CIRCOLARE TECNICA Prot. DC2022OC072 **DATA** Milano, 15-11-2022

A tutti i CAB accreditati e in corso di accreditamento per gli schemi SGQ (IAF 33), ITX, SSI e BCMS

Alle Associazioni degli Organismi di valutazione della conformità

A tutti gli Ispettori/Esperti di Accredia

Loro sedi

OGGETTO **Dipartimento Certificazione e Ispezione**

ERRATA CORRIGE Circolare tecnica DC N° 42/2022 - Disposizione in merito all'accreditamento per lo schema DSEEDC a fronte delle Norme ISO/IEC TS 22237 – Disponibilità, Sicurezza, Efficienza Energetica dei Data Center.

Le modifiche apportate alla presente circolare sono evidenziate in giallo

INTRODUZIONE

L'attuale scenario del mercato dell'UE rende sempre più centrale il tema della gestione dei dati. In questo ambito ha assunto un'importanza strategica anche la gestione delle strutture deputate a svolgere attività di "Data Center".

A questa esigenza dà una risposta efficace la serie di Norme ISO/IEC 22237, che comprende sette diverse Norme specializzate.

Le aree disciplinate sono rispettivamente:

- ISO/IEC 22237-1:2021 - Part 1: General concept;
- ISO/IEC TS 22237-2:2018 - Part 2: Building construction;
- ISO/IEC 22237-3:2021 - Part 3: Power distribution;
- ISO/IEC 22237-4:2021 - Part 4: Environmental control;
- ISO/IEC TS 22237-5:2018 - Part 5: Telecommunications cabling infrastructure;
- ISO/IEC TS 22237-6:2018 - Part 6: Security systems;
- ISO/IEC TS 22237-7:2018 - Part 7: Management and operational information.

CONTESTO NORMATIVO

La Norma ISO/IEC 22237, nelle sue diverse specializzazioni, si inserisce in un contesto che era già oggetto di presidio della Normazione Europea, attraverso la Norma precorritrice EN 50600, anch'essa strutturata in più documenti, pubblicata nel 2010 e, successivamente, aggiornata nel 2014.

Questa Norma, a tutt'oggi valida, offre ora una copertura completa per le migliori pratiche per i data center, dagli standard di progettazione, inclusi alimentazione, raffreddamento, telecomunicazioni e sicurezza (compresa la sicurezza contro gli incendi), agli standard operativi con attenzione agli aspetti di efficientamento energetico.

Si tratta di una Norma omnicomprensiva, che tratta di tutti gli aspetti tecnici inerenti il governo di un Data Center.

ELEMENTI SPECIFICI DELLA NORMA

La Norma ISO/IEC 22237 riceve in eredità dalla precedente EN 50600 la struttura modulare e anche la specializzazione dei contenuti, ma assume un valore "politico" di maggior respiro, essendo una Norma internazionale.

Le aree disciplinate sono rispettivamente:

- ISO/IEC 22237-1:2021 - Part 1: General concepts;
- ISO/IEC TS 22237-2:2018 - Part 2: Building construction;
- ISO/IEC 22237-3:2021 - Part 3: Power distribution;
- ISO/IEC 22237-4:2021 - Part 4: Environmental control;
- ISO/IEC TS 22237-5:2018 - Part 5: Telecommunications cabling infrastructure;
- ISO/IEC TS 22237-6:2018 - Part 6: Security systems;
- ISO/IEC TS 22237-7:2018 - Part 7: Management and operational information.

La Norma non è riferibile alla famiglia HLS, tipicamente certificabile con un approccio da sistema di gestione, bensì risulta idonea per una certificazione di prodotto, secondo la Norma di Accreditamento UNI CEI EN ISO/IEC 17065:2012.

In quest'ottica, il coacervo normativo può essere considerato come uno schema ibrido tra il prodotto (aspetti fisici e infrastrutturali dei Data Center) e il servizio (aspetti prestazionali degli stessi Data Center), con un cappello gestionale, offerto dalla parte 7, che è destinato a ben integrarsi con i sistemi di gestione per la qualità basati sulla ISO 9001:2015, ovvero con maggiore specializzazione con la Norma sulla qualità dei servizi IT (UNI CEI ISO/IEC 20000-1:2020), e con i sistemi di gestione per la sicurezza delle informazioni secondo la Norma ISO/IEC 27001:2013 (UNI CEI EN ISO/IEC 27001:2017).

