QUESTIONARIO RISCHI INFORMATICI

1. IDENTIFICAZIONE DELLA RICHIEDENTE

Ragione Sociale Azienda ULSS n. 2 Marca trevigiana

Indirizzo Via Sant'Ambrogio di Fiera, 37

cap 31100

Città Treviso

Web site www.aulss2.veneto.it

Numero dipendenti: 9.360

Retribuzioni annue lorde: 435.719.675,72

2. PROFILO DELL'AZIENDA DA ASSICURARE E COPERTURE RICHIESTE

2.1 Descrizione delle attività

Assistenza sanitaria

Certificazione in relazione all'attività informatica	□ BS x ISO □ Altro *specificare*……
Ente certificatore	□ Bureau Veritas Italia □ RINA x CSQA
Scadenza certificazione	□ ……/……/…… □ In fase di certificazione
È' stato nominato il responsabile della sicurezza?	□ Impianti □ Logica □ Dati □ Altro *specificare*……..

UBICAZIONE / RISCHIO PRINCIPALE	
Esiste un Centro Elaborazione Dati	x SI □ NO Area CED TV sala 1 800 mq Area CED TV sala 2 90 mq Area CED Pieve sala 1 100 mq Area CED Pieve sala 2 30 mq Area CED Asolo sala 1 100 mq Area CED Asolo sala 2 30 mq

CED ubicato al piano	-2 Asolo -1 Asolo Piano terra Pieve +2 TV
Presenza di addetti 24/24h	□ SI x NO
Presenza di guardia notturna	x SI □ NO

3. SISTEMA INFORMATIVO

	<100	**101-2000**	**>2000**
Numero di Desktops			X
Numero di Servers		X	
Numero di Laptops		X	

Siete proprietari di una Extranet?	x SI	□ NO
Siete proprietari di un WebSite?	x SI	□ NO
Se sì, è ospitato da uno o più provider di servizi di hosting?	□ SI	x NO

Capacità totale di elaborazione e stoccaggio Dati	2000,000 GB……. *(in gigabyte)*	
Possibilità di accesso da remoto alla rete aziendale	x SI	□NO
Se sì, indicare il tipo di accesso	x VPN	x Altro *(specificare)* *Citrix……* *……*

4. SISTEMA DI SICUREZZA DELLE INFORMAZIONI (SSI)

4.1 Policy di Sicurezza e Organizzazione del Sistema di Sicurezza delle Informazioni

	SI	**NO**
La direzione aziendale ha approvato e formalizzato un documento scritto sulla SSI	**X**	
Tale politica è stata approvata dai responsabili del personale e comunicata a tutto il personale	**X**	
Per la gestione del SSI sono definiti l'organizzazione, ruoli e responsabilità	**X**	

Sono effettuati regolari training agli utenti sull'uso sicuro del sistema informativo	**X**	
Sono previsti regolari audit sull'applicazione del SSI che includono i rilievi delle criticità e i fattori correttivi di miglioramento raccomandati	**X**	
L'organizzazione è certificata nella sicurezza dell'Information Technology (ex.: Iso-9001, Iso20000-1, Iso-27000, PCI DSS, etc.).	**X**	
Se sì, indicate/allegate il tipo di certificazione, la scadenza, l'ente certificatore Accreditation Canada…… AGID……		
Confermate che il SSI è attuato in tutte le società controllate, affiliate, partecipate, oggetto del la presente richiesta di copertura?		
Commenti …….. ……		

