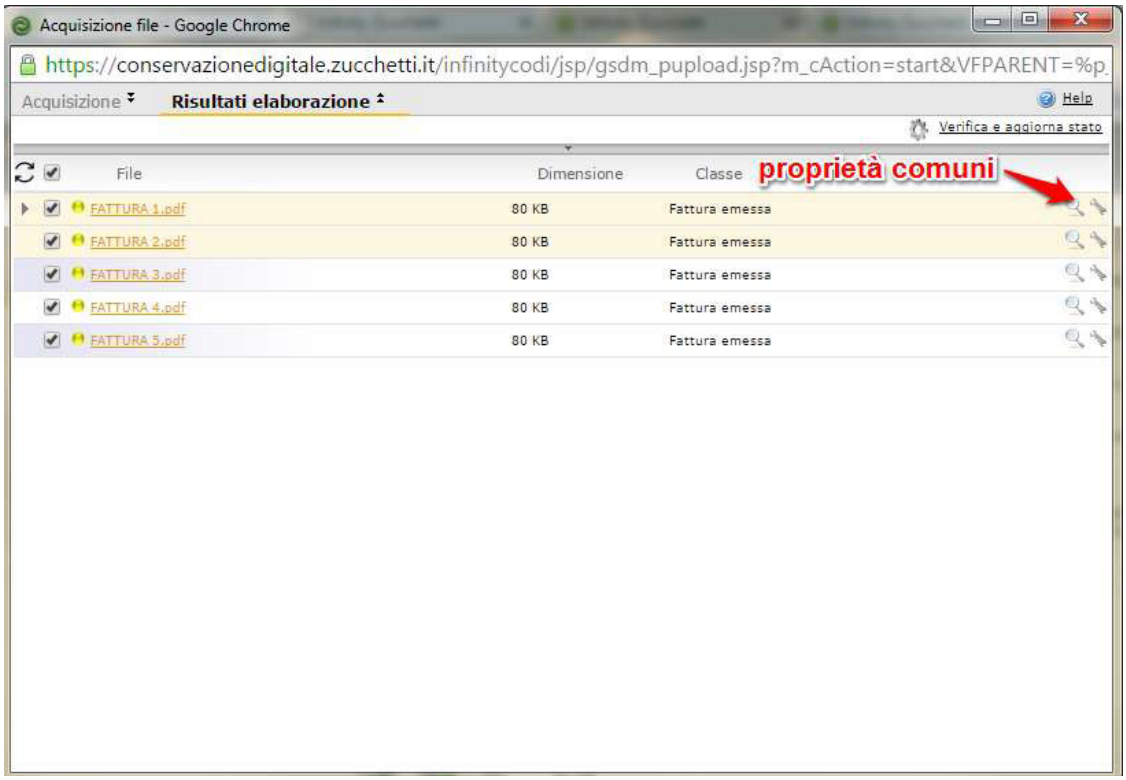
La funzionalità di importazione dei documenti è fruibile solo in determinate condizioni che devono essere concordate con il servizio di Assistenza tecnica, considerate le particolari modalità di acquisizione che in essa sono previste.

2.2.2-Singolo file

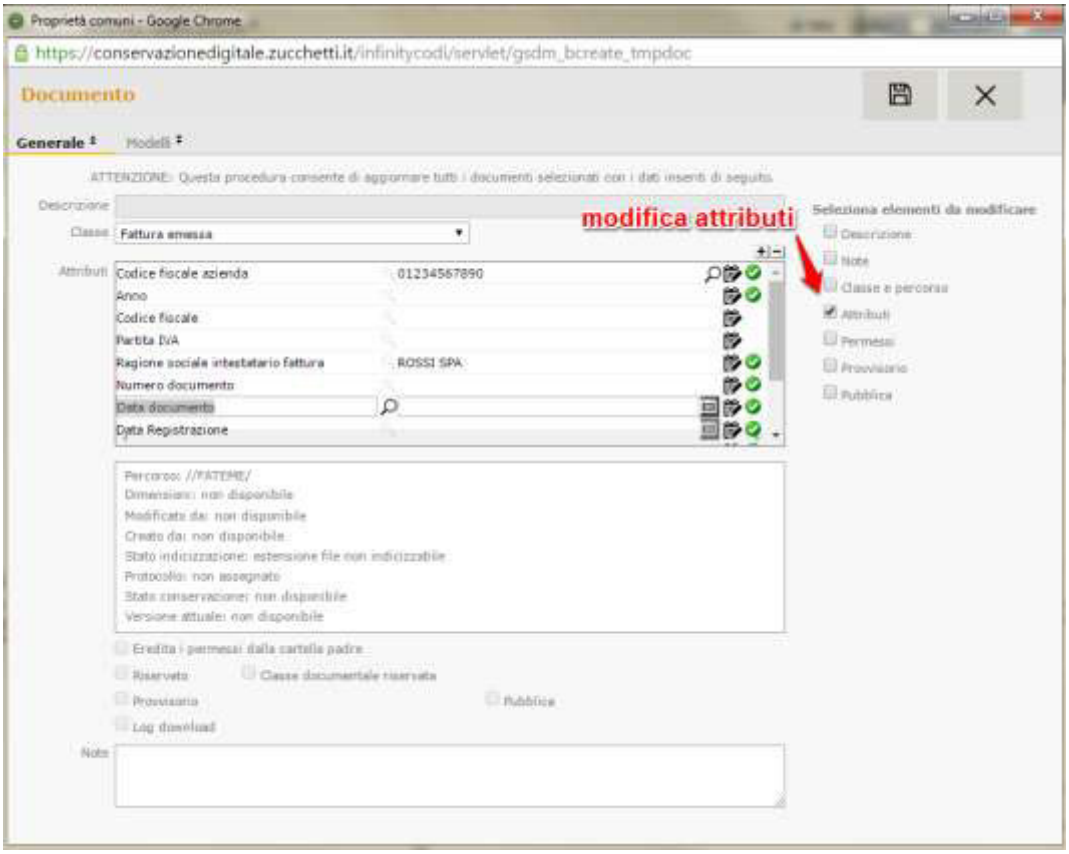
La funzionalità consente di acquisire singoli documenti, con la contestuale imputazione manuale dei metadati.

È sufficiente selezionare il file del documento ed effettuare il drag&drop nell'apposita sezione della schermata, richiamata dalla voce di menù.

Nel tab “Risultati elaborazione” sarà, quindi, possibile procedere alla modifica massiva degli attributi, selezionando tutti i file, cliccando sulla chiave inglese e andando in “Proprietà comuni”.



Selezionare l’opzione “Attributi” per modificare gli attributi comuni dei documenti; qualora non venissero compilati tutti gli attributi, sarà necessario selezionare l’opzione “Provvisorio”.



Successivamente, nel caso sia necessario, è possibile modificare gli attributi per singolo documento; completata l'operazione, sul documento deve essere deselezionato "Provvisorio" e salvato il record.

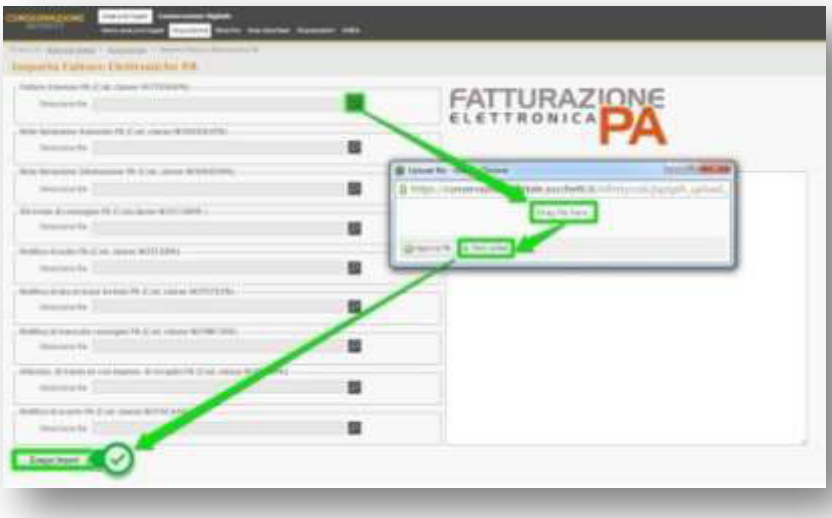
In alternativa a questa operatività, è possibile utilizzare la funzionalità "Conferma massiva documenti provvisori".

Infine, bisognerà nuovamente selezionare tutti i documenti, cliccare sulla chiave inglese e procedere con "Firma documenti".

2.2.4-Importa Fatture Elettroniche PA

Per il caricamento dei files relativi a singole fatture o a lotti di queste ultime (ossia singoli XML firmati contenenti ciascuno più fatture destinate alla medesima P.A.) e delle relative ricevute/notifiche, è necessario:

- accedere al percorso *Area pre-ingest > Acquisizione > Importa Fatture Elettroniche PA*;
- in corrispondenza delle classi documentali desiderate (in linea generale Fatture Emesse PA e Ricevuta di Consegna PA e/o Notifica di Esito PA che si consiglia di caricare contestualmente) premere sull'icona , caricare il file tramite Drag&Drop nella sezione evidenziata dall'immagine seguente (o tramite ricerca nel file system utilizzando il tasto 'Aggiungi file'), quindi, premere "Start upload":



- premere 'Esegui Import' per concludere il processo di caricamento del primo file e della relativa ricevuta (nella sezione di destra 'Log impostazione' è possibile visualizzare un riscontro dell'operazione eseguita).

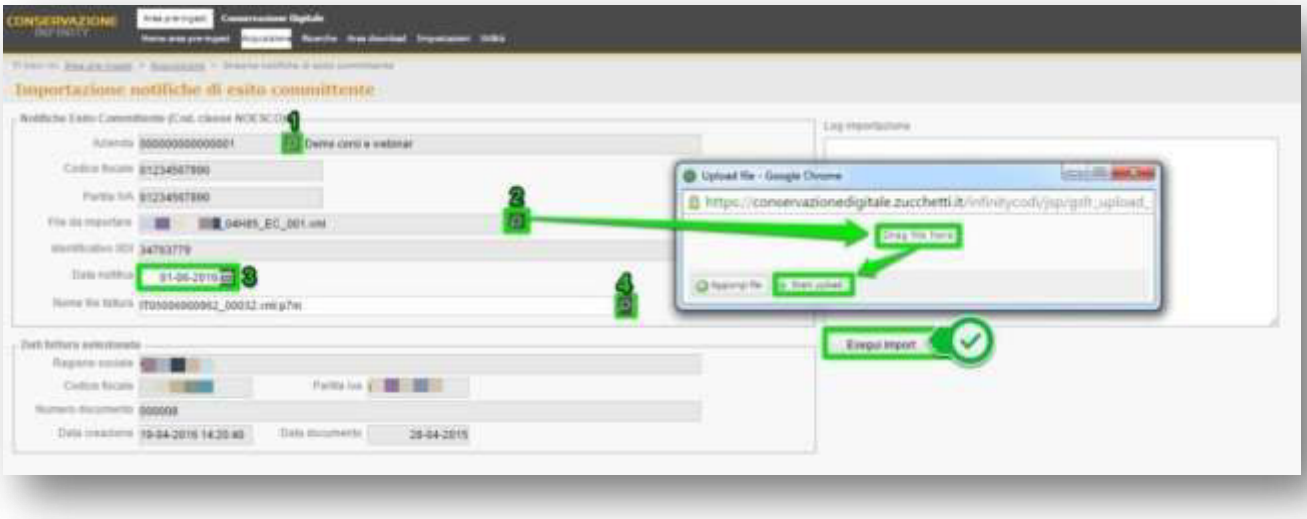
La funzionalità descritta consente di importare, contestualmente e senza l'esigenza di effettuare il data entry dei metadati (es. N° documento, Data documento, Ragione sociale intestatario, etc.), sia la fattura che la relativa ricevuta.

Una volta caricati, i documenti saranno visibili nell'interfaccia MyArea (Area pre-ingest > Home area pre-ingest) e si esauriranno così le azioni di competenza dell'utente.

2.2.5-Importa notifiche di esito committente

Solo dopo aver caricato le fatture, è possibile gestire le notifiche di Esito Committente; a tal fine è stata creata un'apposita interfaccia di importazione in quanto questo particolare tipo di file (la cui generazione e conservazione sono facoltative) non contiene informazioni con cui è agevole effettuare il collegamento alla relativa fattura. A tal riguardo è necessario, quindi, che l'utente proceda con l'inserimento di alcune informazioni e il caricamento del file:

1. Azienda del documento (precompilata con quella cui l'utente è associato di default);
2. Upload del file della notifica di Esito Committente;
3. Data della notifica (viene impostata di default la data di sistema, ma può essere modificata manualmente);
4. Nome del file della fattura (ricercabile tramite l'icona).



