Allegato A)

Protocollo di intesa per la collaborazione scientifica propedeutica alla costituzione e all' avvio

di

un Centro regionale CSIRT (*Computer Security Incident Response Team*) Toscana

TRA

Regione Toscana

E

Centro di Competenza in Cybersecurity Toscano C3T [approvato con Delibera n.4 del 08-01-2018 Regione Toscana]

E

Scuola IMT Alti Studi di Lucca

E

Università degli Studi di Firenze

E

Università degli Studi di Siena

E

C.N.R. - Consiglio Nazionale delle Ricerche

E

Università di Pisa

E

Scuola Normale Superiore

E

Scuola Superiore di Studi Universitari e di Perfezionamento Sant'Anna

Vista la Comunicazione della Commissione europea COM (2010) 245 del 26.08.2010 su "Un'agenda digitale europea";

Vista la Comunicazione della Commissione europea COM (2016) 178 del 19.4.2016 su iniziativa europea per il *cloud computing*. Costruire una economica competitiva dei dati e della conoscenza in Europa;

Vista la Comunicazione della Commissione europea COM (2017) 228, del 10.5.2017 su Revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti, al cui punto 3.3. prevede di promuovere la realizzazione di ecosistemi informatici affidabili: affrontare insieme le sfide della sicurezza informatica;

Preso atto del Documento elaborato dai rappresentanti dagli Organismi di ricerca, che propone la costituzione di un Centro regionale sulla cybersecurity, con una ipotesi di attività diretta alle imprese e alle pubbliche amministrazioni;

Vista la Delibera n.4 del 08-01-2018 Regione Toscana che approva la costituzione di un Centro regionale sulla cybersecurity per le PMI e la Pubblica Amministrazione in attuazione della strategia regionale industria 4.0 e dell'agenda digitale regionale;

Visto lo schema di protocollo di intesa tra Regione Toscana e Università degli Studi di Firenze, Università di Pisa, Università degli Studi di Siena, C.N.R. - Consiglio Nazionale delle Ricerche, Scuola IMT Alti Studi di Lucca, finalizzato alla costituzione di un Centro regionale sulla cybersecurity (C3T) per le PMI e la Pubblica Amministrazione in attuazione della Strategia Regionale Industria 4.0 e dell'Agenda Digitale Regionale approvato con Delibera di Giunta regionale n. 4 del 08.01.2018;

Premesso che la Regione Toscana ha realizzato e mette a disposizione delle amministrazioni toscane il *data center* regionale TIX, progettato e realizzato secondo i migliori standard internazionali, attraverso il quale vengono erogati servizi applicativi per la Regione Toscana e gli enti del territorio;

Premesso che il piano nazionale per la protezione cibernetica e la sicurezza informatica del 2017 - Ind. Op. 5, prevede: a) di sviluppare un modello standardizzato di gestione degli eventi cibernetici, in particolare per la fase di triage; b) di incrementare l'efficacia dell'azione dei CERT ("*Computer Emergency Response Team*") verso le rispettive *constituency*;

Visto l'avviso n.3/2022 dell'Agenzia per la cybersicurezza nazionale (ACN) per la presentazione di proposte per la realizzazione di interventi di potenziamento della resilienza cyber a valere sul PNRR "Missione 1 - Componente 1 - Investimento 1.5 Cybersecurity";

Considerata la Circolare dell'Agenzia per l'Italia Digitale n. 2 del 18 aprile 2017 recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)» (G.U. n.103 del 5-5-2017);

Considerate altresì le *"Linee Guida per la sicurezza delle informazioni Regione Toscana"* mirate a consentire a tutte le strutture della Regione Toscana di perseguire gli obiettivi generali di rispetto delle misure di sicurezza idonee a tutelare il proprio patrimonio informativo e nello specifico nella risposta omogenea all'obiettivo del rispetto del GDPR nei casi di trattamenti di dati personali.

Ritenuta di interesse comune la promozione della costituzione, da parte degli organismi di ricerca presenti sul territorio regionale, di un Centro regionale sulla cybersecurity orientato alla sicurezza informatica delle imprese e della Pubblica Amministrazione;

Ritenuto pertanto opportuno condividere il processo di messa in rete delle varie articolazioni delle competenze e delle infrastrutture di ricerca regionali del sistema della ricerca regionale in materia di cybersecurity, al fine di:

- mettere a disposizione degli Enti e delle pubbliche amministrazioni del territorio toscano aderenti al progetto il sistema delle competenze e delle infrastrutture di ricerca;

- valorizzare anche a livello nazionale ed europeo il sistema di competenze regionale in materia di cybersecurity;

- condividere le attività di divulgazione che il Centro potrà attivare per favorire e promuovere la conoscenza delle problematiche e delle soluzioni connesse al tema della cybersecurity nell'ambito dei processi di digitalizzazione.