4.2 Protezione delle informazioni e controllo degli accessi

	SI	**NO**
É stato formalizzato un inventario dei sistemi critici.	**X**	
E' stata instituita una procedura di classificazione delle informazioni alla luce del loro livello di sensibilità/criticità (riservatezza, disponibilità, integrità)	**X**	
I terzi sono soggetti ad accordi di confidenzialità che includono requisiti di sicurezza	**X**	
L'accesso ai sistemi d'informazione richiede l'identificazione e l'autenticazione degli utenti	**X**	
L'accesso ai sistemi informativi e alle applicazioni critiche è gestito da un software per il rinnovo delle password e la verifica della loro complessità	**X**	
Le autorizzazioni di accesso al sistema si basano sui ruoli dei singoli utenti ed esiste una procedura per la gestione delle autorizzazioni	**X**	
I sistemi critici beneficiano di sicurezza addizionale come segmentazione, audit tracking, strong authentication, etc	**X**	
I diritti di accesso alle applicazioni critiche sono rivisti regolarmente in accordo con il principio dell'ultimo privilegio	**X**	
Gli utenti possono avere accesso ai sistemi usando dispositivi personali (es. smartphone, tablet)		**X**
Se sì, sono presenti software per gestire questi dispositivi in ambiente lavorativo (Mobile device management)		**X**

4.3 Protezione dei Sistemi e Antivirus

	SI	**NO**
Tutte le workstations sono impostate e conformi a quella tipo scelta (Master).	**X**	
Esiste ed è operante una gestione centrale di tutte le apparecchiature del sistema.	**X**	
Si conferma che gli utenti non sono amministratori delle loro workstations.	**X**	

I laptops sono protetti da un personal firewall e/o i laptop possono connettersi con Internet soltanto tramite il network della corporate	**X**	
In tutti i sistemi che lo consentono è installato un Antivirus (in particolare per Windows) el'Antivirus è aggiornato automaticamente	**X**	
Sono ricevute e distribuite regolarmente nel sistema le "security patches"	**X**	
Sono prodotte e monitorate regolarmente le "Dashboards"	**X**	
Le regole di sicurezza e le procedure per la gestione delle variazioni e incidenti sono definite per la gestione del sistema, della sua operatività e configurazione	**X**	

4.4 Gestione delle copie dei Dati e dei Programmi (Backup)

	SI	**NO**
E' formalizzato un piano di backup ed è aggiornato regolarmente	**X**	
La procedura prevede come minimo un backup totale settimanale	**X**	
Almeno una copia dei dati e programmi è depositata in una località differente da quella ove risiede il sistema (altro indirizzo)	**X**	
I backup sono regolarmente testati	**X**	

Ciclo di rotazione dei Backup	**Tempo di ritenzione**	**Volume dei backup (Gbyte)**
x Giornaliero	**Settimana**	**200TB**
x Settimanale	**Mese**	
x Mensile	**Anno**	
x Altro…….	**1 x anno**	

4.5 La sicurezza della rete e delle operazioni

	SI	**NO**
E' installato ed operativo un firewall tra la rete interna e internet con un controllo aggiornato del flusso di informazioni in entrata ed in uscita	**X**	
La navigazione dagli utenti che hanno accesso a siti web di Internet avviene per mezzo e attraverso un dispositivo di rete (proxy) dotato di antivirus web	**X**	
La navigazione dagli utenti che hanno accesso a siti web di Internet avviene per mezzo e attraverso un dispositivo di rete (proxy) dotato di un filtro di accesso (es. non consente il collegamento con siti pericolosi)	**X**	
É stata istituita una segmentazione della rete per separare le aree critiche (servers, amministrazione, telecomunicazioni , etc ..) dalle aree meno critiche	**X**	
Sono attuati regolarmente i test di penetrazione perimetrale nella rete aziendale e le criticità rilevate sono soggette ad azioni di miglioramento	**X**	
Sono attuati regolarmente dei test sulla vulnerabilità dei sistemi informatici e le criticità rilevate sono soggette ad azioni di miglioramento.	**X**	
Audits e revisioni della sicurezza dell'architettura della rete sono condotti regolarmente e le criticità rilevate sono soggette ad azioni di miglioramento.	**X**	

Sono operative le procedure per la gestione degli incidenti e di eventuali cambiamenti al sistema	**X**	
Sono prodotti regolarmente report sulle prestazioni di servizio e di rete	**X**	
Esiste un monitoraggio proattivo sui tentativi di intrusione utilizzando sistemi di correlazione degli eventi ed analizzando i file di log		**X**