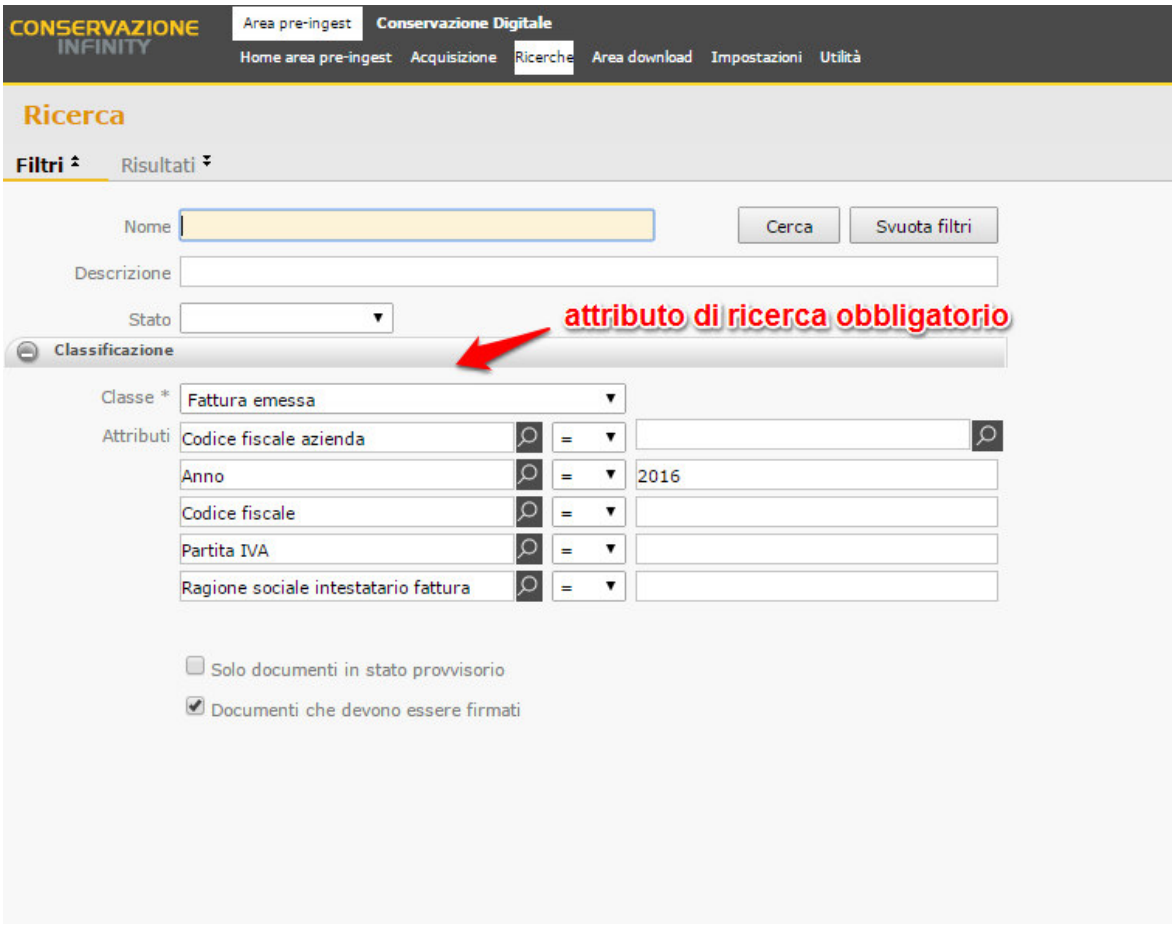
2.3-Ricerche

Nel menù "Ricerche" sono presenti le voci che consentono di effettuare interrogazioni differenti a

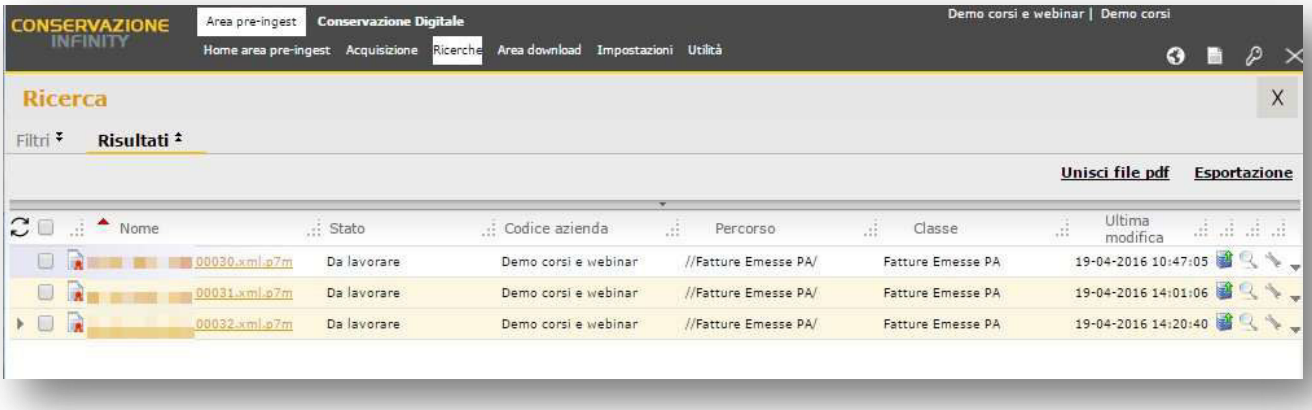
seconda delle esigenze.

“Documenti” rappresenta la scelta di menu da utilizzare qualora si abbia la necessità di interrogare il database per ottenere specifici documenti presenti nel sistema di conservazione.

Nell’interfaccia di filtro l’unico campo obbligatorio da attribuire è quello relativo alla “Classe documentale” sulla base della quale vengono proposti gli ulteriori filtri di ricerca.



Il risultato che si ottiene dall’esecuzione del processo è l’elenco di documenti che soddisfano i parametri impostati.



Per ogni documento sarà possibile, quindi, accedere ad alcune funzionalità quali:

- il download del documento in formato originario tramite le selezione del nome del file;
- la visualizzazione delle informazioni ad esso associate (🔍) quali i metadati e i riferimenti del firmatario, oltre al download del file firmato dal tab “Firma digitale” (📥);
- la visualizzazione del valore assunto dagli Attributi (o metadati) (📦);
- la visualizzazione del contenuto della fattura (o del lotto di fatture) per mezzo del foglio di stile messo a disposizione dall’Agenzia delle Entrate, selezionando 🔧 e l’opzione “Visualizza fattura PA” (nel caso di Fatture PA);
- l’eliminazione (inibita per documenti firmati).

Per esportare in formato CSV (compatibile Excel) la lista dei documenti selezionati è presente l’opzione “Esportazione” in testa alla sezione destra della griglia dei risultati.

2.4-Conferma massiva documenti provvisori

La funzionalità, disponibile dal percorso di menu *Area pre-ingest > Ricerche > Conferma massiva documenti provvisori*, consente di confermare tutti i documenti, in particolare quelli importati in modalità “Massiva” e selezionati come provvisori dopo l’assegnazione degli attributi.

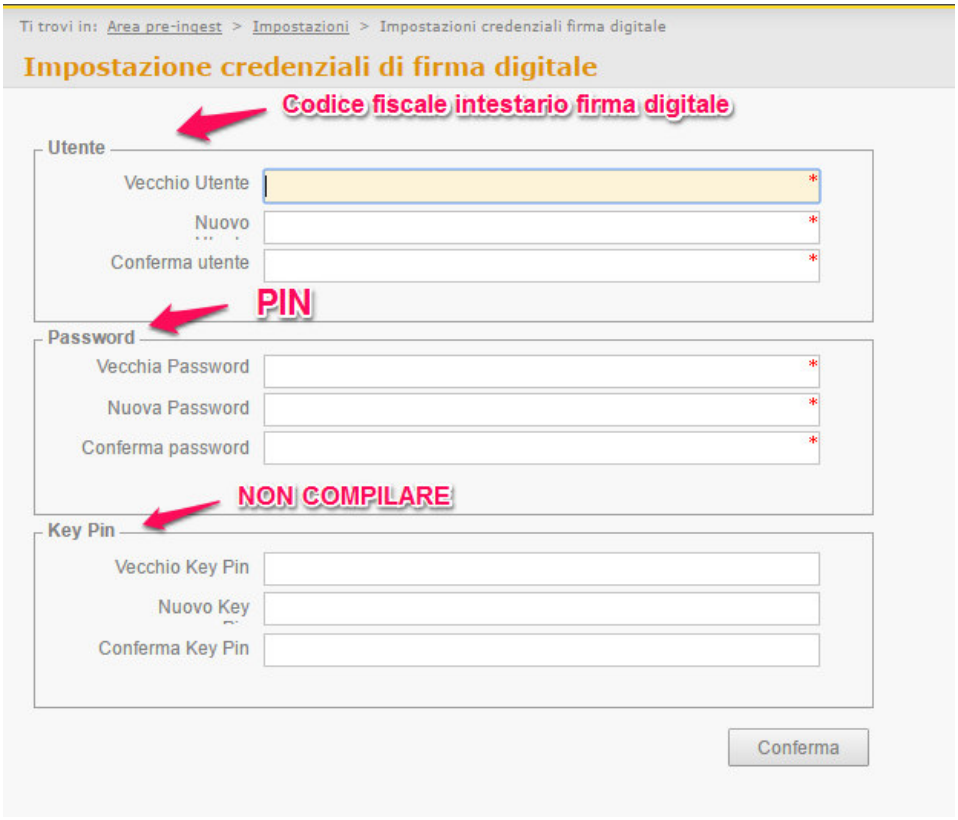
È possibile procedere indicando la classe documentale e la data di acquisizione dei documenti da confermare; per rendere più precisa la ricerca, sono disponibili ulteriori filtri per azienda, numero documento e sezionale.

A selezione effettuata, è sufficiente premere il tasto “Conferma” per eseguire l’operazione.

2.5-Impostazioni credenziali firma digitale

L’impostazione delle credenziali di firma digitale è diversa nel caso in cui l’utente attivi per la prima volta la firma HSM oppure la precedente sia scaduta e debba essere rinnovata.

Nel primo caso vanno indicate solo le credenziali del nuovo utente, mentre nel secondo anche quelle del vecchio.

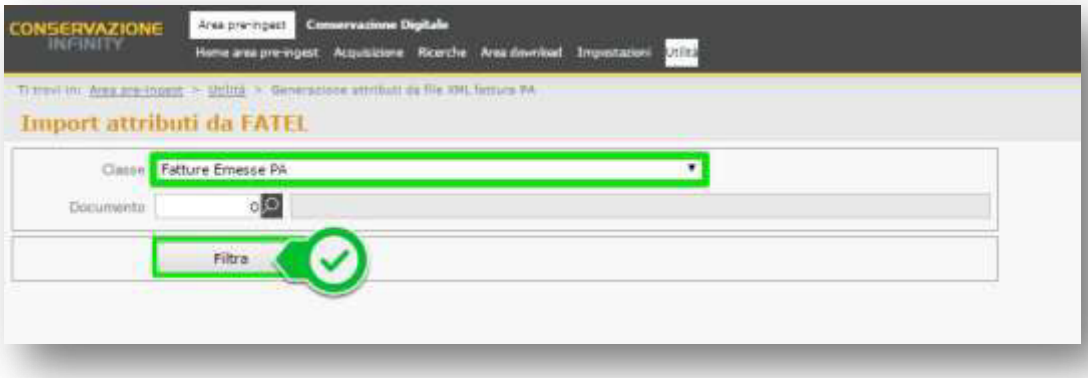


2.6-Generazione attributi da file XML fattura PA [funzione abilitata solo per determinate categorie contrattuali del servizio]

Una volta caricati i documenti PA è necessario associare agli stessi i relativi attributi.

Previa configurazione dell'utente, la funzione di lettura degli attributi provvede, contestualmente, alla generazione delle anagrafiche dei cedenti prestatori delle fatture importate.

Per procedere alla generazione degli attributi è necessario accedere al menu *Area pre-ingest > Utilità > Generazione Attributi da File XML Fattura PA* e selezionare la classe di interesse o il singolo documento; quindi, premere "Filtra".



Il programma proporrà così l'elenco di tutti i documenti privi di attributi; a questo punto basterà cliccare il tasto "Importa" affinché venga avviato il processo di rilevazione dei metadati.

Quest'ultima fase sarà da ripetere anche per le altre classi previste inerenti agli altri documenti caricati, oltre alle Fatture Emesse PA quali: Ricevuta di Consegna PA e Notifica di Esito PA.

Terminato il tutto in MyArea saranno visibili, in capo alle varie anagrafiche, i documenti da preparare importati nell'ambiente; la loro conservazione avverrà secondo la schedulazione prevista dal sistema.

3-Conservazione Digitale

È l'area dell'applicativo dove sono presenti le funzionalità proprie del sistema di conservazione.

Il servizio è demandato completamente a Zucchetti, ma l'utente ha la possibilità di eseguire alcune operazioni per reperire le informazioni riguardanti i documenti conservati e chiedere la loro eventuale cancellazione; le funzioni vengono richiamate dalla voce di menù *Conservazione Digitale > Home Conservazione Digitale*.

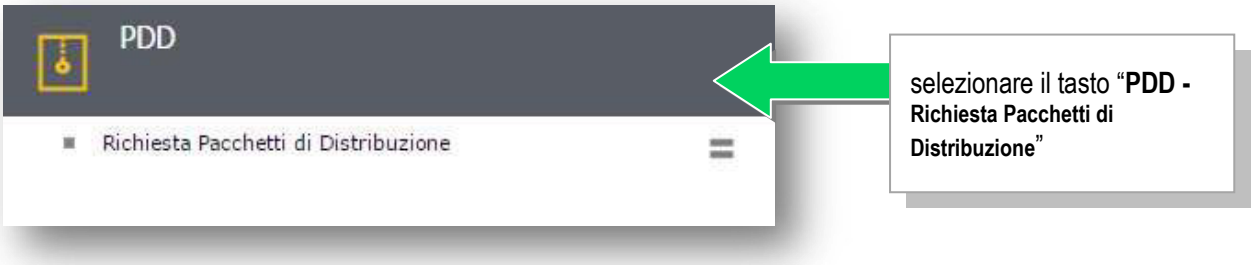
3.1-PDV e conservazione dei documenti

La creazione del Pacchetto di Versamento e la successiva conservazione dei documenti in esso contenuti sono operazioni demandate completamente a Zucchetti, che in questo modo assolve al servizio per il quale il cliente ha firmato la delega prevista dal contratto.

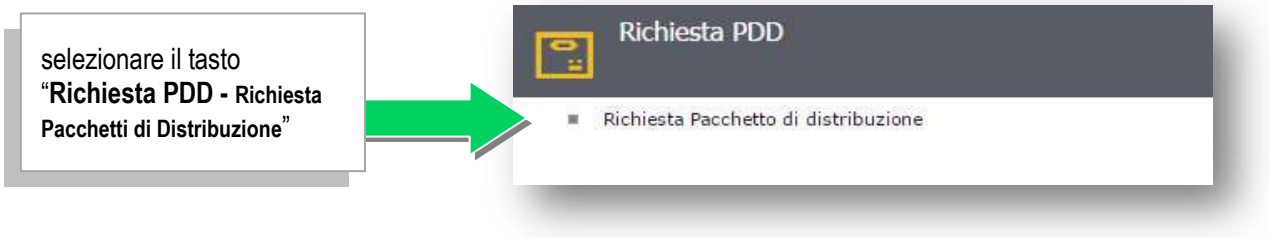
3.2-PDD

Il Pacchetto di Distribuzione è l'evidenza informatica mediante la quale un utente ha la possibilità di estrapolare dal sistema di conservazione i documenti in esso contenuti e con valenza opponibile ai terzi.