Tutto ciò premesso le Parti convengono quanto segue:

ART. 1
Premesse

Le premesse fanno parte integrante del presente Protocollo di Intesa, che costituisce il presupposto su cui si fonda il consenso tra le Parti per realizzare una attività condivisa finalizzata alla costituzione di un Centro regionale sulla cybersecurity, quale forma di coordinamento tra le Parti sottoscrittrici del presente Protocollo di intesa.

ART. 2
Oggetto

1. Le Parti, con il presente Protocollo di intesa, mediante il Centro di Competenza in Cybersecurity Toscano (C3T), ed in particolare tramite la Scuola IMT Alti Studi di Lucca che coordina le attività nell'ambito della sicurezza informatica svolte all'interno dei dipartimenti e degli istituti delle Parti, convengono di porre in essere un'attività condivisa propedeutica alla costituzione di un CSIRT (*Computer Security Incident Response Team*) regionale, e mirata al supporto tecnico e scientifico agli Enti del territorio toscano per l'identificazione di vulnerabilità ICT e possibili minacce, la valutazione e il potenziamento delle capacità di difesa sulla base dei fabbisogni di cybersecurity rilevati.

2. Il CSIRT (*Computer Security Incident Response Team*) Toscana gestirà eventuali situazioni di violazione alla sicurezza informatica e in particolare assolverà le seguenti funzioni:

- monitoraggio e aggiornamento delle evoluzioni delle minacce alla sicurezza e della tecnologia di protezione, fornisce informazioni sulle vulnerabilità di sicurezza, le intrusioni informatiche, i virus o altre minacce;
- redazione di linee guida per la realizzazione e l'erogazione dei servizi con adeguati livelli di sicurezza e indica le modalità di comportamento per la gestione dei problemi;
- monitoraggio e verifica della possibilità di attacchi o intrusioni informatiche e verifica periodicamente lo stato di sicurezza delle infrastrutture per azioni correttive e/o migliorative;
- offerta di attività formative e di sensibilizzazione sui temi della sicurezza informatica e servizi di consulenza sul Risk Management nell'ambito della cybersecurity.

Svolgerà inoltre un ruolo di coordinamento di interventi degli Enti, dei SOC e dei vari attori coinvolti a seguito di incidenti di sicurezza.

3. Gli ambiti di attività oggetto del presente Protocollo e propedeutici all'avvio e consolidamento del Centro per la cybersecurity in Toscana concernono:

a. la validazione a livello scientifico e metodologico del modello organizzativo e delle attività previste dal Centro;
b. il supporto scientifico al coordinamento ed alla pianificazione e allo svolgimento delle attività del Centro;
c. le attività di formazione e sensibilizzazione sulle problematiche legate alla cybersicurezza agli stakeholders del Centro.

4. Il CSIRT Toscana dovrà curare il trasferimento di know-how, la formazione, la consulenza, l'erogazione dei servizi operativi e informativi e il supporto alle Pubbliche Amministrazioni locali, ai cittadini, alle imprese e alle aziende del territorio, in stretta collaborazione con le infrastrutture nazionali dedicate e con l'Agenzia per la cybersicurezza nazionale (ACN).

5. Il CSIRT Toscana rappresenterà un'entità più vicina agli Enti Locali in senso geografico, operando, da un lato, come struttura di supporto verso le stesse e, dall'altro, fungendo da elemento di raccordo fra periferia e centro (CSIRT Italia ed ACN).

6. Il CSIRT Toscana potrà poi essere interconnesso con i diversi SOC presenti nei vari ambiti, ad esempio il SOC del Sistema Cloud Toscana, ed altri SOC che saranno attivati in ambiti specifici (su sanità, su ambiti comunali o intercomunali).