4.6 Business Continuity (BC) / Disaster Recovery (DR)

	SI	**NO**
Un BC plan e/o un DR plan esiste, è formalizzato ed aggiornato regolarmente	**X**	
I sistemi critici e le applicazioni sono totalmente ridondati.	**X**	
Sono effettuati regolarmente Test sul ripristino dei sistemi e delle applicazioni critiche	**X**	
C'è un contratto esterno di backup (outsourced) oppure è definita una soluzione interna	**X**	
E' stato predefinito un piano di reazione ad una situazione di crisi del sistema informativo	**X**	
E' stata condotta un analisi del rischio informatico	**X**	

4.7 Sicurezza fisica del Centro Elaborazione Dati (CED) / Webfarm

	SI	**NO**
I sistemi critici sono posti in specifici locali separati con accesso controllato e limitato.	**X**	
In caso affermativo sono ospitati in un "DataCenter" o in un luogo con livello di sicurezza equivalente	**X**	
I sistemi critici sono duplicati in funzione di un architettura "Active/Passive" o "Active/Active"	**X**	
I sistemi critici sono duplicati in due separate località	**X**	
I rivelatori antincendio nelle aree critiche sono installati, operativi e segnalano ad una stazione costantemente presidiata	**X**	
Sono installati ed operativi i sistemi automatici di estinzione	**X**	
Il sistema di condizionamento è ridondato completamente.	**X**	
I controlli ambientali (temperature, umidità, polveri, etc..) sono connessi ad allarmi automatici rimandati a stazione costantemente presidiata	**X**	
L'alimentazione è protetta da UPS e batterie soggette a programma regolare di manutenzione	**X**	
L'alimentazione è sostenuta da generatore elettrico soggetto a regolare contratto di manutenzione	**X**	

4.8. Servizio di gestione del sistema informativo presso terzi (Outsourcing)

	SI	**NO**
Con l'Outsourcer è stato definito contrattualmente un Service Level Agreement (SLA)	**X**	

Sono previste contrattualmente penalità per il mancato rispetto del SLA	**X**	
Sono definite contrattualmente procedure per gestire eventuali modifiche al sistema e/o incidenti.	**X**	
Il servizio prevede anche la regolare fornitura di reports sul servizio svolto dall'outsourcer	**X**	
L'outsourcer partecipa al comitato direttivo e di controllo, così da verificare e migliorare il servizio prestato	**X**	
Non avete contrattualmente rinunciato a rivalervi contro il fornitore di servizi	**X**	

Quali funzioni dei Sistemi Informativi sono esternalizzate?	**SI**	**NO**	**Società di Servizi (Outsourcer)**
Gestione Desktop	**X**		Consip SGM - Fastweb
Gestione Server	**X**		Consip SGM - Fastweb
Gestione RETI	**X**		Consip SGM - Fastweb
Gestione Sicurezza RETI	**X**		Consip SGM - Fastweb
Gestione Applicativi		**X**	
Utilizzo di cloud computing o Software as a service (SAAS)	**X**		Email
Help desk – Fonia	**X**		Consip SGM - Fastweb

5. STORICO SINISTRI *Indicare gli incidenti che hanno avuto un impatto sul sistema informativo negli ultimi 12 mesi*

Data	**Descrizione dell'evento**
/	/

6. PRIVACY

6.1 Dati personali gestiti dall'organizzazione

- **Numero delle registrazioni gestite**: 2010000 *(numero di file individuali)*
- **I file individuali riguardano e sono suddivisi come segue** :*(barrare i quadrati e indicare una % orientativa)*

x Impiegati/dipendenti propri/collaboratori 0,5% 5000

x Pazienti 99% 2000000

□ Clienti …..%

x Fornitori 0,5% 5000

□ Altro (specificare) ……%

- I Dati personali includono : *(barrare le caselle che vi riguardano)*

X Identificazione di una persona (nome, indirizzo, età, ...)

X Salute (anamnesi, analisi, storia clinica, cartelle cliniche, ...)

□ Dati finanziari (n. ° c/c – carte di credito, reddito, codici accesso, ...)

□ Marketing/dati commerciali (consumi, tempo libero, interessi, acquisti ...)