A tal fine è necessario, innanzitutto, fare richiesta del Pacchetto di Distribuzione nella prima schermata del portale:



nella videata seguente:

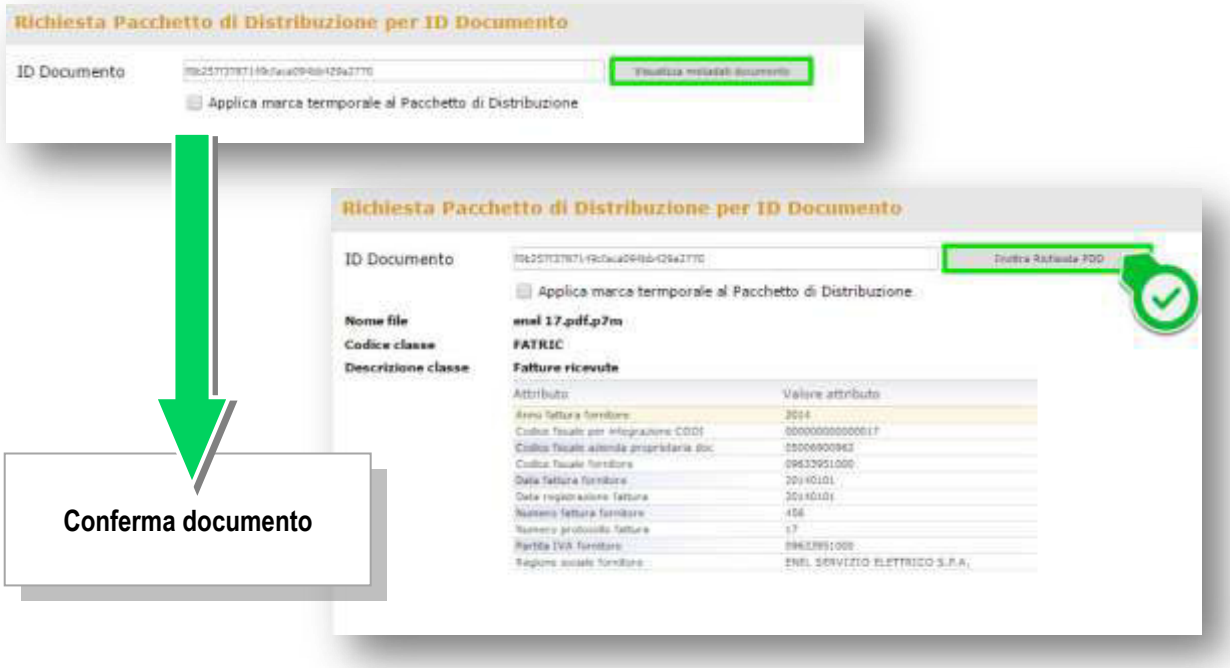


Successivamente, effettuare la ricerca dei documenti selezionando innanzitutto la Classe Documentale ed eventualmente applicando gli ulteriori filtri disponibili:

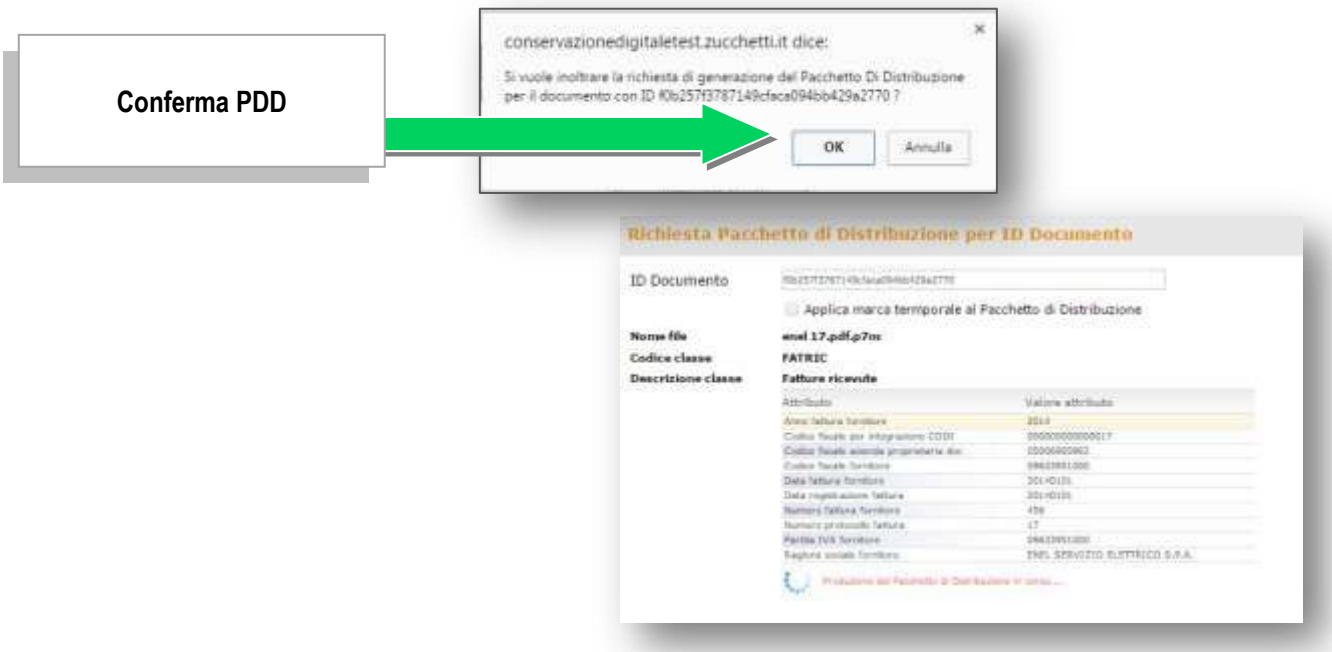
- il **nome del file** (o una sua porzione, se compilata tra simboli '%'), tramite l'apposito campo "Nome";
- gli **identificativi fiscali del soggetto** (cliente per le fatture emesse, fornitore per le fatture ricevute, contribuente per i dichiarativi);
- sulle **date dei documenti** (data documento, data registrazione, data creazione e modifica) con la possibilità di applicare dei range "da data a data";
- sul **numero protocollo** con la possibilità di filtrare "da numero a numero".

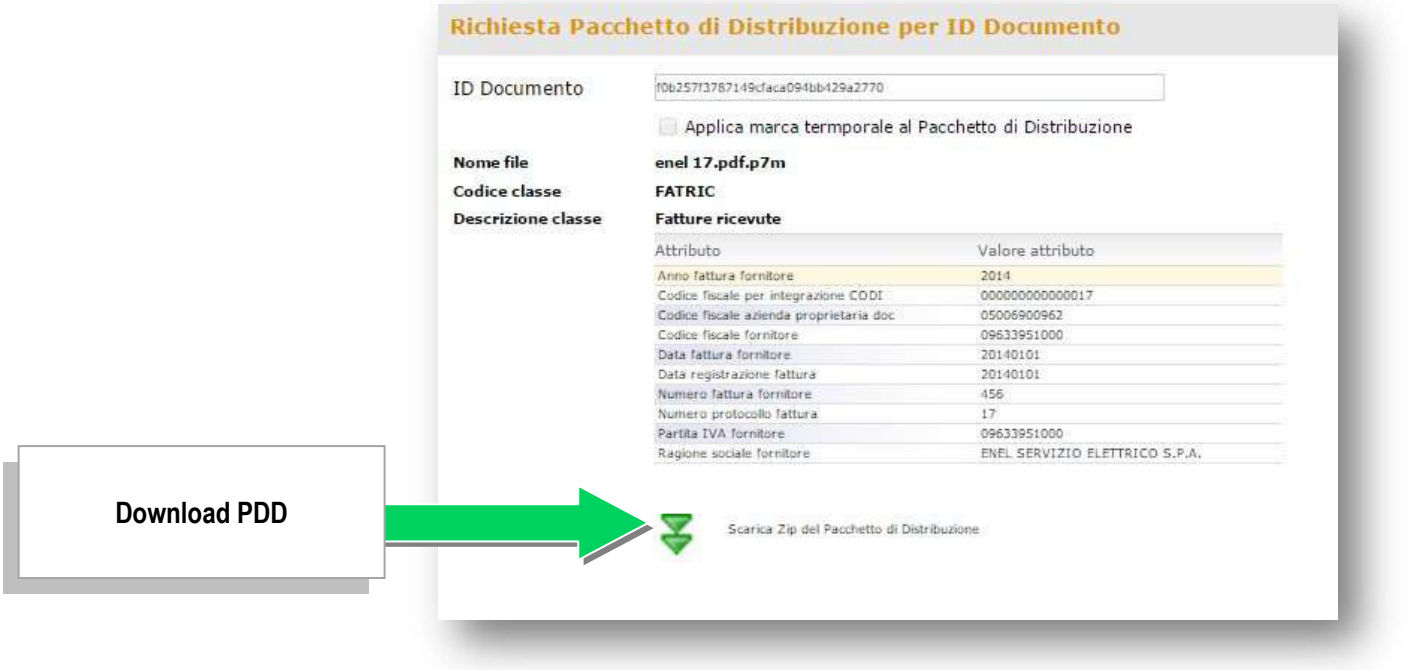
Qualora in base ai filtri applicati il risultato della ricerca corrisponda a un unico documento la procedura propone una modalità rapida di ottenimento del Pacchetto di Distribuzione.

Nella prima videata successiva è necessario premere "***Visualizza metadati documento***" in modo da ottenere i dettagli riguardanti il file; per procedere con la creazione definitiva del Pacchetto di Distribuzione è necessario, quindi, selezionare "***Inoltra Richiesta PDD***":



A questo punto il sistema chiede una conferma a procedere e a seguito di una breve elaborazione rende disponibile lo zip del Pacchetto di Distribuzione affinché sia possibile effettuarne il download tramite il tasto: "***Scarica Zip del Pacchetto di Distribuzione***"



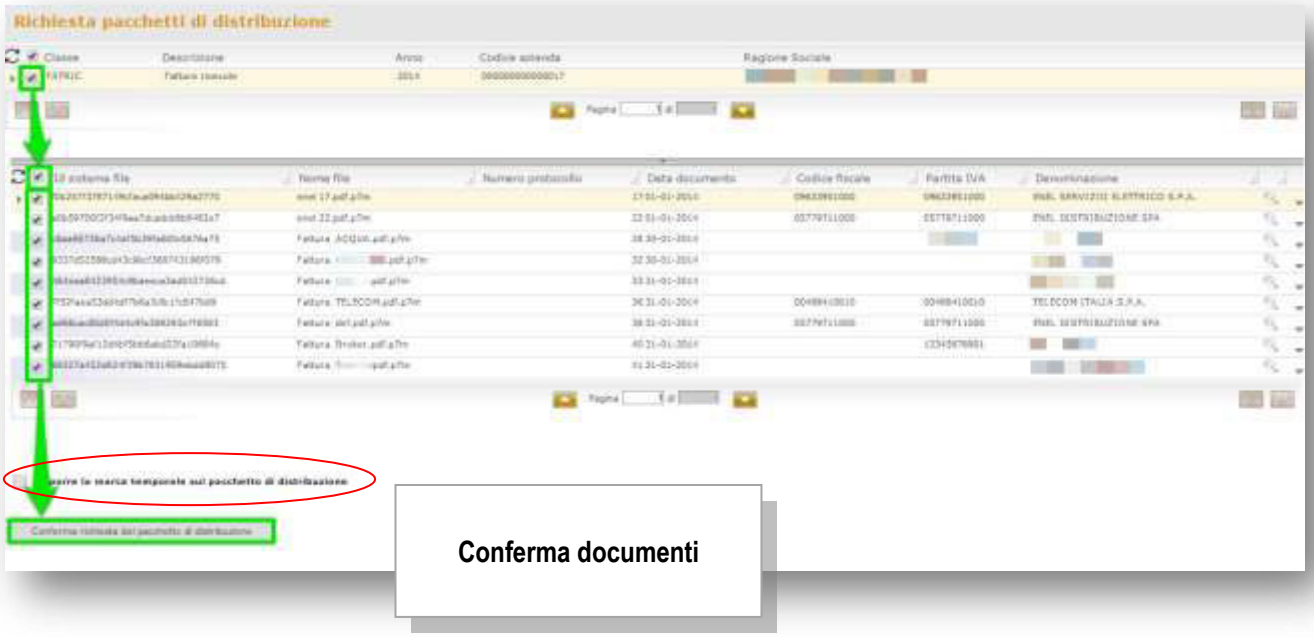


N.B. Qualora il soggetto destinatario del P.d.D. necessiti che quest'ultimo sia marcato temporalmente è possibile soddisfare la richiesta applicando la spunta alla voce "Applica la marca temporale sul pacchetto di distribuzione".

Qualora, invece, i filtri applicati conducano ad un risultato composto da più documenti la procedura da effettuare per l'ottenimento del relativo Pacchetto di Distribuzione è la seguente:

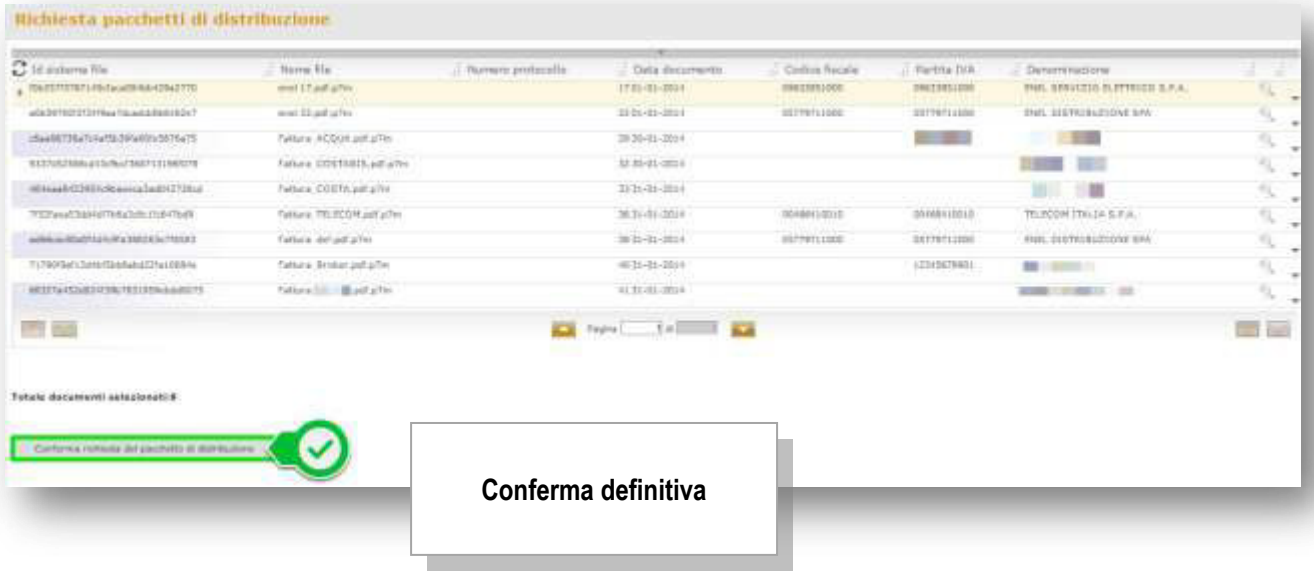
- selezionare la classe documentale di appartenenza dei documenti d'interesse e premere "Visualizza Dettagli";