Il processo di Accreditamento prende in considerazione le attività condotte dai CAB sulla base di uno schema olistico, descritto al paragrafo che segue.

Processo di Certificazione

REGOLE DI CERTIFICAZIONE	
Norma di Certificazione	ISO/IEC 22237 nella sua completezza (tutte le Norme della serie, nella versione applicabile).
Soggetti che possono richiedere la certificazione	La Certificazione è relativa ai Data Center e copre tutti i requisiti individuati dalle Norme di Certificazione sopra richiamate. Per richiedere la Certificazione a fronte delle Norme indicate, il Data Center deve essere già in possesso, per lo stesso ambito di applicabilità, della Certificazione del proprio sistema di gestione per la qualità a fronte della Norma ISO

	9001:2015, integrata dalla Norma ISO/IEC 27001:2013 e, possibilmente, dalle Norme ISO/IEC 20000-1:2018 e ISO 22301:2019.
Requisiti dello schema di certificazione	1. Per richiedere la Certificazione di un Data Center, lo stesso deve essere gestito sulla base dello schema che prevede, quali pre-requisiti: a. L'esistenza e la certificazione preliminare del sistema di gestione per la qualità, che copra il campo di applicazione delle attività dello stesso Data Center. Preferibilmente, il sistema di gestione integrato del Data Center deve essere conforme anche alle Norme ISO/IEC 20000-1 e alla Norma ISO 22301. Tutte le certificazioni debbono rigurdare l'intero perimetro per il quale è richiesta la certificazione DSEEDC; b. L'esistenza e la certificazione a fronte della Norma ISO/IEC 27001 del sistema di gestione per la sicurezza delle informazioni che copra il perimetro pertinente (fisico, logico e organizzativo), per il quale è richiesta la certificazione DSEEDC dello stesso Data Center; 2. Lo schema prevede la certificazione in fase progettuale e quella in fase operativa: a. Per la certificazione in fase progettuale, devono essere considerati le modalità previste (adeguatezza delle scelte progettuali) per rendere operativi tutti i requisiti Normativi, in conformità ai seguenti punti: i. Valutazione delle scelte progettuali a fronte dei requisiti Normativi e del tipo di servizio offerto; ii. Valutazione sulle modalità adottate per provvedere alla valutazione dei rischi ipotizzabili in sede progettuale (analisi dei rischi del processo di progettazione e dei processi di supporto); iii. Valutazione delle modalità previste per la formazione, coinvolgimento e consapevolezza delle Risorse Umane, in funzione dei rischi inerenti i processi nei quali saranno coinvolte. iv. Valutazione delle modalità previste per la selezione dei fornitori che provvederanno alle diverse fasi di realizzazione del Data Center, dal punto di vista della sicurezza (humint) e modalità previste per il loro monitoraggio; v. Valutazione delle modalità adottate per individuare e mantenere sotto controllo (mantenimento delle registrazioni) delle forniture di beni che richiedono certificazioni di prodotto (es.: marcature CE; livelli di attenuazione del segnale; livelli di efficienza ambientale/energetica; certificazioni di sicurezza IoT, per quanto applicabile); vi. Procedure di collaudo presidiato, reportistica richiesta (es.: test memoranda su materiali installati e su funzionamento e prestazioni); vii. Modalità adottate per garantire l'ispezionabilità, manutenibilità e sicurezza antintrusione delle infrastrutture, ivi compresi i cavedi; viii. Sviluppo di adeguate "Policies" per la realizzazione e l'esercizio di SOC e NOC dedicati al Data Center.

b. Per la certificazione operativa, sono previsti quattro livelli di maturità nell'applicazione delle Norme oggetto di Certificazione:
   i. Livello 1 – ingresso – le Norme della famiglia 22237 sono in fase di applicazione; livello non certificabile;
   ii. Livello 2 – applicazione – le Norme della famiglia 22237 sono applicate ma non ancora in modo efficace; livello non certificabile;
   iii. Livello 3 – conformità – le Norme della famiglia 22237 sono applicate garantendo la conformità a tutti i requisiti applicabili. L'applicazione delle Norme è integrata in un modello organizzativo sistemico, che deve comprendere la gestione dei servizi, la sicurezza delle informazioni e la sicurezza cibernetica rispettivamente a fronte delle Norme ISO/IEC 20000-1, ISO/IEC 27001 e a fronte della Norma ISO 22301;
   iv. Livello 4 – come livello 3 e livello di affidabilità "six nines" (99,9999% - max. 31.5 secondi di "down-time" annui;