ART. 3

Nucleo tecnico di coordinamento

1. È costituito un Nucleo tecnico di coordinamento composto da n.1 rappresentante per ciascuno degli Organismi di ricerca sottoscrittori e dai rappresentanti regionali, nello specifico, dal direttore della Direzione Sistemi Informativi, Infrastrutture tecnologiche e innovazione, dal Direttore della Direzione Sanità, Welfare e Coesione, dal C.I.S.O. (*Chief information security officer*) di Regione Toscana e dall'Amministratore Unico del Consorzio Metis, con il compito di verificare e monitorare le attività previste dal presente protocollo di intesa.

2. I componenti del Nucleo di coordinamento si riuniscono, con cadenza semestrale, anche in modalità *mista*, per esaminare collegialmente programmi, piani di attività, proposte di intervento, obiettivi da perseguire e per lo svolgimento delle attività di cui al comma 1 del presente articolo.

ART. 4
Costituzione di un board di governance

1. Nelle more della costituzione di un CSIRT (*Computer Security Incident Response Team*) regionale le Parti convengono di costituire un *board di governance* articolato e strutturato su più livelli per la ripartizione delle funzioni di indirizzo, di direzione e controllo, nonché le funzioni di supporto scientifico/metodologico alle iniziative svolte e tecnico/operative per il corretto funzionamento del CSIRT regionale.

2. Il modello di Governance del CSIRT (*Computer Security Incident Response Team*) regionale sarà organizzato su tre livelli:

- 1° livello (strategico-direttivo): composto da Regione Toscana, nella persona del Direttore della Direzione Sistemi informativi Infrastrutture digitali e Innovazione e dal C.I.S.O. (*Chief information security officer*) di Regione Toscana, nonchè dal direttore della Direzione Sanità, Welfare e Coesione, sentito il Nucleo tecnico di coordinamento di cui all'art. 3 del presente protocollo di intesa. Questa struttura è responsabile di fornire l'indirizzo strategico sulle politiche di conduzione del CSIRT regionale e, al contempo, di indirizzare la strategia definita, definendo processi e procedure che garantiscano il raggiungimento degli obiettivi prefissati.

- 2° livello (supporto scientifico-metodologico): rappresentato da un Comitato tecnico-scientifico composto dai referenti degli organismi di ricerca già facenti parte del Centro C3T Regionale (Scuola Alti Studi IMT di Lucca, Università di Pisa, il C.N.R. - Consiglio Nazionale delle Ricerche di Pisa, Università degli Studi di Firenze e Università degli Studi di Siena, nonché dalla Scuola Normale Superiore e dalla Scuola Superiore di Studi Universitari e di Perfezionamento "Sant'Anna", anch'esse aderenti al presente Protocollo di Intesa. Questo

Comitato ha il compito di supportare a livello tecnico scientifico e metodologico le attività e le iniziative svolte in seno al CSIRT regionale.

 3° livello (operativo): operato da Consorzio Metis, SOC ed esperti cyber rappresentanti degli Enti aderenti al Consorzio Metis. Questa struttura è responsabile dell'implementazione e della manutenzione dei processi e delle procedure definite a livello direttivo.

3. In sede di successiva progettazione esecutiva, che sarà curata dalla Direzione Sistemi Informativi, Infrastrutture tecnologiche e Innovazione , saranno dettagliati i servizi inclusi nella soluzione di CSIRT (*Computer Security Incident Response Team*) Toscana, precisati i ruoli, i tempi di attuazione, le responsabilità e le modalità di funzionamento del modello organizzativo proposto, i processi di attivazione e coordinamento per la gestione di eventuali incidenti di sicurezza, le regole e i costi di gestione, i modelli di adesione e di partecipazione alla spesa e la dettagliata ripartizione dei costi.

4. Regione Toscana, con il supporto del Consorzio Metis, assolve un ruolo di coordinamento e direttivo nella fase di implementazione della soluzione, per la formalizzazione del progetto esecutivo (servizi inclusi nella soluzione di CSIRT Regionale, modello organizzativo e di *governance*, processi di attivazione e coordinamento per la gestione di eventuali incidenti di sicurezza), nonché nella manutenzione e gestione della soluzione nella fase attuativa. Inoltre, sulla base del proprio ruolo e dei mandati normativi, Regione Toscana potrà intervenire a supporto delle attività locali in carico a singoli Enti aderenti al Consorzio. Regione Toscana contribuisce inoltre alla realizzazione delle linee di intervento e delle attività al loro interno specificate mettendo a disposizione un gruppo di lavoro per il coordinamento del progetto.