- nella nuova finestra, spuntare la classe documentale per ottenere l'effettivo dettaglio dei singoli documenti che saranno inclusi nel Pacchetto di Distribuzione e premere "Conferma richiesta pacchetto di distribuzione";



N.B. Qualora il soggetto destinatario del PdD necessiti che quest'ultimo sia marcato temporalmente è possibile applicare la spunta alla voce "Applica la marca temporale sul pacchetto di distribuzione"

- per tutela dell'utente è prevista un'ulteriore conferma a fronte della quale viene inserita nel sistema la richiesta del Pacchetto di Distribuzione;



all'indirizzo mail abbinato all'utente, quindi, viene notificata la correttezza dell'operazione eseguita tramite una PEC contenente le informazioni identificative del Pacchetto di Distribuzione;

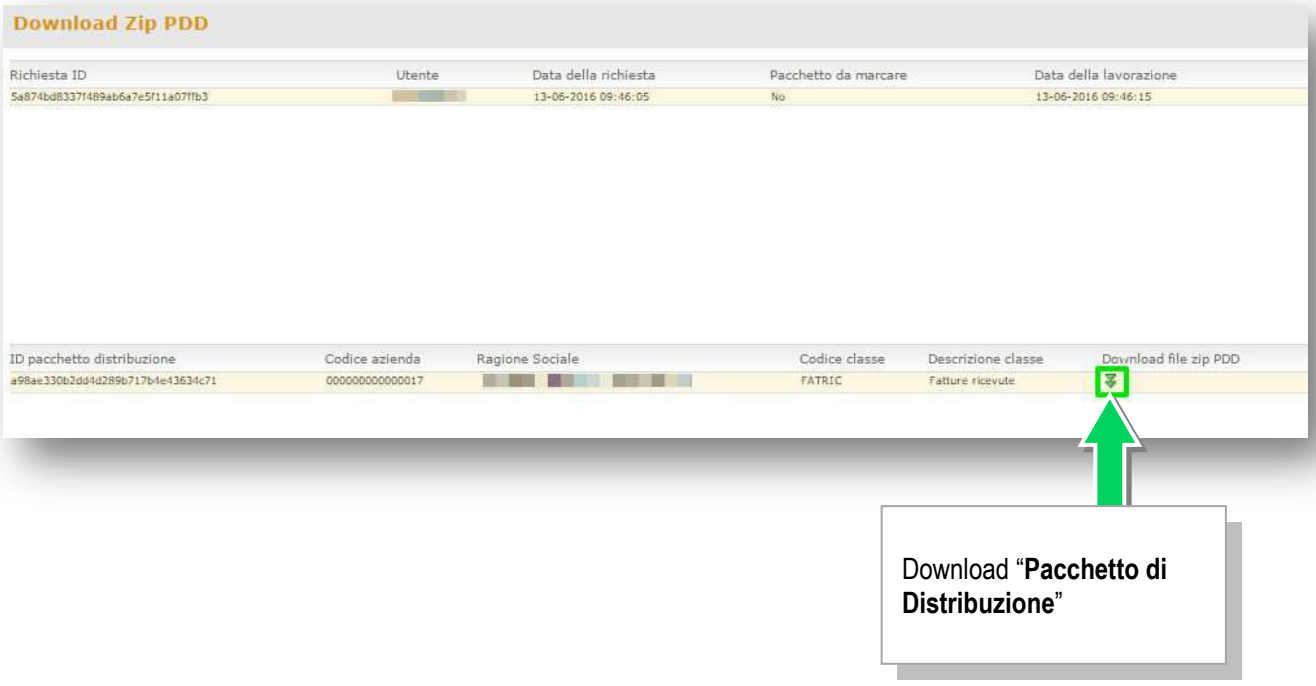
- Ricezione **della 1ª PEC di conferma** dell' inserimento nel sistema di conservazione della richiesta del Pacchetto di Distribuzione.

Il sistema di conservazione, alla ricezione di una richiesta del Pacchetto di Distribuzione per più documenti, procede alla generazione del relativo Zip. Per poter scaricare il pacchetto l'utente deve, quindi, procedere come di seguito:

- attendere la 2a PEC che avvisa della disponibilità dello Zip del Pacchetto di Distribuzione;
- effettuare il login al portale: https://conservazionedigitale.zucchetti.it/codi;
- selezionare il tasto "PDD - Richiesta Pacchetti di Distribuzione";

- accedere al menu "Download Zip PDD - Download Zip Pacchetti di Distribuzione";

- eseguire il definitivo download del file Zip del Pacchetto di Distribuzione selezionando quello di interesse e utilizzando l'apposito link evidenziato nell'immagine riportata di seguito:



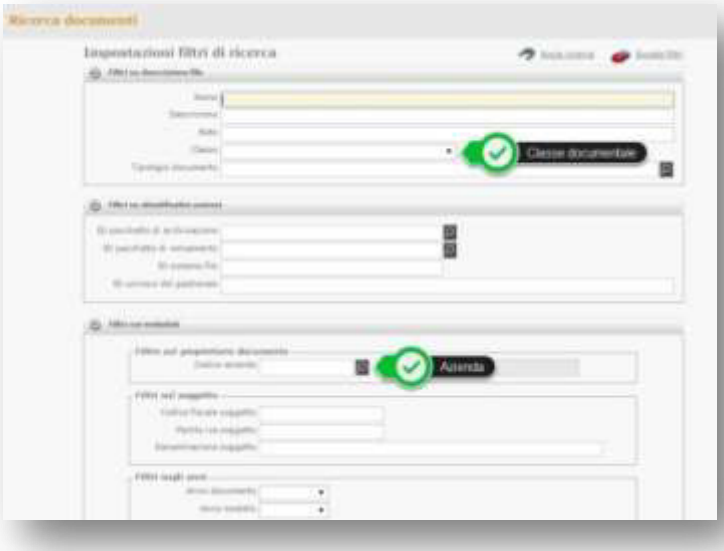
Il file identificativo del Pacchetto di Distribuzione è uno Zip contenente almeno i seguenti files:

- i documenti per cui è stata effettuata la richiesta (firmati);
- i file indice dei Pacchetti di Archiviazione nei quali i documenti sono inseriti e conservati (i file sono firmati e in formato SInCRO), oltre ai file delle relative marche temporali applicate (in formato ".tsr");
- il file indice del Pacchetto di Distribuzione (firmato e in formato SInCRO) oltre all'eventuale marca temporale (se prevista al punto 6 del paragrafo "Richiesta del Pacchetto di Distribuzione").

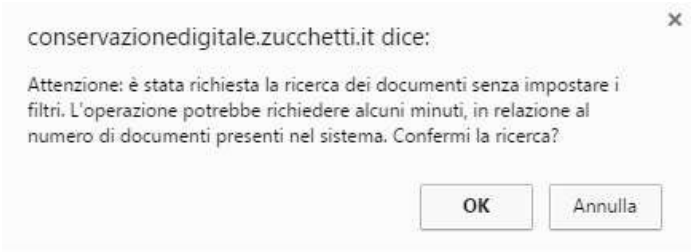
3.3-Ricerca documenti

È possibile ottenere l'elenco dei documenti presenti e i relativi report in formato PDF o CSV, selezionando "Ricerca documenti":

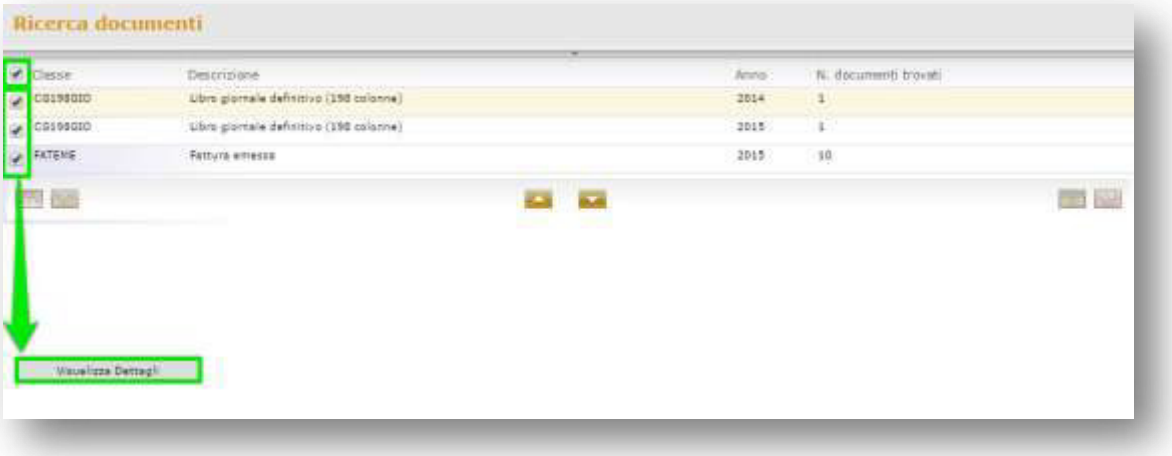
Si presenterà così la videata relativa ai diversi filtri di ricerca disponibili. Prima di avviare la ricerca mediante l'apposito tasto è consigliabile applicare almeno un filtro, ad esempio relativamente alla classe documentale, all'azienda di cui si desidera ottenere i dati o all'anno dei documenti, per ridurre i tempi di ricerca:



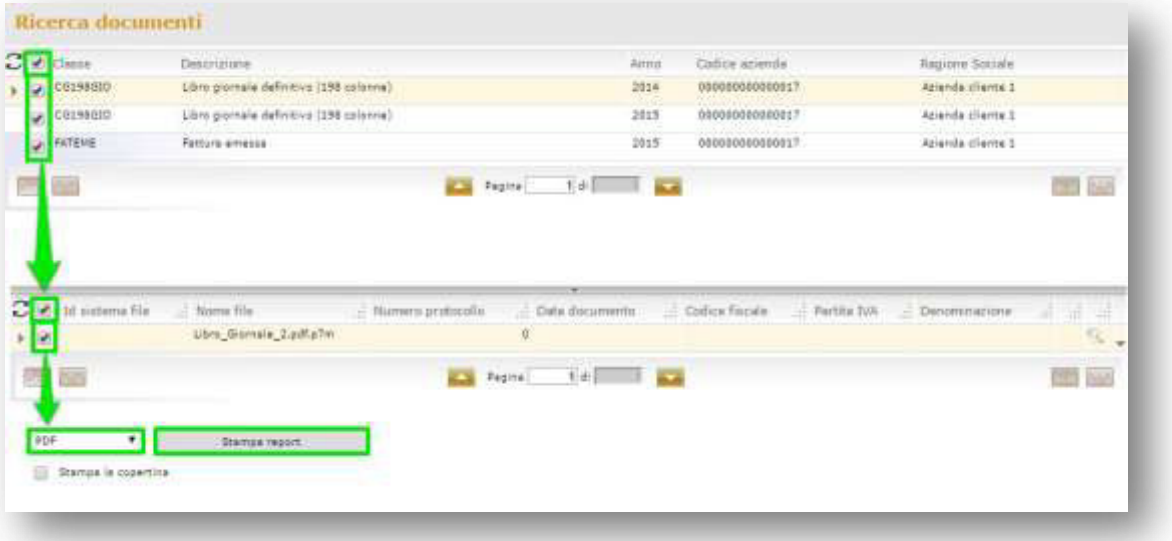
La ricerca è possibile anche senza applicare filtri; in questo caso, però, comparirà un messaggio di conferma prima di proseguire.



Dopo aver avviato la ricerca viene fornito un primo risultato aggregato per anno e classe documentale. E' necessario quindi selezionare quanto d'interesse e premere "Visualizza dettagli".



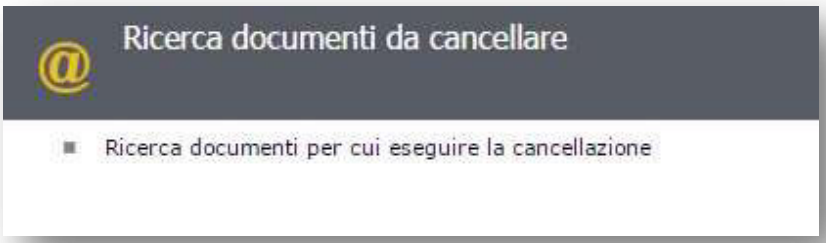
La videata successiva consente, selezionando le voci in testata, di visualizzare e selezionare massivamente le voci di dettaglio nella sezione sottostante. Una volta effettuata la selezione desiderata sarà possibile scegliere la tipologia di report tra PDF e CSV e procedere con la stampa.



3.4-Richiesta cancellazioni

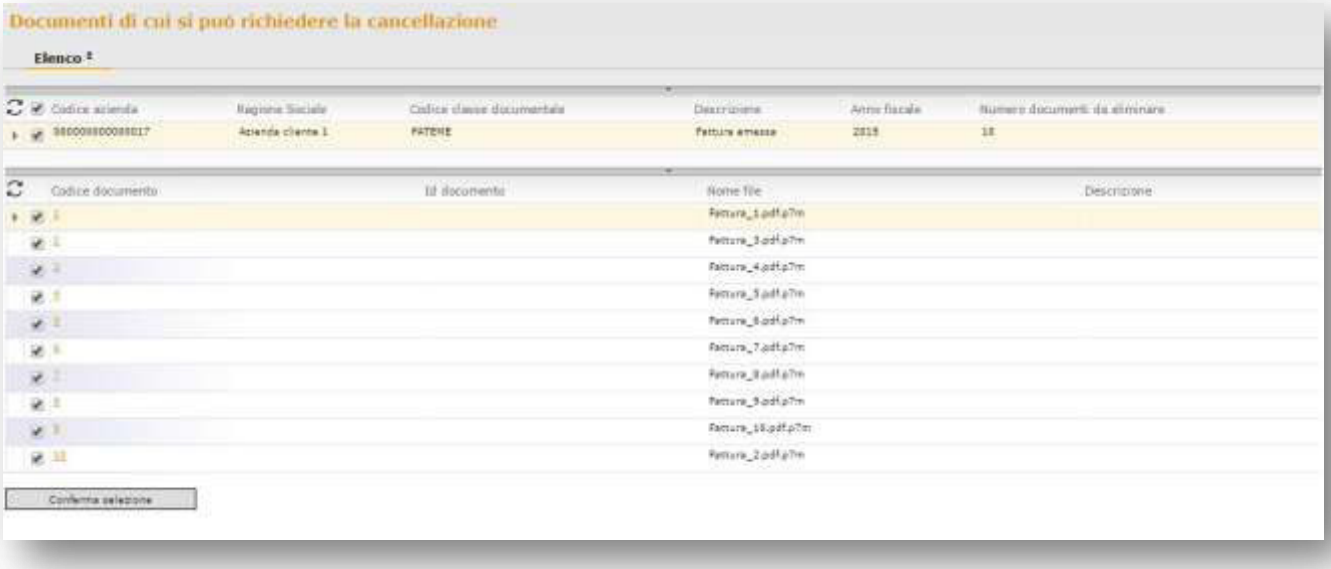
Il sistema di conservazione mette a disposizione del Responsabile della Conservazione (persona sempre identificata all'interno dell'azienda produttrice dei documenti) una funzionalità volta ad eliminare in modo definitivo i documenti presenti al proprio interno.