3. Dovranno essere oggetto di valutazione, nell'ambito indicato, tutte le Norme della serie 22237 (da 1 a 7), senza esclusioni. L'estensione della Certificazione e relativo Accreditamento a tutte le Norme indicate è supportata, nonostante che alcune siano in stato di "TS", dal fatto che i relativi requisiti sono richiamati e funzionali all'applicazione di tutte le Norme citate sia integralmente, sia in modo incrociato come segue:
   a. ISO/IEC 22237-1 richiama la ISO/IEC 22237-6;
   b. ISO/IEC TS 22237-2 richiama le ISO/IEC 22237-(3, 4 e 6);
   c. ISO/IEC 22237-3 richiama le ISO/IEC 22237-(1,4 e 6);
   d. ISO/IEC 22237-4 richiama le ISO/IEC 22237-(1,3 e 6);
   e. ISO/IEC TS 22237-5 richiama le ISO/IEC 22237-(1. 2, 4 e 7);
   f. ISO/IEC TS 22237-6 richiama le ISO/IEC (1, 2, 3, 4, 5);
   g. ISO/IEC TS 22237-7 richiama tutte le precedenti;
4. Inoltre, tutte le Norme richiamano la filosofia applicativa che vede nella ISO/IEC 22237-7 il riferimento per la chiusura del ciclo di controllo operativo (anello cibernetico a ciclo chiuso, approccio di DEMING);
5. Nel caso di Data Center strutturati su più unità operative, tutte le unità dovranno essere oggetto di valutazione. La valutazione dell'aderenza ai diversi requisiti normativi deve prevedere una logica di campionamento robusta, atta a garantire la verifica dell'operatività di tali unità satellite, prevedendo il test dei controlli operativi che mitigano i rischi maggiori in ottica di efficacia del Data Center;
6. Il processo di Audit deve prevedere la verifica di tutti i requisiti Normativi, con focus primario sulle logiche di "risk management", che debbono essere basate sulla Norma (Guida) ISO 31000 e prevedere una valutazione di accettazione del rischio residuo funzionale al livello di operatività atteso e dichiarato del Data Center. Sulla base di tale valutazione dovranno essere progettati e sviluppati i controlli operativi. Tale campionamento robusto deve consentire di valutare in modo

inequivocabile le strutture e le loro prestazioni. Il campionamento dei requisiti deve garantire la rappresentatività nei confronti di tutto il Data Center, la presa in carico di parametri prestazionali (KPI e KRI), che evidenzino la validità delle scelte di governo dei processi. Il campionamento deve tener conto dei diversi aspetti governati (ambientali e di security in primo luogo), i processi che li gestiscono e i siti ove vengono realizzati tali risultati. Tali valutazioni dovranno essere riferite a tutti i requisiti delle sette Norme di riferimento, dando evidenza dei criteri utilizzati per l'individuazione degli obiettivi, dei risultati chiave che li sostengono, dei relativi KPI e KRI e, infine, dell'effettivo livello di raggiungimento degli obiettivi medesimi. Tutto ciò deve essere rendicontato dai CAB in ottica di conformità e di adeguatezza alle politiche dichiarate e rese pubbliche dalla Direzione;