5. Il CSIRT Toscana, con il supporto a livello operativo del Consorzio Metis, dovrà coordinare e supportare rispettivamente enti sanitari e comuni nella gestione della propria sicurezza, fungendo anche da collettore e centralizzatore di alcuni servizi di sicurezza che potranno quindi essere integrati con il CSIRT regionale, nelle modalità che saranno definite nel progetto esecutivo.

6. Sarà inoltre attuata una costante correlazione ed integrazione con altri Enti/Società che ne facciano richiesta o che in futuro intratterranno rapporti con Regione Toscana, quali CSIRT Italia, il CNAIPIC, la Polizia di Stato.

7. Sono fatte salve, in sede di successiva progettazione esecutiva, eventuali variazioni all'assetto di *governance* delineato al comma 2 dell'art. 4 del presente Protocollo di Intesa.

ART. 5
Impegni della Regione Toscana

1. La Regione, nel quadro degli strumenti di programmazione, si impegna a promuovere, a seguito del loro esame, le attività del Centro previste di cui all'art. 2 del Protocollo di Intesa, e in particolare:

a. la definizione delle procedure operative a livello regionale sulle infrastrutture, in raccordo con l'Agenzia per la cybersicurezza nazionale (ACN), sentiti gli indirizzi e le proposte del Comitato tecnico-scientifico di cui al co. 2 dell'art. 4 del presente protocollo di intesa;

b. individuazione di uno o più sedi operative, ove realizzare attività specializzate a supporto delle imprese e delle pubbliche amministrazioni;

c. valutazione di forme di cofinanziamento delle attività del Centro nel quadro degli strumenti di intervento (progetti di ricerca, borse di studio e ricerca, assegni di ricerca, borse di dottorato Pegaso, infrastrutture di ricerca e dimostratori tecnologici);

d. azioni di supporto alla attivazione di scambi di buone pratiche e attività di collaborazione fra i soggetti firmatari e istituzioni di ricerca, e pubbliche amministrazioni su scala nazionale e internazionale;

e. attivazione di accordi di collaborazione scientifica per la realizzazione di studi e approfondimenti sul tema della cybersecurity, sulle potenziali aree di applicazione in Toscana e sui fabbisogni delle imprese, degli organismi di ricerca e delle pubbliche amministrazioni;

f. valorizzazione e promozione delle competenze presenti in Toscana sulla cybersecurity anche attraverso l'Osservatorio per la Ricerca e Innovazione e il portale di promozione dell'osservatorio, toscanaopenresearch.it.

2. Regione Toscana si impegna a svolgere e porre in essere le azioni di indirizzo strategico – direttivo e decisionale, previste all' art 4 comma 2, mirate al raggiungimento degli obiettivi prefissati.

ART. 6
Impegni degli Organismi di ricerca

1. Gli Organismi si impegnano a svolgere le seguenti attività:

a. elaborare una proposta operativa di costituzione del Centro, nel rispetto dei rispettivi ordinamenti e tenendo conto dello stato dell'arte della ricerca sulla cybersicurezza e sui centri di risposta ad attacchi cyber a livello internazionale, da sottoporre all'esame dei rispettivi organismi di governo e della Regione Toscana (organo di 1° livello direttivo/strategico), comprensivo di un indicativo piano dei costi;

b. supportare a livello scientifico e metodologico la pianificazione e allo svolgimento delle attività del CSIRT Toscana;

c. presentare un programma biennale delle attività in programma e degli obiettivi da raggiungere, che saranno poi dettagliate nei piani di attività annuali da sottoporre all'esame della Regione e concernenti le seguenti attività-supporto tecnico scientifico alle imprese, agli organismi di ricerca, alle pubbliche amministrazioni e ai cittadini;

d. redazione di progetti di ricerca e trasferimento da presentare su bandi regionali, nazionali e della Commissione europea;

e. accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e migliorare le attività di sensibilizzazione su questi temi mediante individuazione di possibili percorsi di alta formazione sul tema della cybersecurity;

f. collaborazione con la Regione nella predisposizione di percorsi di formazione ed educazione in materia di cybersecurity.

ART. 7
Modalità di attuazione

1. Per ogni iniziativa e/o attività del presente Protocollo d'Intesa che perseguano un interesse generale, le Parti firmatarie concorderanno i reciproci impegni con successivo accordo esecutivo di carattere tecnico, eventualmente anche di carattere finanziario, in relazione alle specifiche attività progettuali da svolgere nell'ambito degli obiettivi previsti nell'art. 2 del presente Protocollo d'Intesa.