Preventivamente, è necessario eseguire la ricerca dei documenti da cancellare.



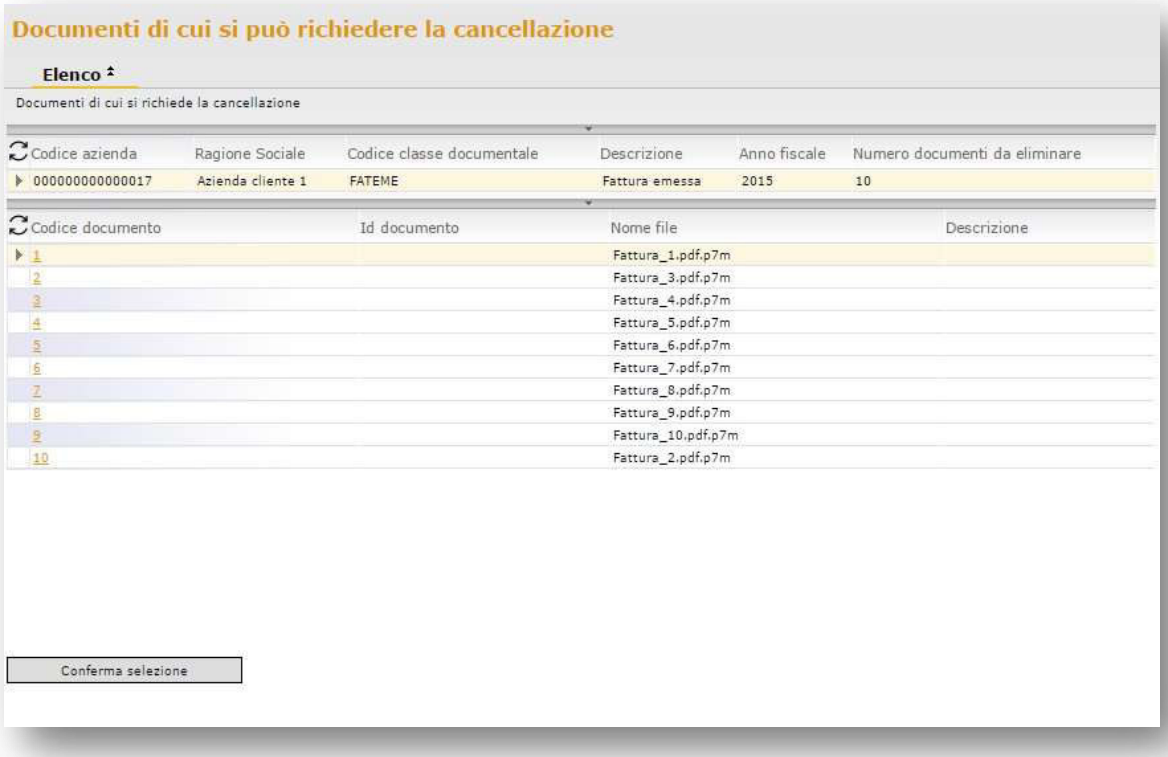
Sarà, quindi, necessario applicare i filtri desiderati per ottenere l'elenco dei documenti da eliminare, scegliendo, ad esempio, tra il nome di uno specifico file, la classe documentale di appartenenza e i relativi metadati.

I risultati della ricerca effettuata sono elencati in maniera aggregata per azienda di appartenenza, classe documentale e anno di riferimento.

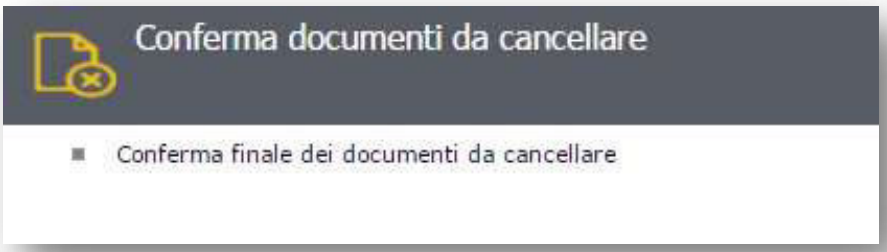


Selezionando la/e aggregazione/i desiderata/e vengono automaticamente selezionati anche tutti i documenti ad essa/e appartenenti; è sempre possibile deselezionare quelli eventualmente da escludere dal processo di eliminazione.

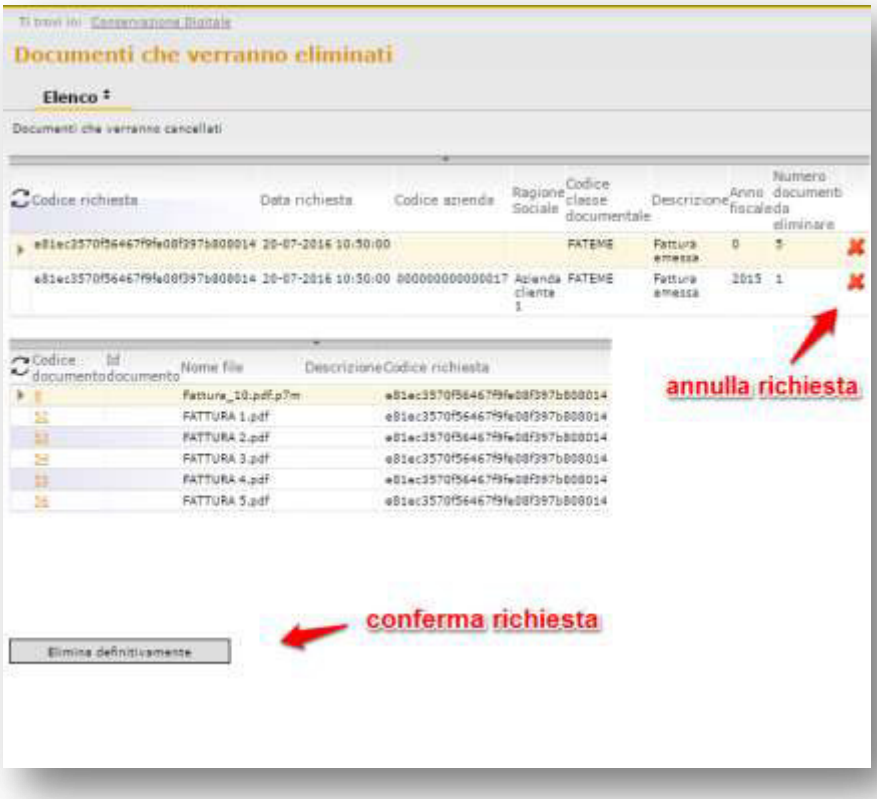
Utilizzando il tasto "*Conferma selezione*" la procedura inserisce la richiesta e, contestualmente, viene inviata un'e-mail di notifica all'indirizzo fornito in fase di sottoscrizione del contratto.



Per una maggiore sicurezza, la richiesta dovrà essere successivamente confermata tramite la funzione “Conferma cancellazioni”.



In questa sezione è possibile confermare l’eliminazione dei documenti selezionati o annullare la richiesta. Una volta confermata la richiesta, il sistema, tramite processo schedulato, provvederà all’eliminazione definitiva dei documenti.



Zucchetti spa
Via Solferino, 1 • 26900 Lodi
Tel. 0371/ 594.28.88 • Fax 0371/594.38.81
www.zucchetti.it

ZUCCHETTI
LE SOLUZIONI CHE CREANO SUCCESSO

ALLEGATO N.4

servizi-it
PIU SOLUZIONI, MENO PENSIERI

DATACENTER ZUCCHETTI – SERVICE LEVEL AGREEMENT

AZIENDA SOCIALE SUD EST MILANO * A.S.S.E.M.I.

IL CLIENTE (timbro e firma)

Sommario

AZIENDA SOCIALE SUD EST MILANO A.S.S.E.M.I.

CLIENTE (timbro e firma)

1. Premessa

Il Service Level Agreement (SLA) descrive i servizi erogati dal Datacenter Zucchetti, fornendo garanzie d'esercizio basate su elementi misurabili.

Lo SLA integra il contratto con il cliente relativo al servizio cui si riferisce e riporta:

- definizioni,
- elenco servizi oggetto di misurazione,
- elementi dei servizi
- criteri di misurazione dei livelli di servizio prestati,
- valori obiettivo e indicatori.

1.1. Termini, definizioni, convenzioni

a) Termini, definizioni e convenzioni *di carattere generale*:

- *Servizi di Business* - Le prestazioni erogate dal Datacenter aventi caratteristiche misurabili.
- *Elementi di servizio* - Descrivono analiticamente le parti (singole attività) costituenti un servizio.
- *Livelli di servizio* - Ogni servizio è caratterizzato da indicatori che lo misurano e livelli obiettivo che illustrano i valori che il Datacenter vuole garantire.
- *Indicatori di livello* - Gli indicatori (spesso in relazione diretta con gli elementi di servizio) misurano come realmente il Datacenter Zucchetti eroga un certo servizio.
- *Livelli obiettivo* - Valori soglia il cui mancato rispetto costituisce una violazione del livello di servizio. Confrontati con gli indicatori descrivono la capacità del Datacenter Zucchetti di erogare un servizio.
- *Orario di svolgimento del servizio* - Descrive le fasce ordinarie di erogazione dei servizi e di disponibilità operativa del personale del Datacenter Zucchetti.
- *Contingenze* - Ogni intervento condotto a seguito di accordi specifici con il cliente ed eseguito senza considerazione delle fasce ordinarie d'operatività. Interventi in regime di contingenza saranno oggetto di offerta separata riportante elementi tecnici ed economici.
- *Esclusioni* - Le condizioni sotto le quali non si misurano i valori degli indicatori al fine del raffronto con i livelli obiettivo.

b) Termini, definizioni e convenzioni *specifiche del supporto*:

- *Ticket* - A ogni richiesta o segnalazione d'assistenza (effettuata via mail, via fax, per telefono, tramite sito web quando previsto) viene associato un biglietto elettronico (ticket) per garantirne il corretto sviluppo risolutivo.
- *Acquisizione* - indica la fase nella quale viene recepita una richiesta o segnalazione: a seguito di tale processo si procede alla numerazione e categorizzazione (livello di gravità) della richiesta, si raccolgono ulteriori informazioni e dettagli.
- *Presa in carico* - Dopo aver delineato con precisione i dettagli della richiesta, in questa fase il Datacenter determina la pianificazione delle risorse per completarla.

AZIENDA SOCIALE SUD EST MILANO A.S.E.M.I.

IL CLIENTE (timbro e firma)

- *Gestione della richiesta* - Sono le fasi di lavorazione della richiesta, finalizzate alla risoluzione del problema.
- *Risoluzione* - Si conducono tutte le attività necessarie al soddisfacimento della richiesta.
- *Incidente* - Una situazione che potenzialmente può compromettere disponibilità, confidenzialità e integrità dei dati e dei processi elaborativi.
- *Cambiamento* - Una richiesta che per la natura dell'intervento comporta una modifica sostanziale, con possibili conseguenze in termini di erogazione del servizio. Stante queste condizioni, un Cambiamento viene sempre sottoposto ad un percorso di approvazione e a una fase di confronto tra le parti interessate.
- *Richiesta Generica* - Ogni altra richiesta non catalogabile come Incidente o Cambiamento.
- *Priorità* - Per razionalizzare gli interventi e disporre sempre di risorse pronte all'intervento, le richieste vengono sottoposte ad un ordine di priorità in relazione all'urgenza e all'impatto sul servizio.
- *Impatto* - La misura dell'effetto dell'incidente sul servizio.
- *Urgenza* - La valutazione del tempo che intercorre tra il sorgere del problema/incidente e le ripercussioni sul servizio.

c) Termini, definizioni e convenzioni *relative alla disponibilità dei servizi*:

- *Sistema* - Uno o più elaboratori elettronici cooperanti per il medesimo fine elaborativo.
- *Sistema Indipendente* - Sistema costituito da un solo elaboratore.
- *Sistema bilanciato o in cluster* - Sistema costituito da due o più elaboratori adottanti metodi collaborativi e tecnologie atte a minimizzare il rischio di interruzioni.
- *Sistema fisico* - Basato su elaboratori fisici (hardware)
- *Sistema virtuale* - Basato su tecnologie che consentono la creazione di una versione virtuale di una risorsa normalmente fornita fisicamente.
- *Disaster recovery* - L'adozione di tecniche volte a ripristinare la disponibilità di un servizio nel minor tempo possibile e riducendo la perdita di dati, a fronte di situazioni d'emergenza.
- *Impianto tecnologico di networking* - L'insieme degli apparati e dei servizi correlati, volti a fornire connettività ad un sistema.
- *Fermi programmati* - Fermi agli impianti in genere che sono stati programmati e pubblicati.
- *Finestre di manutenzione* - Fasce orarie che orientativamente, ma non necessariamente, sono scelte per interventi di manutenzione.

AZIENDA SOCIALE SUD EST MILANO A.S.S.E.M.I.

IL CLIENTE (timbro e firma)

2. Servizi misurabili in ambito Datacenter

Di seguito sono descritti i servizi erogati da Datacenter che sono oggetto di misurazione.

I servizi non sottoposti a misurazione, non sono descritti nel presente documento.