7. Ove vi siano dei processi gestiti in outsourcing (es. manutenzioni) la direzione del Data Center deve dare evidenza dei criteri e strumenti adottati per garantire il controllo di tali processi, sui quali mantiene la completa responsabilità;
8. Lo schema di certificazione sviluppato dai CAB deve prevedere lo svolgimento di una validazione delle metodiche di valutazione dei rischi delle quali la direzione del Data Center si sarà dotata. Le indicazioni di buona tecnica per lo sviluppo della valutazione dei rischi dovranno essere individuate, in modo pertinente, tra quelle riportate dalla Norma (Guida Tecnica) ISO 31010;
9. Le tecniche di valutazione adottate dai CAB dovranno prevedere sia valutazioni documentali, sia de visu, sia interviste alla Risorse Umane che operano presso il Data Center, ivi comprese quelle dei processi dati in outsourcing (vedi il precedente § 4);
10. Il business del Data Center può prevedere in alternativa:
    a. Servizio di base, quale la semplice messa a disposizione di spazi, security antintrusione, alimentazione e raffrescamento e cablaggio interno al Data Center sino all'attestazione all'interfaccia con i "carrier" o con gli ISP individuati dal Cliente. Questo tipo di servizio prevede sotto la responsabilità del Data Center della realizzazione del cablaggio di connessione sino allo switch, a cui il Cliente connette le proprie macchine;
    b. L'erogazione di servizi avanzati, che comprendono il servizio base e la connettività (servizi di comunicazione "carrier telefonici o ISP") o l'erogazione di Servizi Cloud "aaS". In questi casi deve essere svolto con periodicità almeno semestrale, un Vulnerability Assessment da parte di un Laboratorio Accreditato e, sulla base delle indicazioni desumibili dalla valutazione dei rischi, anche degli specifici Penetration Test [Prescrizione valida sul territorio Italiano. Ove non disponibili tali LAB si tenga conto dei criteri seguenti: qualifica dei Tecnici di Laboratorio, aggiornamento dati base delle vulnerabilità, procedure che garantiscano un approccio di ripetibilità delle prove e supportate da buona tecnica riferita a modelli noti e condivisi]. In particolare, per l'erogazione dei servizi Cloud è richiesta l'adozione

	e certificazione del Data Center sulla base della valutazione dei rischi già menzionate ai fini della selezione e applicazione dei controlli operativi richiamati dalle Norme (Guide) ISO/IEC 27017 e ISO/IEC 27108, con perimetro pertinente ai servizi del Data Center, come già evidenziato. L'esecuzione dei Vulnerability Assessment da parte di Laboratori Accreditati non esime il gestore del Data Center dalla responsabilità della continua verifica della presenza e corretta correzione di vulnerabilità note e di errori di sistema che richiedono approfondimenti tecnici (ragione della richiesta di esistenza di SOC / NOC). La valutazione di terza parte è da considerare come un benchmark operativo a fronte di tali responsabilità; 11. Lo schema di certificazione deve prevedere un processo di valutazione dinamico dei fornitori di servizi critici per il Data Center, con riferimento ai requisiti dei servizi critici, a fronte delle Norme individuate in questa Circolare.
Possibili esclusioni	Lo schema non prevede esclusioni.
Criteri di competenza del Gruppo di verifica	Gli Auditor saranno qualificati a livello tecnico dagli stessi CAB (o possono essere certificati da CAB con Accreditamento PRS specifico), sulla base di: • Un'esperienza lavorativa di almeno 10 anni in ambito IT, dei quali 5 anni come Auditor SSI e ITX, con almeno tre audit su Data Center, comprendenti tutti i domini previsti dalla Norma ISO/IEC 22237, ovvero secondo standard di mercato assimilabili per completezza e complessità (a mero titolo di esempio, Ansi TIA 942, EN 50600, BICSI 002); • Il superamento di un corso specialistico sulle Norme della famiglia ISO/IEC 22237, della durata minima di tre giorni più esame, svolti da Ente riconosciuto come l'Ente Nazionale di Normazione o sulla base del "syllabus" da questo sviluppato.
Criteri di competenza del decision maker e del contract reviewer	I "decisori / deliberatori" devono avere le medesime conoscenze degli Auditor, ma non necessariamente il medesimo livello di competenza. Il personale addetto alla gestione contrattuale deve avere le stesse conoscenze degli Auditor, richiedendo l'approvazione degli aspetti tecnici delle offerte ai Responsabili di Schema, che debbono essere qualificati come Auditor nello specifico schema.
Tempi di audit	Per le certificazioni rilasciate in fase progettuale, si stima un tempo minimo di analisi pari a 8 gg/uomo. Tutte le attività di valutazione debbono prevedere, sia in fase progettuale, sia in fase operativa, almeno una giornata di valutazione preliminare (ST1), da svolgere anche da remoto, per la valutazione del livello di preparazione dell'organizzazione per sostenere la valutazione di certificazione. Gli audit di certificazione debbono essere svolti in campo, ivi comprese le attività di valutazione dei siti satelliti. Eventuali attività da remoto devono essere giustificate con una specifica valutazione dei rischi da parte del CAB, che rimarrà agli atti a disposizione di ACCREDIA, per le valutazioni necessarie. Dei siti remoti, sarà sempre richiesto un campionamento in