ART. 8
Riservatezza e trattamento dati personali

1. Le Parti, qualora le attività oggetto del presente Protocollo di Intesa comportino un trattamento di dati personali, tratteranno in via autonoma i dati personali oggetto dello scambio per trasmissione o condivisione, per le finalità connesse all'esecuzione del presente Protocollo di Intesa.

2. Le Parti, in relazione agli impieghi dei predetti dati nell'ambito della propria organizzazione, assumeranno, pertanto, la qualifica di Titolare autonomo del trattamento ai sensi dell'articolo 4, nr. 7) del GDPR, sia fra di loro che nei confronti dei soggetti cui i dati personali trattati sono riferiti.

3. I dati personali oggetto del trattamento potranno riguardare e dovranno essere distinti a seconda della tipologia dei dati personali (es: dati comuni), le categorie degli interessati (es: professionisti, titolari imprese, rappresentanti legali, personale dipendente ditte interessate) e la tipologia del formato dei dati (es: testo, immagini).

4. Il trattamento dei dati personali sarà inoltre improntato ai principi di correttezza, liceità e tutela dei diritti degli interessati, e sarà relativo ai dati strettamente necessari, non eccedenti e pertinenti alle finalità di cui all'art.2.

5. I dati personali oggetto del trattamento potranno riguardare:
- tipologia dei dati personali: dati comuni dei soggetti coinvolti nell'organizzazione delle attività di cui all'art. 1 (dati identificativi e di contatto)
- categorie degli interessati: dipendenti delle amministrazioni, professionisti, titolari e rappresentanti legali delle aziende, personale dipendente delle aziende interessate, cittadini;
- tipologia del formato dei dati: dati in formato testuale.

6. Le Parti si danno reciprocamente atto che le misure di sicurezza messe in atto al fine di garantire lo scambio sicuro dei dati sono adeguate al contesto del trattamento. Al contempo, le Parti si impegnano a mettere in atto ulteriori misure qualora fossero da almeno una delle Parti ritenute insufficienti quelle in atto e ad applicare misure di sicurezza idonee e adeguate a proteggere i dati personali trattati in esecuzione del presente protocollo, contro i rischi di distruzione, perdita, anche accidentale, di accesso o modifica non autorizzata dei dati o di trattamento non consentito o non conforme alle finalità ivi indicate.

7. Le Parti si impegnano – laddove richiesto e nel rispetto della legislazione vigente – alla riservatezza sui dati e su quanto venuto a conoscenza durante l'esecuzione del presente Protocollo di intesa, impegnandosi – sin dalla data di sottoscrizione – a non divulgare notizie riservate, elaborati

progettuali, ricerche e dati statistici frutto delle attività comuni, senza il reciproco e preventivo accordo scritto.

8. La Regione attesta la messa in atto delle seguenti misure: con l'approvazione della delibera n. 521 del 23 aprile 2019 e con il conseguente decreto dirigenziale n. 7677 del 17 maggio 2019, la Giunta regionale della Toscana si è dotata della propria Data Protection Policy, rinvenibile sul sito web (https://www.regione.toscana.it/-/ecco-la-data-protection-policy-di-regione-toscana).

9. Al contempo, le Parti si impegnano a mettere in atto ulteriori misure qualora fossero da almeno una delle due Parti ritenute insufficienti quelle in atto. L'eventuale diniego dell'altra Parte comporta l'annullamento del presente Protocollo di Intesa.

10. Le Parti si garantiscono reciprocamente che i dati trattati da ciascuna di esse in esecuzione del presente Protocollo di intesa formano oggetto di puntuale verifica di conformità alla disciplina rilevante in materia di trattamento di dati personali - ivi compreso il GDPR - e si impegnano altresì alla ottimale cooperazione reciproca nel caso in cui una di esse risulti destinataria di istanze per l'esercizio dei diritti degli interessati previsti dall'articolo 12 e ss. del GDPR ovvero di richieste delle Autorità di controllo che riguardino ambiti di trattamento di competenza dell'altra parte.

11. Con riguardo al trattamento dei dati personali, con la sottoscrizione del presente Protocollo di Intesa, le Parti dichiarano di essersi reciprocamente comunicate tutte le informazioni previste dagli artt. 13 e 14 del Regolamento UE 2016/679.