□ Altro, (specificare)

	SI	**NO**
Conservate informazioni sensibili ? (es. stato di salute, origine razziale o etnica, convinzioni religiose, opinioni politiche, vita sessuale, ...)	X	
Trasferite a terzi i Dati personali ?	X	
In caso affermativo:		
- I soggetti interessati ne sono informati	X	
- il terzo sottoscrive un impegno a rispettare il Vostro regolamento interno per la protezione dei Dati personali	X	
- Avete verificato come il terzo protegge i Dati personali	X	

6.2 Raccolta dei dati personali

I Dati vengono legalmente *(barrare le caselle che vi riguardano):*

X forniti volontariamente dalle persone interessate

□ automaticamente raccolti durante la navigazione web

□ raccolti tramite accordi di condivisione con terzi

□ Altro, (specificare od allegare dettaglio) ……

Il vostro metodo di raccolta dei dati personali	**SI**	**NO**
Avete verificato se i Dati personali raccolti devono essere dichiarati al Garante per la protezione dei Dati	X	
Richiedete il consenso degli individui a raccogliere i loro Dati personali	X	
Al momento della raccolta dei Dati personali, le persone vengono informate su quali Dati verranno conservati	X	
Al momento della raccolta dei Dati personali, le persone vengono informate del motivo per cui si conservano i loro Dati personali ed i termini del trattamento degli stessi	X	
Al momento della raccolta dei Dati personali, le persone vengono informate se gli stessi saranno trasferiti a terzi	X	
Al momento della raccolta dei Dati personali, le persone sono messe a conoscenza del periodo di durata della conservazione	X	
Le persone interessate possono avere accesso e, se necessario, correggere i propri Dati personali		X
Le persone interessate possono cancellare i propri Dati personali		X

6.3 Politica per la protezione dei dati personali

Il Vostro regolamento interno per la protezione dei dati personali	**SI**	**NO**
Il regolamento interno per la protezione e trattamento dei Dati personali è formalizzato ed approvato dalla direzione	X	
Gli aspetti giuridici del regolamento interno per la protezione dei Dati personali sono approvati da un ufficio legale.	X	
All'interno della vostra organizzazione è stato nominato il responsabile della protezione della Privacy	X	
Vengono utilizzate specifiche procedure di sicurezza per l'accesso, la gestione e la trasmissione dei Dati personali	X	
Il personale addetto è aggiornato sulle procedure di sicurezza per l'accesso, l'elaborazione e la trasmissione dei Dati personali	X	
Il personale addetto ha sottoscritto un impegno ed una clausola di riservatezza nel contratto di lavoro con l'azienda	X	
Il rispetto delle leggi e de regolamento interno per la protezione dei Dati personali sono regolarmente monitorati	X	
Le procedure sulle informazioni personali sono state controllate da un revisore esterno negli ultimi due anni		X

6.4 Protezione dei dati personali

La Vostra procedura di protezione dei dati personali	**SI**	**NO**
Esiste nella vostra organizzazione un archivio dei Dati personali che conservate e trattate	X	
Sono stati analizzati i rischi associati ai Dati personali ed il loro impatto sulla vostra organizzazione	X	
L'accesso ai Dati personali è limitato ai soli utenti che li utilizzano per svolgere il loro compito	X	
Le autorizzazioni di accesso sono limitate e riviste periodicamente	X	
Gli accessi ai Dati personali sono registrati nei file di log che sono protetti contro le manomissioni	X	
I Dati personali vengono crittografati quando vengono archiviati		X
I Dati personali sono criptati durante la trasmissione sulla rete	X	
Gli hard disk dei portatili sono criptati		X

Le Vostre prevenzioni per evitare perdite di dati personali	**SI**	**NO**
Non è permesso copiarli nei notebook	X	
Non è permesso copiarli in dispositivi di archiviazione rimovibili	X	
Non è permesso trasmetterli via e-mail	X	
I Vostri sistemi sono dotati di un Data Leakage Prevention (DLP)		X

6.5 Sinistri sulla privacy

Data	Descrizione dell'evento
/	/

7 Elenco e tipologia di servizio dei principali Outsourcer (vedi 4.8):

Servizi esternalizzati	SI	NO	Outsourcer
Vedi 4.8	X		Consip SGM - Fastweb
PACS radiologico	X		Fuji,Esaote,GE
Laboratorio Chimica Clinica	X		Noemalife, Dedalus
Conservazione	X		Infocert