Servizio di Datacenter	Descrizione Elementi di servizio
Supporto Helpdesk	Acquisizione di Ticket
	Presa in carico delle richieste per la gestione della chiamata
	Risoluzione delle richieste
Disponibilità dei sistemi	Disponibilità Sistemi in modalità StandAlone Virtuali
	Disponibilità Sistemi in modalità StandAlone Fisici
	Disponibilità Sistemi Bilanciati o Clustering
	Disponibilità Sistemi Virtuali in modalità D/R
Networking	Disponibilità Networking
	Disponibilità Networking in modalità D/R
	Liste di controllo accessi
Alimentazione elettrica	Disponibilità
Salvataggio e Ripristino	Periodo di Conservazione
	Ripristino
	Successo dei Salvataggi

3. Supporto Helpdesk

Zucchetti si propone di garantire i servizi di helpdesk nel rispetto degli SLA descritti di seguito.

3.1. Misura del Tempo di intervento

Misura il tempo intercorso tra l'apertura del ticket e l'intervento tecnico, misurato in ore all'interno degli orari di servizio del supporto di Helpdesk. Il calcolo del corrispondente indicatore si effettua su base annua.

$$\text{Indicatore} = \frac{\text{Numero di interventi entro il valore Obiettivo}}{\text{Numero totale di interventi}} * 100$$

AZIENDA SOCIALE SUD EST MILANO A.S.S.E.M.I.

IL CLIENTE (timbro e firma)

3.2. Categorizzazione delle richieste

Per ogni richiesta di supporto l'helpdesk effettua una classificazione indicando una priorità poi riportata nel Ticket. Per categorizzare le richieste di supporto, gli elementi valutati nell'apertura di

un ticket sono:

- IMPATTO - è la misura dell'effetto dell'incidente sul servizio di Business.
- URGENZA - è la valutazione del tempo intercorso tra il problema/incidente e le ripercussioni sul servizio.

TABELLA IMPATTI

Tipologia	Gravità	Descrizione
Impatto 3	Alta	blocco totale del servizio del cliente
Impatto 2	Media	singolo utente bloccato o parte del servizio bloccato
Impatto 1	Bassa	situazioni non bloccanti

TABELLA URGENZE

Tipologia	Livello	Descrizione
Urgenza 3	Alta	Ripercussioni sul servizio immediate
Urgenza 2	Media	Ripercussioni sul servizio a breve termine – entro 8 ore
Urgenza 1	Bassa	Ripercussioni sul servizio oltre la giornata

L'insieme dei due elementi, analizzati in prima battuta dall'operatore di Helpdesk, genera il valore di PRIORITÀ.

TABELLA PRIORITÀ

	Urgenza 1	Urgenza 2	Urgenza 3
Impatto 1	1	1	2
Impatto 2	1	2	3
Impatto 3	2	3	3

Urgenza e Impatto (e la Priorità derivante) sono state introdotte principalmente per la gestione degli Incidenti, tuttavia si è ritenuto opportuno estendere questa logica anche alle Richieste Generiche e ai Cambiamenti, per razionalizzare e migliorare complessivamente l'organizzazione del supporto.

AZIENDA SOCIALE SUD EST MILANO A.S.S.E.M.I.

IL CLIENTE (timbro e firma)

3.3. SLA del Tempo di intervento

Elemento di Servizio	Tipologia	Priorità	Obiettivo	Indicatore

Apertura Ticket	· **Incidente** · **Richiesta Generica** · **Cambiamento**	assegnazione priorità / organizzazione	0,5 ora	98%
Presa in carico	· **Incidente**	Priorità: 3 (alta)	0,5 ora	98%
		Priorità: 2 (media)	0,5 ora	97%
		Priorità: 1 (bassa)	1 ora	95%
	· **Richiesta Generica**	Priorità: 3 (alta)	2 ore	95%
		Priorità: 2 (media)	2 ore	92%
		Priorità: 1 (bassa)	4 ore	90%
	· **Cambiamento**	Priorità: 3 (alta)	4 ore	95%
		Priorità: 2 (media)	4 ore	90%
		Priorità: 1 (bassa)	8 ore	90%
Risoluzione Ticket	· **Incidente**	Priorità: 3 (alta)	2 ore	98%
		Priorità: 2 (media)	4 ore	92%
		Priorità: 1 (bassa)	6 ore	90%
	· **Richiesta Generica**	Priorità: 3 (alta)	4 ore	95%
		Priorità: 2 (media)	6 ore	92%
		Priorità: 1 (bassa)	8 ore	90%
	· **Cambiamento***	Priorità: 3 (alta)	6 ore	95%
		Priorità: 2 (media)	8 ore	90%
		Priorità: 1 (bassa)	12 ore	90%

*= la richiesta deve essere gestita dopo un processo di approvazione da parte del referente tecnico preposto.

3.4. Orari del supporto

Di seguito gli orari di riferimento del supporto dell'Helpdesk di Datacenter:

Servizio	Giorni	Fasce Orarie
Supporto Helpdesk Datacenter	Lunedì – Venerdì	Dalle 08:00 alle 20:00
	Sabato	Dalle 08:30 alle 12:30

Sono escluse le festività ufficialmente riconosciute; eventuali variazioni saranno tempestivamente notificate.

AZIENDA SOCIALE SUD EST MILANO * A.S.S.E.M.I.

IL CLIENTE (timbro e firma)

4. Servizi

La classificazione dei Servizi si articola come segue:

- servizi a richiesta: vengono erogati a fronte di richieste esplicite, possono prevedere la necessità di un preventivo accordo;
- servizi programmati: vengono erogati in modo continuato da parte del Datacenter e non necessitano di richieste esplicite.
- interventi contingenti: vengono erogati a seguito di accordi specifici con il cliente ed eseguiti senza considerazione delle fasce di supporto indicato. Interventi in regime di contingenza saranno oggetto di offerta separata riportante elementi tecnici ed economici.

Eventuali indisponibilità o degrado prestazionale dei servizi, manifestatisi a seguito di interventi contingenti e non relativi alla modalità standard di erogazione dei servizi, non vengono considerati ai fini della valutazione dei livelli di servizio.

4.1. Periodo di Disponibilità del servizio

Di seguito il periodo di Disponibilità dei servizi:

Servizio	Periodo
Disponibilità Servizi di Datacenter	24/24 – 365giorni/anno

Si sono individuate due finestre di manutenzione (domenica dalle 02:00 alle 06:00 e nei giorni lavorativi dalle 03:00 alle 06:00) che possono eventualmente essere usate per pianificare ed effettuare interventi di manutenzione di rete e dei sistemi. Il sistema di misurazione dello SLA non considera dette finestre nei calcoli di disponibilità.

5. Disponibilità dei Sistemi (Availability)

5.1. Misura della Disponibilità dei Sistemi

La Disponibilità del Servizio è misurata con una percentuale su base annuale dei servizi di Business a livello di sistema, calcolata come segue:

$$\textit{Disponibilità Sistema} = \frac{\textit{Numero ore di Sistema attivo}}{\textit{Numero ore di Disponibilità Sistema}} * 100$$

Per "Numero ore di Sistema attivo" si intende il numero di ore di disponibilità tolte le ore di disservizio. Nel calcolo dei disservizi sono esclusi:

AZIENDA SOCIALE SUD EST MILANO A.S.S.E.M.I.

IL CLIENTE (timbro e firma)

- fermi programmati e contingenze.
- fermi dovuti a eventi di forza maggiore.
- interventi di urgenza volti a garantire la sicurezza degli impianti, la protezione di dati e sistemi, la continuità d'esercizio, pur non procedendo come previsto per gli interventi programmati e pubblicati.
- il numero di ore in cui il Servizio per gli utenti finali non sia stato disponibile, a causa di un malfunzionamento di una qualsiasi componente non affidata in gestione a Zucchetti spa.
- le finestre di manutenzione di rete e dei sistemi che, come regola generale, possono essere pianificate ed effettuate di domenica dalle 02:00 AM alle 06:00 AM e nei giorni lavorativi dalle 03:00 alle 06:00 (vedi 4.1).

5.2. SLA della Disponibilità dei Sistemi

Per Disponibilità dei sistemi server si intende l'erogazione del Servizio in condizioni di normalità, in termini di fruibilità e di accesso ai dati attesi per l'utente finale.

Servizio	Tipologia	Ambito di applicazione	Indicatore
Disponibilità Sistemi	**Sistema Virtuale indipendente**	Singolo elaboratore in modalità StandAlone su piattaforma Virtuale	99%
	Sistema Fisico indipendente	Singolo elaboratore in modalità StandAlone su piattaforma Fisica	98%
	Sistemi Bilanciati o in Cluster	Sistemi configurati in modalità Bilanciata o Clustering (Fisico o Virtuale)	99,9%

In modalità Disaster Recovery (esclusivamente per ambienti virtuali, ove contrattualmente previsto) lo SLA prevede quanto segue:

Servizio	Tipologia	Elemento di Servizio	Obiettivo	Indicatore
Disponibilità Sistemi	**Disaster Recovery per ambiente Virtuale**	RTO (tempo per ripresa operativa del sistema)	4 ore	99%
		RPO (misura, in ore, dei dati che il sistema può perdere)	4 ore	99%
		Capacità elaborativa dei servizi in modalità D/R	Almeno il 60% della capacità elaborativa totale	99%

AZIENDA SOCIALE SUD EST MILANESE A.S.S.E.M.I. ONLUS

IL CLIENTE (timbro e firma)

6. Networking di Datacenter

Zucchetti spa si propone di garantire il servizio di networking nel rispetto degli SLA meglio descritti di seguito in termini di disponibilità.

6.1. Misura della Disponibilità del networking

La Disponibilità del Servizio è misurata con una percentuale su base annuale dei servizi di Business a livello di impianto tecnologico, calcolata come segue:

$$\text{Disponibilità Networking} = \frac{\text{Numero ore di Networking attivo}}{\text{Numero ore di Disponibilità Networking}} * 100$$

Per "Numero ore di Networking attivo" si intende il numero di ore di disponibilità tolte le ore di disservizio. Nel calcolo dei disservizi sono esclusi:

- fermi programmati e contingenze.
- fermi dovuti a eventi di forza maggiore.
- interventi di urgenza volti a garantire la sicurezza degli impianti, la protezione di dati e sistemi, la continuità d'esercizio, pur non procedendo come previsto per gli interventi programmati e pubblicati.
- il numero di ore in cui il Servizio per gli utenti finali non sia stato disponibile, a causa di un malfunzionamento di una qualsiasi componente non affidata in gestione a Zucchetti spa.
- le finestre di manutenzione di rete e dei sistemi che, come regola generale, possono essere pianificate ed effettuate di domenica dalle 02:00 AM alle 06:00 AM e nei giorni lavorativi dalle 03:00 alle 06:00 (vedi 4.1).

6.2. SLA della Disponibilità del Networking

Per Disponibilità si intende l'erogazione del Servizio di Networking in condizioni di normalità, in termini di fruibilità dell'accesso ad internet ed alle restanti risorse di Datacenter.

Servizio	Ambito di applicazione	Indicatore
Disponibilità del Networking	impianto tecnologico di Networking di Datacenter	**99,9%**

In condizione di Disaster Recovery Zucchetti spa si propone di garantire il seguente SLA:

Servizio	Ambito di applicazione	Indicatore
Disponibilità del Networking	impianto tecnologico di Networking di Datacenter **in modalità di D/R**	**95%**

AZIENDA SOCIALE SUD EST MILANO A.S.S.E.M.I.

IL CLIENTE (timbro e firma)

7. Disponibilità dell'Alimentazione Elettrica

7.1. Misura della Disponibilità Alimentazione Elettrica

La Disponibilità è misurata con una percentuale su base annuale dell'impianto tecnologico e calcolata come segue:

$$\text{Disponibilità Elettrica} = \frac{\text{Numero ore di Alimentazione attiva}}{\text{Numero ore di Disponibilità dell'Alimentazione}} * 100$$

Per "Numero ore di Alimentazione attiva" si intende il numero di ore di disponibilità tolte le ore di disservizio. Nel calcolo dei disservizi sono esclusi:

- fermi programmati e contingenze.
- fermi dovuti a eventi di forza maggiore.
- interventi di urgenza volti a garantire la sicurezza degli impianti, la protezione di dati e sistemi, la continuità d'esercizio, pur non procedendo come previsto per gli interventi programmati e pubblicati.
- il numero di ore in cui il Servizio per gli utenti finali non sia stato disponibile, a causa di un malfunzionamento di una qualsiasi componente non affidata in gestione a Zucchetti spa.
- le finestre di manutenzione di rete e dei sistemi che, come regola generale, possono essere pianificate ed effettuate di domenica dalle 02:00 AM alle 06:00 AM e nei giorni lavorativi dalle 03:00 alle 06:00 (vedi 4.1).

7.2. SLA della Disponibilità Alimentazione Elettrica

Per Disponibilità dell'alimentazione elettrica si intende l'erogazione del Servizio in condizioni di normalità e in modalità ridondata.

Servizio	Ambito di applicazione	Indicatore
Disponibilità dell'Alimentazione	impianto di alimentazione elettrica di Datacenter in modalità ridondata	**99,99%**

8. Salvataggio e Ripristino dei dati

Zucchetti spa si propone di garantire i servizi di Salvataggio e Ripristino dei dati nel rispetto degli SLA descritti nel presente documento. Per attività di Salvataggio e Ripristino si intende l'erogazione del Servizio di salvataggio e ripristino dei dati in condizioni di normalità, in termini di fruibilità dei dati per l'utente finale.

AZIENDA SOCIALE SUD EST MILANO * A.S.S.E.M.I.

IL CLIENTE (timbro e firma)

8.1. Misura del Successo dei Salvataggi

Misura la percentuale dei salvataggi andati a buon fine senza il processo di verifica. Il calcolo si effettua su base annua.

$$Indicatore = \frac{Numero\ di\ salvataggi\ con\ esito\ positivo}{Numero\ totale\ dei\ salvateggi\ effettuati} * 100$$

8.2. SLA di Successo dei Salvataggi

Zucchetti spa si propone di garantire i servizi di salvataggio dei dati nel rispetto degli SLA meglio descritti di seguito:

Elemento di Servizio	Obiettivo	Indicatore
Successo dei Salvataggi	**Salvataggio avvenuto con successo**	98%

8.3. Ripristino

Servizio	Numero massimo ripristini
Ripristino	**4/mese**

I tempi di esecuzione seguono l'impostazione delle Richieste Generiche, ivi compresi i tempi di presa in carico.