ART. 9
Controversie

Per tutte le controversie derivanti dall'interpretazione o dall'esecuzione del presente Protocollo, le Parti procederanno per via amministrativa, dopo aver esperito e senza alcun risultato, un tentativo di bonaria composizione extragiudiziale.
Nel caso in cui non si dovesse pervenire ad un accordo, competente per eventuali controversie, è il Foro di Firenze.
Per quanto posso occorrere, restano comunque salve le competenze inderogabili previste dalle applicabili disposizioni di legge.

ART. 10
Registrazione

1. Il presente Protocollo è soggetto a registrazione solo in caso d'uso ai sensi degli artt. 5, 6 e 39 del D.P.R. n. 131 del 26 aprile 1986 e non è soggetto ad imposta di bollo ai sensi e per lo effetto del D.P.R. 642/72 e successive modifiche ed integrazioni. Le spese per l'eventuale registrazione sono a carico della Parte richiedente.

2. Il Protocollo avrà piena efficacia a decorrere dalla data della sua sottoscrizione anche a mezzo di firma digitale ai sensi e nel rispetto del D.P.C.M. del 22 Febbraio 2013, pubblicato sulla G.U. n. 117 del 21 Maggio.

ART. 11
Modifiche ed integrazioni

1. Eventuali modifiche sostanziali al presente Protocollo di Intesa potranno essere apportate con il consenso unanime delle Parti.
2. Eventuali variazioni non sostanziali che si dovessero rendere necessarie in fase di progettazione o di attuazione di quanto previsto potranno essere approvate, senza che ciò determini variazioni al presente protocollo e saranno oggetto dell'esame e approvazione da parte del Dirigente responsabile del procedimento.

ART. 12
Validità del protocollo di intesa

1. Il presente Protocollo ha validità di due anni a decorrere dalla data di sottoscrizione e potrà essere prorogato di comune accordo tra le Parti.

2. In caso di recesso restano salve le eventuali iniziative già avviate congiuntamente, salvo che le Parti di comune accordo non decidano diversamente.

Letto, approvato e sottoscritto

Firenze lì..... 2023

Per Regione Toscana
Il Direttore
Ing. Gianluca Vannuccini

VANNUCCINI GIANLUCA
28.09.2023 14:57:42
GMT+01:00

……

Per Centro di Competenza in Cybersecurity Toscano C3T*
Il Direttore
Prof. Rocco De Nicola

……

Per Scuola IMT Alti Studi Lucca*
Il Rettore
Prof. Rocco De Nicola

IMT SCUOLA ALTI STUDI LUCCA

Firmato digitalmente da: DE NICOLA ROCCO
Data: 23/08/2023 16:47:16

Per Università di Pisa
Il Rettore
Prof. Riccardo Zucchi

……

Per C.N.R. - Consiglio Nazionale delle Ricerche
La Presidente
Prof.ssa Maria Chiara Carrozza

Maria Chiara Carrozza
13.09.2023 09:59:18 GMT+01:00

……

Per Università degli Studi di Firenze
La Rettrice
Prof.ssa Alessandra Petrucci

UNIVERSITÀ DEGLI STUDI FIRENZE
ALESSANDRA PETRUCCI
25.09.2023 07:44:33 GMT+01:00

……

Per Università degli Studi di Siena
Il Rettore
Prof. Roberto Di Pietra

UNIVERSITÀ DI SIENA 1240
ROBERTO DI PIETRA
24.08.2023 14:38:19 GMT+01:00

……

Per Scuola Normale Superiore
Il Direttore
Prof. Luigi Ambrosio

Firmato digitalmente da: Luigi Ambrosio
Data: 25/08/2023 11:56:03

Per Scuola Superiore di Studi Universitari e di Perfezionamento "Sant'Anna"
La Rettrice
Prof.ssa Sabina Nuti

Firmato digitalmente da: NUTI SABINA
Data: 25/08/2023 10:28:16

*[Le cariche di Direttore del Centro di Competenza in Cybersecurity Toscano C3T e di Rettore della Scuola IMT Alti Studi Lucca sono ricoperte dal Prof. Rocco De Nicola. Pertanto, per entrambe le Parti interessate, la sottoscrizione del Protocollo di Intesa avverrà con apposizione di unica firma digitale].

(Il documento è firmato digitalmente ai sensi del D. Lgs. n. 82/2005 CAD e s.m.i. e norme collegate e sostituisce il documento cartaceo e la firma autografa)

Il presente atto è pubblicato integralmente sulla banca dati degli atti amministrativi della Giunta regionale ai sensi dell'articolo 18 della L.R. 23/2007.