	presenza di almeno il 50%, ma con supporto di valutazione dei rischi specifica. Per le certificazioni rilasciate in fase di progetto sono previsti da 2 a 4 gg/uomo di attività, che il CAB dovrà valutare sulla base della complessità del DC e dei servizi erogati. Per le certificazioni rilasciate in fase operativa, per le sole Norme della famiglia ISO/IEC 22237, si prevedono otto giorni lavorativi, più il tempo necessario per i campionamenti dei siti secondari (tutti in fase di certificazione e rinnovo, anche se non con pari intensità, e secondo MD1 in fase di sorveglianza), con un minimo di un giorno lavorativo per ogni sito, considerando che presso tali siti dovranno essere previsti dei piani di test della funzionalità dei sistemi in relazione ai requisiti normativi. I test saranno condotti secondo una logica di campionamento studiata dal CAB, in collaborazione con DC, ma sempre nella sola responsabilità del CAB. Tale attività deve prevedere e garantire la valutazione (test) di tutti i controlli operativi destinati a mitigare i rischi con magnitudo tale da superare o raggiungere il livello di tolleranza al rischio del DC (sia a livello economico, sia a livello giuridico, sia come reputazione). Il CAB è responsabile di produrre e conservare ai fini delle verifiche di ACCREDIA la valutazione dei rischi sul processo di certificazione, i suoi aggiornamenti sulla base dell'esperienza e le conseguenti valutazioni operative sulle necessità di incremento dei tempi di audit sopra menzionati (es. per chiusura rilievi che comportino valutazioni su più siti). Non sono ammesse riduzioni sui tempi di audit indicati. I CAB debbono considerare nelle proprie offerte un giorno uomo aggiuntivo per la programmazione e pianificazione degli audit in fase di progetto e due giorni aggiuntivi per la programmazione e pianificazione degli audit in fase operativa. Non sono ammesse riduzioni di alcun tipo del tempo di audit sopra individuato.
Modalità di svolgimento dell'audit	La documentazione di audit, deve riportare, fra le altre registrazioni, anche quanto segue: ▪ il perimetro e l'applicabilità del Sistema di Gestione ISO/IEC 22237; ▪ l'analisi di contesto; ▪ la mappatura dei processi (interni ed esterni) e l'elenco delle relative leggi, Norme e regolamenti applicabili; ▪ la valutazione dei rischi per il campo di applicazione specifico del Data Center, con riferimento a tutti i processi, anche ai processi dati in outsourcing; ▪ l'analisi degli "incidents" e "problems" già occorsi, completata dalla valutazione sulle modalità di gestione previste e adottate, alla luce delle indicazioni delle Autorità (EDPB – Garante per la protesione dei Dati Personali) e delle Norme esistenti applicabili ISO/IEC 27035 e ISO/IEC 27043;

	▪ La definizione ragionata degli obiettivi, dei risultati chiave che li sostengono, dei relativi KPI e KRI e le relative attività di pianificazione.
Scopo del certificato	Certificazione della Disponibilità, Sicurezza fisica, logica e organizzativa, Efficienza Energetica delle Infrastrutture e Processi di Supporto dei Data Center [XXX] costituito da: [Sito principale; sito secondario; sito secondario…].
Documenti IAF applicabili	IAF MD 01, 02, 04 e 05 [non si applicano criteri ASRP].

PROCESSO DI ACCREDITAMENTO

Le verifiche necessarie per il rilascio di certificazioni ISO/IEC 22237 devono essere condotte da Organismi di certificazione accreditati secondo la Norma UNI ISO/IEC 17021-1.

Il certificato di accreditamento è rilasciato senza alcuna limitazione settoriale.