8.4. Conservazione

I dati vengono resi disponibili secondo le seguenti modalità:

Servizio	Periodo di Conservazione	Granularità
Salvataggio	**30 gg**	Giornaliera
	365 gg	Mensile

9. Liste di controllo accessi su firewall

Si intendono sia le liste su firewall perimetrali, sia le liste su quelli interni (segregazione delle reti)

Elemento di Servizio	Numero massimo di richieste gestione liste
Liste di controllo accessi	**10/anno**

I tempi di esecuzione seguono l'impostazione delle Richieste Generiche, ivi compresi i tempi di presa in carico. Tuttavia particolari richieste potrebbero essere sottoposte ad un processo di approvazione da parte del referente tecnico preposto.

AZIENDA SOCIALE SUD EST MILANO A.S.S.E.M.I.

IL CLIENTE (timbro e firma)

ALLEGATO N.5

Prodotto Inaz IFKTalk

GUIDA RAPIDA

Versione: 1.2.0

SOMMARIO

1 NOVITÀ DELLA VERSIONE 1.2.0

Inserita nuova gestione **compatibilità badge** nella pagina delle **Proprietà Generali**.
Inserita nuova funzione **Aggiorna kernel** nel menu del Terminale.
Sono state apportate alcune modifiche interne per l'ottimizzazione del colloquio tra Client e Server.

2 NOVITÀ DELLA VERSIONE 1.1.0

Gestione dei terminali IFK che utilizzano il kit UMTS per la trasmissione delle timbrature tramite internet.
Le connessioni UMTS, poiché utilizzano indirizzi IP dinamici, non consentono ai terminali di essere chiamati direttamente da IFKTalk Client come invece avviene con quelli installati sulle reti locali. Per controllare questi terminali viene affidato a loro stessi il compito di mettersi in comunicazione con IFKTalk Server ogni 5 minuti. Questo tempo consente un consumo limitato di traffico e insieme un'attesa ragionevole per l'esecuzione dei comandi in coda.

Identificazione del tipo di terminale.

I terminali gestiti da IFKTalk sono di due tipi : **LAN** identificati dall'icona  e **WAN** identificati dall'icona 
I terminali di tipo **WAN** comprendono sia i terminali collegati con il kit **UMTS** che quelli posti dietro ad un **firewall** che impedisce le connessioni in ingresso. Quest'ultima possibilità riduce o elimina la necessità di configurazioni sulle reti distribuite.

Controllo dei terminali.
Per i terminali di tipo WAN (Wide Area Network), i comandi e le modifiche delle proprietà non vengono inviati direttamente al terminale ma vengono inseriti in una **coda di comandi**, gestita da IFKTalk Server, che ciascun terminale eseguirà al primo contatto utile. Questo comportamento va tenuto in considerazione quando si utilizza la scelta 'Scarica timbrature da.. a..' che genera il file entro 5 minuti dalla richiesta.

Configurazione di base dei terminali UMTS con IFKTools.
Al momento dell'installazione, per garantire che il collegamento UMTS avvenga come previsto, è necessario eseguire alcune impostazioni iniziali sui terminali collegando un pc portatile direttamente al terminale con un cavo di rete ed eseguendo il programma **IFKTools** realizzato appositamente per guidare questa configurazione. **IFKTools** è disponibile come **autoestraente sul portale** e contiene tutte le informazioni necessarie per essere utilizzato, si consiglia di scaricarlo e leggerne le istruzioni prima di recarsi dai Clienti.
IFKTools non deve essere utilizzato per i terminali LAN, e non deve essere installato dove si installa IFKTalk.

Connessione automatica al server dopo il login.
Da questa versione la conservazione dei dati dell'impianto è stata trasferita alla componente Server di IFKTalk, per questo motivo IFKTalk Client deve collegarsi al Server per ottenere la lista dei terminali e la loro disposizione nella struttura ad albero. Nella riga di stato in basso a destra del programma vengono date le informazioni relative alla connessione. La scelta Connetti, nel menu File, va utilizzata solo per un eventuale ripristino della connessione.

Avvio automatico del visualizzatore Log.
Se la connessione al server avviene con successo, il visualizzatore log si avvia automaticamente.

Lista di attesa.
La prima volta che un terminale UMTS, opportunamente configurato con **IFKTools**, si mette in comunicazione con IFKTalk Server, viene inserito nella **lista di attesa.** Nella riga di stato di IFKTalk Client appare una **segnalazione in giallo** che indica il numero di terminali presenti nella lista di attesa; cliccando sulla riga gialla viene attivato l'**Inserimento terminali in lista di attesa** che consente di selezionare i terminali presenti nella lista per inserirli nell'impianto.

Lettura RF125KHz compatibile con IDT.
Nelle proprietà Generali è stata inserita una scelta che abilita la lettura dei Badge RFID in modo compatibile con i terminali IDT.

Ultimo contatto del terminale.
Nella lista con i dettagli dei terminali è stata introdotta la colonna Ultimo contatto. Se un terminale (sia LAN che WAN) contatta il server con regolarità, il campo è **verde**. Dopo un ritardo di **10 minuti** il campo diventa **giallo**. Se il ritardo si prolunga oltre **6 ore** il campo diventa **rosso**.

3 INTRODUZIONE

IFKTalk è costituito da due parti principali:

- **IFKTalk Client** consente la configurazione e il monitoraggio dello stato dei terminali.
- **IFKTalk Server**, installato come servizio, riceve le timbrature dai terminali e le scarica nel file predefinito oppure nei file scelti con le configurazioni.

Inoltre è presente anche **IFKTalk Monitor** che mostra lo stato del servizio con una icona nell'area di notifica in basso a destra.

L'installazione predefinita di IFKTalk, oltre ad installare i programmi, crea la cartella **C:\InazFiles\IFKTalk** contenente le seguenti sottocartelle:

- **DatiImpianto** : contiene i file di configurazione dell'impianto e dei terminali, i file sono crittografati e gestiti esclusivamente da IFKTalk.
- **Logs** al suo interno troviamo i file :
  - **LogIFK<AAAAMMGG>.log,** file di log giornalieri che riportano tutti gli eventi significativi del server e del client
  - ReportImpiantoIFK.pdf
  - TransazIFK.sav
  - altri file con le eventuali segnalazioni di errore
- **Timbrature** al suo interno troviamo :
  - **TransazIFK.dat** file di scarico predefinito
  - **TimbratureScartate.txt** file dove vengono salvate eventuali timbrature non valide

  Si suggerisce di usare questa cartella come destinazione dei file per eventuali percorsi di scarico personalizzati.

Lo scopo di questa guida è di fornire gli elementi essenziali per mettere in funzione l'impianto.

4 IFKTALK SERVER

IFKTalk Server non richiede alcuna configurazione, perché con l'installazione di IFKTalk vengono eseguite anche le seguenti operazioni:

- avvio del servizio IFKTalk Server (sulla porta predefinita 8888)
- Avvio di IFKTalk Monitor
- Aggiunta di una regola al Firewall di Windows, per consentire al servizio di accettare le connessioni in arrivo dai terminali.

N.B.
Alcuni antivirus integrano dei componenti che potrebbero impedire il corretto funzionamento del servizio perché bloccano le connessioni in ingresso.
Per controllare che IFKTalk Server sia raggiungibile dai terminali, dopo avere verificato con **IFKTalk Monitor** che il servizio sia avviato, aprire un browser da un computer diverso da quello dove si è eseguita l'installazione e digitare l'indirizzo **http://***IndirizzoIPdelServer***:8888** (es.: http://192.168.0.2:8888).
Se la connessione va a buon fine verrà mostrata una pagina di conferma, altrimenti potrebbe essere necessario configurare manualmente l'antivirus per abilitare il traffico TCP in entrata verso il servizio INAZ IFKTalk Server.
Questo test può essere eseguito direttamente dai terminali con firmware 6.14 e successivi nel modo seguente:
Entrare in configurazione premendo esc per almeno 10 secondi, inserire la password, selezionare **HTTPC test page**

5 IFKTALK CLIENT

Quando il programma viene avviato vengono richieste le credenziali di accesso :

Nel campo **Utente**: inserire **admin**
Nel campo **Password**: inserire **password**

Dopo l'accesso, il programma si collega al Server per scaricare l'elenco dei terminali, avvia il visualizzatore Log e infine si mette nello stato normale che possiamo definire di **monitoraggio**.

Al primo avvio del programma sarà necessario passare alla fase di configurazione per inserire i terminali presenti nell'impianto. In presenza di terminali WAN è necessario aspettare che questi appaiano nella lista di attesa prima di passere alla configurazione.

6 LOG DEGLI EVENTI (LOGGER)

IFKTalk, sia Server che Client, registrano costantemente gli eventi significativi utilizzando un log con sei livelli di importanza da 1 a 6 : Critical, Error, Warning, Info, Verbose, Debug.
Con la barra degli strumenti, posta nella parte bassa della finestra, possiamo avviare o fermare la lettura degli eventi con gli appositi bottoni oppure escludere la visualizzazione dei messaggi di livello più basso cliccando sulle icone con i numeri. Quando la lettura è ferma è possibile rileggere i file di log precedenti cliccando sull'icona con la cartella azzurra.
Quando è avviata, la lettura degli eventi resta attiva anche nelle fasi di configurazioni.
È importante ricordare che la registrazione è sempre attiva anche se la lettura è ferma, perciò qualsiasi evento potrà essere sempre visualizzato rileggendo il file di log giornalieri.

7 MONITORAGGIO

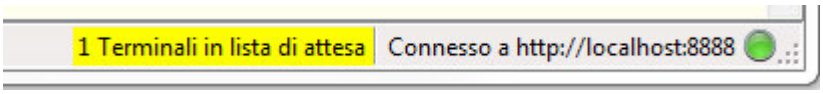
Durante il monitoraggio è possibile osservare gli eventi di log e lo stato dei terminali in base alle icone :

	Terminali LAN		Terminali WAN
	Terminale nuovo appena inserito		Terminale nuovo appena inserito
	Il terminale è raggiungibile e può inviare le timbrature.		Il terminale contatta il server regolarmente e può inviare le timbrature.
	Il terminale è raggiungibile ma l'acquisizione delle timbrature è sospesa.		Il terminale contatta il server regolarmente ma l'acquisizione delle timbrature è sospesa.
	Il terminale non è raggiungibile.		

Il bottone '**Avvia acquisizione per tutti**' si abilita se almeno un terminale ha sospeso l'acquisizione delle timbrature.
Dalla versione 1.1.0 durante il monitoraggio vengono aggiornate anche la colonna **Ultimo contatto** e la **lista di attesa**, visibili nelle due immagini che seguono.

Descrizione	Id termin...	Indirizzo IP	Aquisiz...	Modello	Firmware	Numero di serie	Tipo lettore	Ultimo contatto
Nuovo SN3390140100188	LAB2	151.18.132....	SI	IFK500	6.14l	SN3390140100188	RF 125Khz ...	08 apr 18:51:27

Se un terminale (sia LAN che WAN) contatta il server con **regolarità**, il campo è **verde**. Dopo un **ritardo di 10 minuti** il campo diventa **giallo**. Se il ritardo si prolunga **oltre 6 ore** il campo diventa **rosso**.



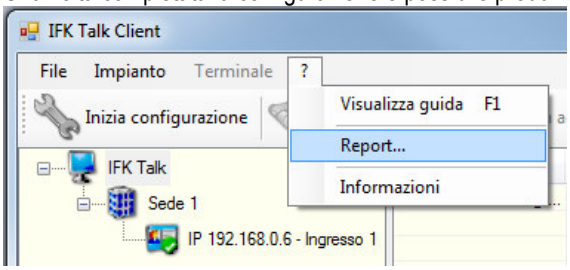
Cliccare sulla riga gialla per attivare **l'inserimento da lista di attesa** che consente di selezionare i terminali presenti nella lista per inserirli nell'impianto.

Premendo Il bottone **'Inizia configurazione'** viene sospeso il monitoraggio e si entra in configurazione.

8 CONFIGURAZIONE

Al primo avvio, se i terminali sono già stati collegati alla rete locale, è conveniente utilizzare la funzione di **Auto discovery** per riconoscerli ed inserirli automaticamente nell'impianto.
Successivamente sarà possibile configurare le opzioni dell'impianto e le proprietà dei singoli terminali.
Premendo Il bottone **'Termina configurazione'** vengono salvate tutte le configurazioni dei terminali e la struttura ad albero.

Una volta completata la configurazione è possibile produrre un **Report in Pdf** dell'impianto utilizzando la scelta **Report...** del menu **?**



N.B.
Quando il programma si trova nello stato di configurazione, l'aggiornamento dei dati a video è sospeso. Pertanto la colonna **Ultimo contatto** resta ferma sugli stessi orari e la barra di stato con la **lista di attesa** non segnala la presenza di nuovi terminali.
È sufficiente terminare la configurazione per aggiornare tutti i campi e gli stati dei terminali (con una frequenza di 3 secondi).

9 AUTO DISCOVERY (SOLO TERMINALI LAN)

Il bottone **Auto discovery** è abilitato solo durante la configurazione, premendolo si accede alla finestra che consente di eseguire la ricerca di tutti i terminali di tipo LAN installati in un solo passaggio.
È possibile inserire indirizzi IP singoli oppure gamme di indirizzi contigui, premendo il relativo bottone Aggiungi. Una volta che gli indirizzi da cercare sono inseriti nella lista, è possibile iniziare la ricerca premendo Ok. Viene proposta la lista di tutti gli indirizzi per conferma e poi la ricerca parte simultaneamente per tutti gli indirizzi inseriti.
Se vengono inseriti indirizzi IP già presenti nell'elenco dei terminali, questi vengono esclusi automaticamente dalla ricerca.

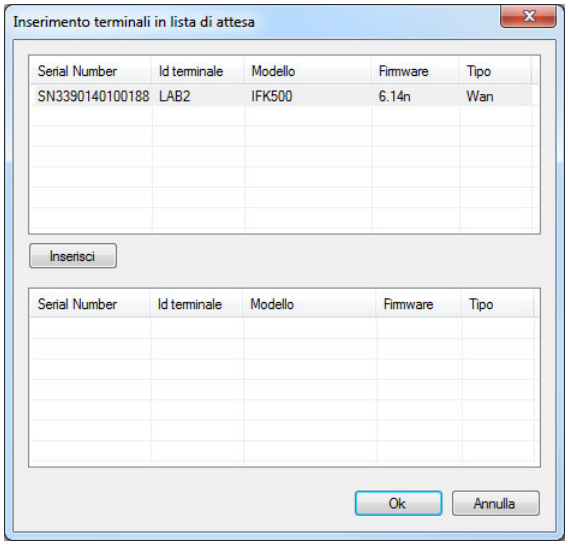
Se i terminali non vengono trovati la ricerca continua ogni 20 secondi (5 di timeout della connessione + 15 di intervallo tra due ricerche).
In condizioni normali i terminali vengono trovati in meno di un secondo. Se non vengono trovati dopo alcuni tentativi, si può interrompere la ricerca premendo ancora sul bottone **Auto discovery**.