ALLEGATI :

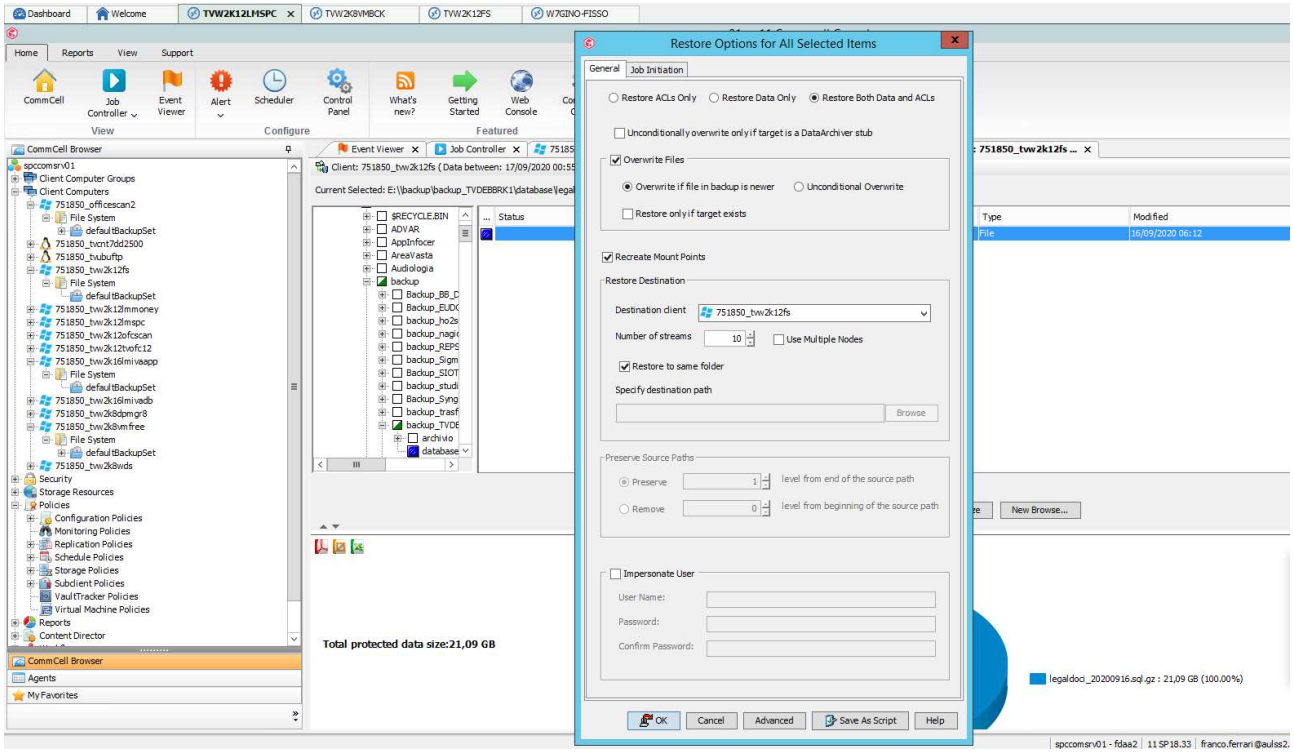
1) Copia delle conclusioni dell'ultimo test di restore.