Si potranno presentare diverse casistiche, in base agli accreditamenti ACCREDIA già posseduti dall'Organismo di Certificazione che presenta la domanda di accreditamento o estensione.

Nel caso in cui il CAB possegga già accreditamenti rilasciati da altri Enti di Accreditamento, deve essere effettuata una valutazione caso per caso, in base agli accordi EA / IAF MLA applicabili.

Rimangono invariati i prerequisiti previsti dal RG-01 ed RG-01-03 per la concessione dell'accreditamento ed estensione, integrati dalle seguenti regole.

ITER DI ACCREDITAMENTO/ESTENSIONE		
Inf.	L'Accreditamento per lo schema DSEEDC verrà rilasciato a fronte della Norma UNI CEI EN ISO/IEC 17065:2012. Potranno presentare domanda di accreditamento solamente i CAB già accreditati secondo la Norma UNI CEI EN ISO/IEC 17021-1:2015, per gli schemi SGQ (IAF33), ITX, SSI e BCMS.	
Stante il precedente Accreditamento a fronte degli schemi SGQ (IAF33) ITX, SSI e BCMS:		
A	CAB già in accreditati in conformità alle Norme ISO/IEC 17065:2012 e ISO/IEC 17021-1:2015 per gli schemi SGQ (IAF 33), ITX, SSI e BCMS.	Esame documentale di 0,5 gg/uomo da remoto. 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
B	Il CAB già accreditato in conformità alla Norma ISO/IEC 17021-1:2015 per gli schemi SGQ (IAF 33), ITX, SSI e BCMS, ma non alla ISO/IEC 17065:2012.	Esame documentale di 1,5 gg/uomo (da effettuarsi, almeno in parte, in remoto). Verifica presso la sede del CAB di 2 gg/uomo, da effettuarsi o in presenza o da remoto.

		1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
	CAB non accreditato per la Norma ISO/IEC 17021-1 né per la Norma ISO/IEC 17065.	Si proceda, in primo luogo, sia all'accreditamento SGQ (IAF 33), sia ITX, SSI e BCMS, quindi si passi al riquadro immediatamente sopra.

DOCUMENTAZIONE DA PRESENTARE AD ACCREDIA PER L'ESAME DOCUMENTALE

Documentazione da presentare ad ACCREDIA per l'esame documentale:

a) Regolamento Generale per la Norma ISO/IEC 17065:2021 e Regolamento Particolare di schema;
b) Lista di riscontro o linea guida o istruzioni predisposte dall'OdC per il GVI;
c) Criteri di qualifica di chi effettua il riesame del contratto, degli Auditor e dei decision maker;
d) Curricula degli Ispettori e dei decision maker e giustificazione per la loro singola qualifica;
e) Procedura per la costituzione e gestione dei Gruppi di Audit;
f) Attestato/Certificato rilasciato dall'OdC;
g) Lista dei certificati già emessi, e delle prossime attività di verifica (dato necessario per poi pianificare la verifica in accompagnamento);
h) Procedure / regolamenti contrattuali applicabili alla verifica, nonché le procedure interne per la gestione della pratica di certificazione (dall'offerta alla Certificazione).

MANTENIMENTO DELL'ACCREDITAMENTO

Per il mantenimento dell'accreditamento, durante l'intero ciclo di accreditamento, salvo situazioni particolari (es: gestione reclami e segnalazioni, modifiche intervenute sullo schema di certificazione, cambiamenti nella struttura dell'Organismo o altre situazioni similari), verranno condotte le seguenti verifiche:

- se l'OdC ha emesso meno di 50 certificati nello schema di certificazione, devono essere effettuate una verifica in accompagnamento e 1 verifica in sede;
- se l'OdC ha emesso tra 51 e 200 certificati nello schema di certificazione, devono essere effettuate 2 verifiche in accompagnamento e 1 verifica in sede;
- se l'OdC ha emesso più di 201 certificati nello schema, devono essere effettuate 2 verifiche in accompagnamento e 2 verifiche in sede.

L'occasione è gradita per porgere cordiali saluti.

Dott. Emanuele Riva

Direttore Dipartimento
Certificazione e Ispezione

Firmato digitalmente da:
EMANUELE RIVA
Data: 15/11/2022 12:28:46