Quando un terminale viene trovato, vengono lette le sue configurazioni correnti, corrispondenti ai valori predefiniti in fabbrica secondo le specifiche Inaz, e viene inserito nella radice della struttura ad albero dei terminali, nella parte sinistra della finestra del programma.
Contestualmente viene sincronizzata l'ora del terminale con quella del computer in uso.

Se si desidera, è possibile organizzare i terminali trovati trascinando l'icona di un terminale in alto o in basso oppure sull'icona di un contenitore. Nel programma viene già creato un contenitore predefinito Sede 1, è possibile inserirne di nuovi oppure rinominarli e cancellarli. Per rinominare un ramo (sia Terminale che Contenitore) cliccare sulla sua descrizione due volte o premere F2 dopo averlo selezionato.

10 LISTA DI ATTESA (TERMINALI WAN)

I terminali WAN appaiono in lista di attesa quando sono stati correttamente configurati con **IFKTools.** Nella riga di stato di IFKTalk Client viene presentata una **segnalazione in giallo** che indica il numero di terminali presenti nella lista di attesa; cliccando sulla riga gialla viene attivato l'**Inserimento terminali in lista di attesa** che consente di selezionare i terminali presenti nella lista per inserirli nell'impianto. Se un terminale già configurato viene rimosso dall'impianto con IFKTalk, riapparirà successivamente nella lista di attesa. Se un terminale in lista di attesa viene spento o scollegato, dopo 10 minuti viene rimosso dalla lista.



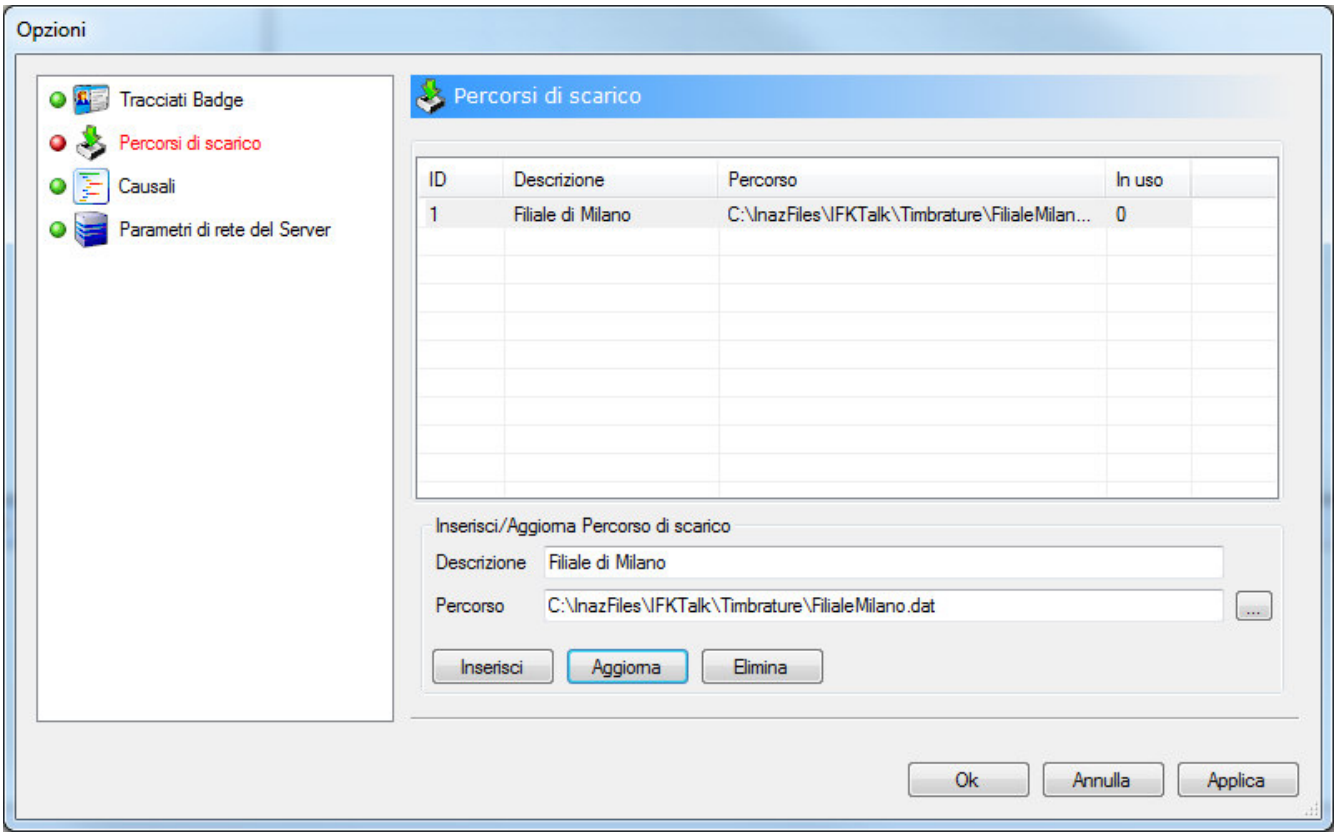
11 OPZIONI

Dal **Menu Impianto** con la scelta **Opzioni** è possibile, ma non obbligatorio, accedere alla configurazione delle seguenti opzioni dell'impianto: Tracciati Badge, Percorsi di scarico, Causali, Parametri di rete del Server.
Per i primi tre, i valori inseriti verranno resi disponibili nella fase di configurazione delle proprietà dei singoli terminali.
I Parametri di rete del Server, con la versione attuale, non devono essere modificati.

Con l'opzione **Percorsi di scarico**, ogni terminale può, se necessario, inviare le proprie timbrature ad un percorso di scarico personalizzato.
I percorsi di scarico devono essere creati a livello di impianto con questa opzione perché potranno essere usati da più di un terminale.
In seguito verranno resi disponibili nella fase di configurazione delle proprietà dei singoli terminali.

Il file di scarico predefinito **TransazIFK.dat** non richiede alcuna configurazione. Viene associato a tutti i terminali automaticamente.

Nell'esempio abbiamo predisposto un percorso che utilizzeremo per ricevere le timbrature da un terminale di un'altra sede.



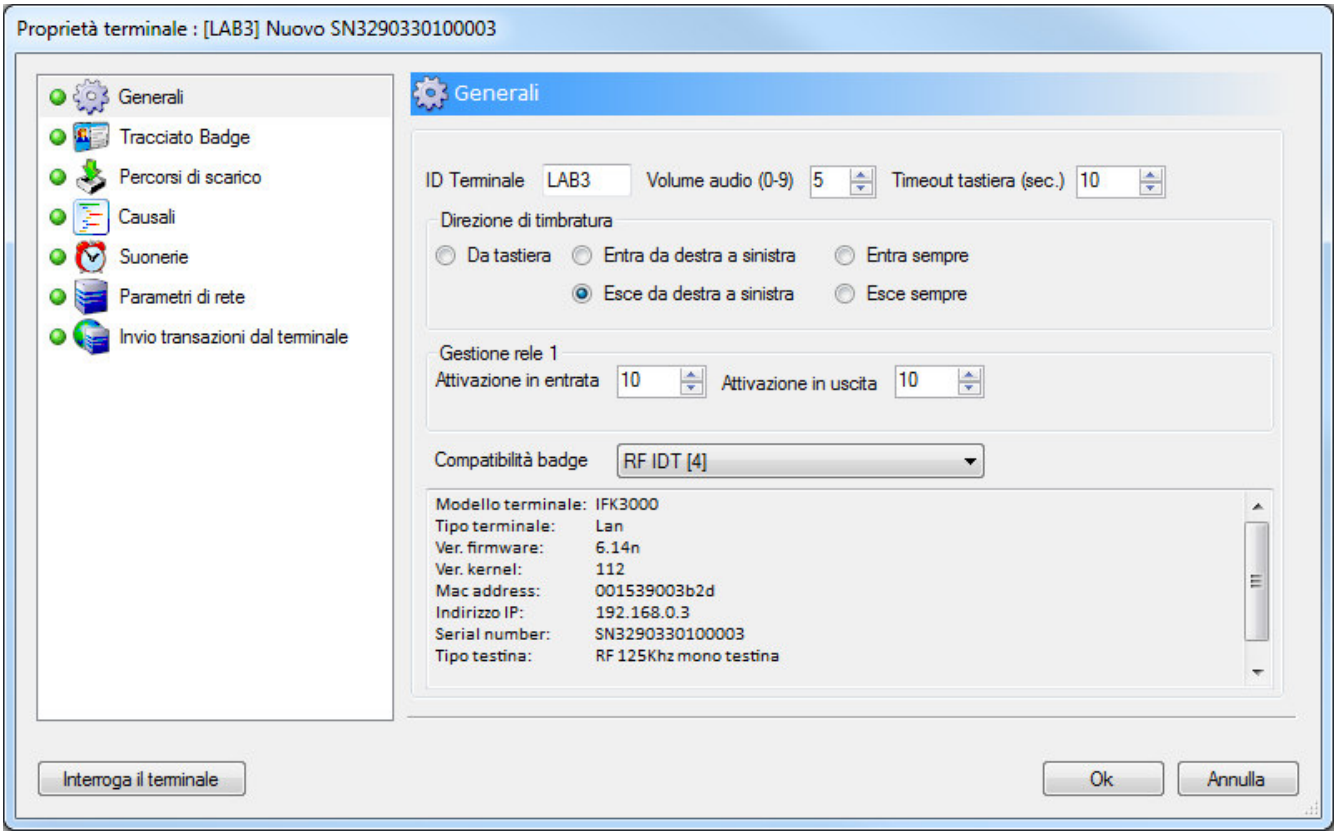
L'evidenziazione in rosso di una o più opzioni, indica che i valori inseriti a video non sono ancora stati salvati, si può passare da un'opzione all'altra senza perdere le modifiche. Il salvataggio avviene premendo il bottone **Applica** (Salva e rimane nelle Opzioni) oppure il bottone **Ok** (salva tutte le Opzioni modificate ed esce dalla finestra Opzioni).
La colonna '**In uso'** indica quanti terminali stanno usando quel percorso di scarico, se almeno un terminale usa quel percorso viene impedita la cancellazione.

12 PROPRIETA'

Dopo avere selezionato un terminale nella struttura ad albero, dal **Menu Terminale** con la scelta **Proprietà** entriamo nella finestra di configurazione del terminale. Come già detto, in questa guida affrontiamo solo gli aspetti essenziali della configurazione.

Generali

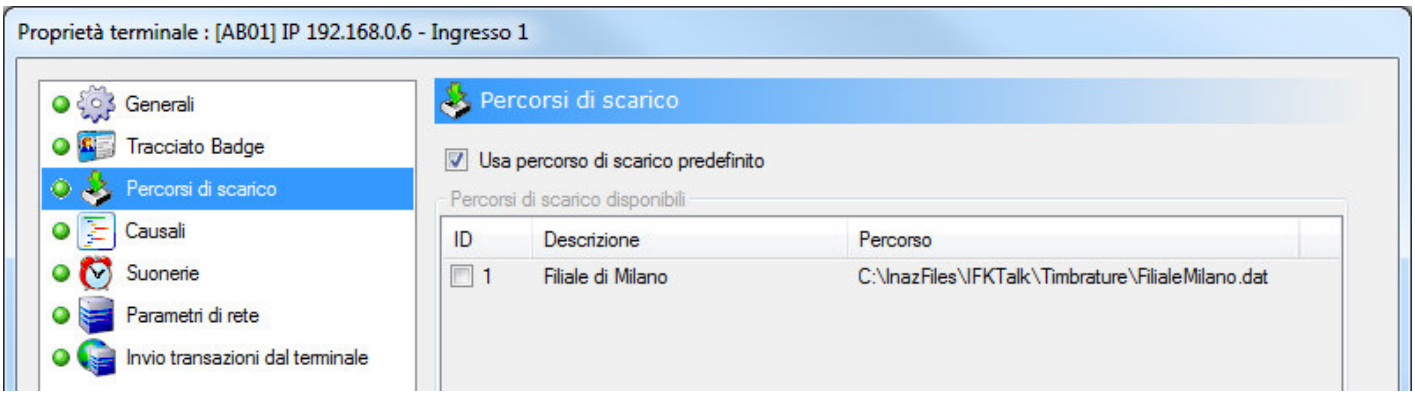
Nelle proprietà **Generali** è buona norma configurare **l'ID Terminale** con un identificativo, univoco per ogni terminale, di 4 caratteri alfanumerici, questo campo appare sempre negli ultimi quattro caratteri della timbratura.



Percorsi di scarico

Per assegnare un **Percorso di scarico** diverso da quello predefinito, togliere la spunta da "**Usa percorso di scarico predefinito**" e spuntare uno dei "**Percorsi di scarico disponibili**" inseriti in precedenza nelle opzioni dell'impianto.

N.B.: lo smistamento delle timbrature su file diversi avviene in funzione dell' **ID Terminale**. Per ridurre la possibilità di errori, i percorsi di scarico personalizzati non sono consentiti con **ID Terminale** predefinito **'0000'**.
È importante che i terminali con percorso di scarico personalizzato abbiano un ID Terminale univoco.



Invio transazioni dal terminale

In questa proprietà è OBBLIGATORIO indicare l'URL del Server per consentire al terminale di inviare le timbrature.
Sostituire l'indirizzo predefinito con l'indirizzo del computer dove è stato installato IFKTalk.

Nei terminali WAN, inseriti da lista di attesa, questo campo è già compilato correttamente, altrimenti il terminale non avrebbe potuto contattare IFKTalk Server. Pertanto non dovrebbe essere modificato.
L'indirizzo indicato per i terminali WAN potrebbe differire da altri terminali LAN presenti nello stesso impianto, perché gli indirizzi della rete locale sono generalmente indirizzi privati (es.: reti 192.168.x.x) mentre per i terminali WAN l'indirizzo utilizzato deve essere un IP pubblico e statico.

L'inserimento di parametri errati per i terminali WAN può interrompere la comunicazione con il terminale, rendendo necessario un intervento in loco per il ripristino della configurazione.

L'evidenziazione in rosso di una o più opzioni, indica che i valori inseriti a video non sono ancora stati salvati, si può passare da un'opzione all'altra senza perdere le modifiche. Il salvataggio avviene premendo il bottone **Ok**.

Non vi sono ulteriori informazioni.