Test di restore backup in cloud SPC

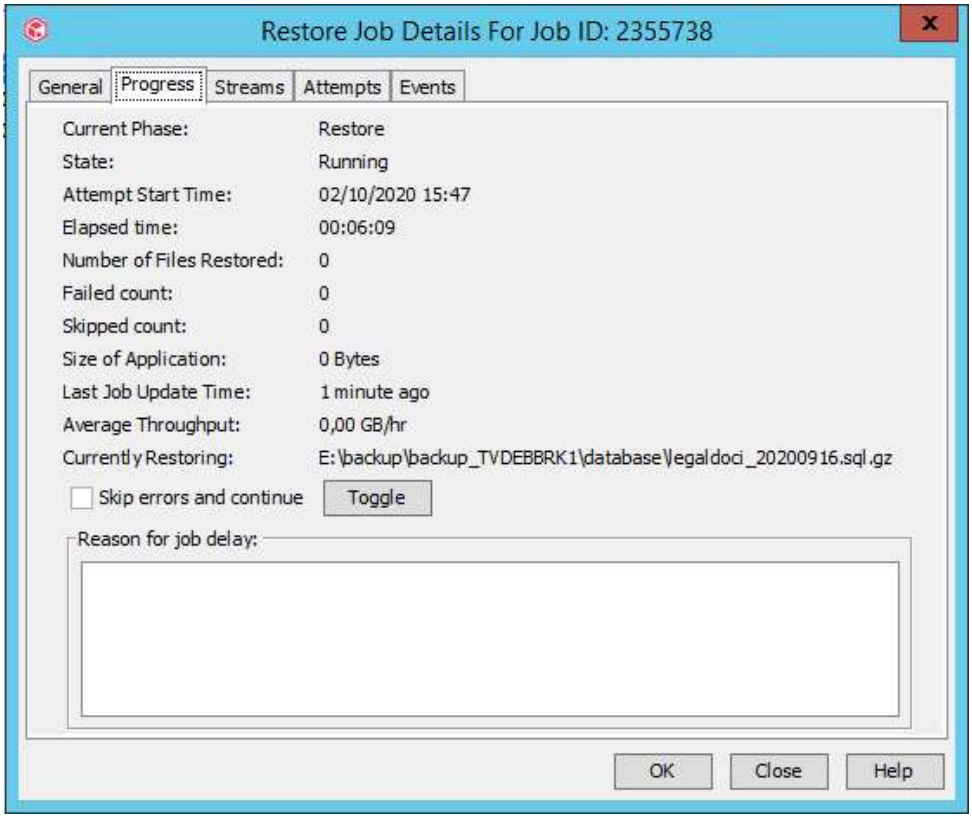
Si vuole eseguire il test di ripristino di un file di grosse dimensioni (circa 22 GB) eliminato dal percorso :

\\tvw2k12fs\dfs\backup\backup_TVDEBBRK1\database

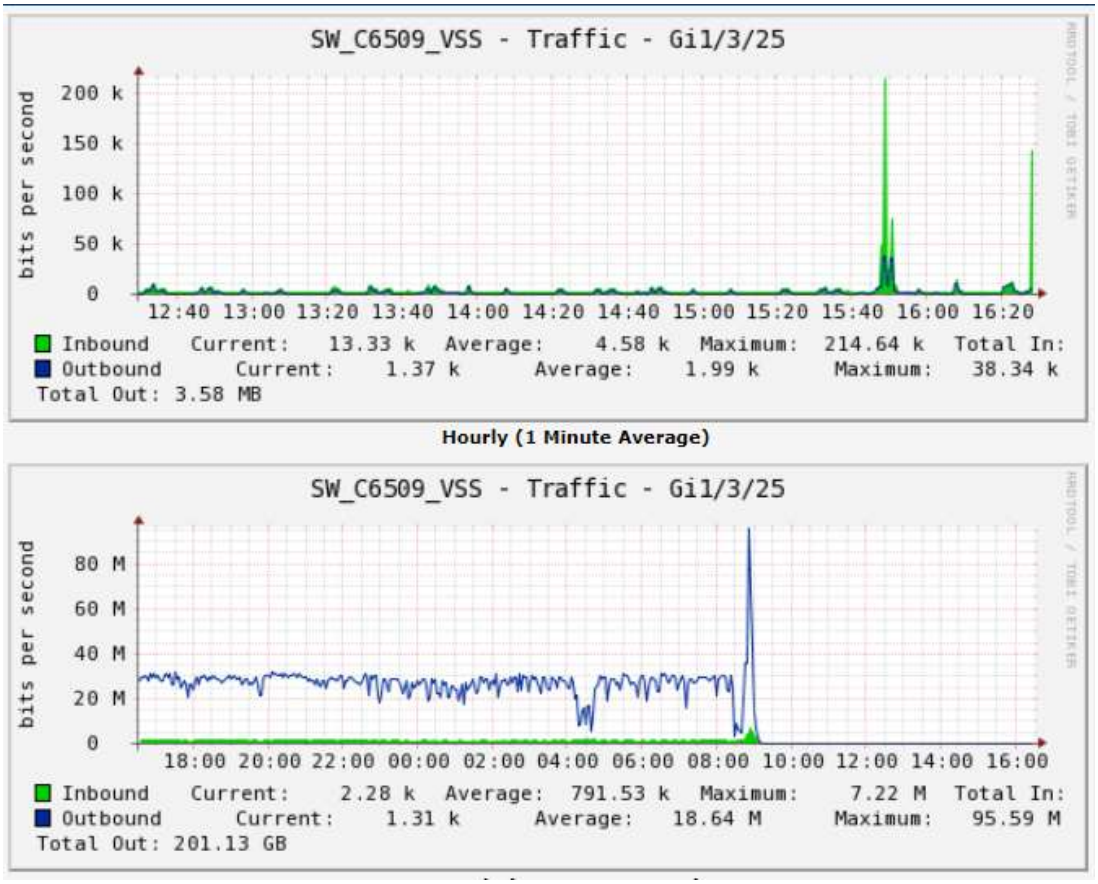
Vado ad sfogliare il backup fino al path desiderato e seleziono il file da recuperare :



Avvio del job di ripristino :

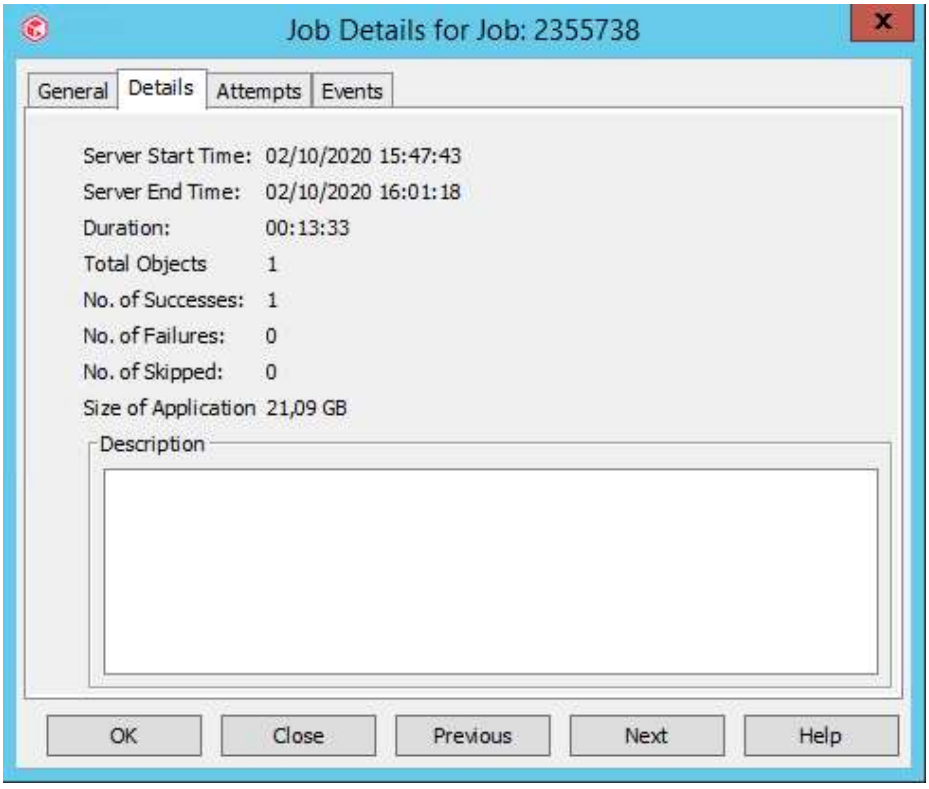


Carico sulla linea inbound durante il restore :



L'inbound del ripristino non è stato registrato nel secondo grafico in quanto non è durato abbastanza per registrare i valori nella scala oraria (asse X).

Dopo circa 13 minuti il job è terminato con esito positivo :



Ecco il file correttamente ripristinato :