UNIVERSITÀ
DI SIENA
1240

DIVISIONE PERSONALE TECNICO AMMINISTRATIVO
UFFICIO GESTIONE RISORSE UMANE E RELAZIONI SINDACALI

Siena, data della firma digitale

Classificazione: I/10

N. allegati: 3

Al Presidente del Collegio dei Revisori dei Conti
dell'Università di Siena

Ai Membri del Collegio dei Revisori dei Conti
dell'Università di Siena

Oggetto: relazione illustrativa e tecnico-finanziaria relativa all'Ipotesi di Contratto collettivo integrativo dell'Università degli studi di Siena, relativa all'impiego di sistemi digitali per l'incremento dei livelli di sicurezza informatica anche nello svolgimento di lavoro in modalità agile e/o da remoto, redatta ai sensi dell'art. 40, comma 3 sexies del D.lgs. 165/2001 e della circolare MEF - RGS n. 25 del 19.7.2012

Spett.le Collegio dei Revisori dei Conti,

a seguito della firma dell'Ipotesi di Contratto Collettivo Integrativo dell'Università degli Studi di Siena relativa all'impiego di sistemi digitali per l'incremento dei livelli di sicurezza informatica anche nello svolgimento di lavoro in modalità agile e/o da remoto, si sottopone alla cortese attenzione del Collegio la relazione illustrativa e tecnico finanziaria redatta ai sensi dell'art. 40, comma 3 sexies del D.lgs. 165/2001 e s.m.i. e della circolare MEF - RGS n. 25 del 19.7.2012.

ALLEGATO 1: Relazione illustrativa relativa all'Ipotesi di Contratto Collettivo Integrativo dell'Università degli Studi di Siena relativa all'impiego di sistemi digitali per l'incremento dei livelli di sicurezza informatica anche nello svolgimento di lavoro in modalità agile e/o da remoto;

ALLEGATO 2: Ipotesi di Contratto Collettivo Integrativo dell'Università degli Studi di Siena relativa all'impiego di sistemi digitali per l'incremento dei livelli di sicurezza informatica anche nello svolgimento di lavoro in modalità agile e/o da remoto sottoscritta il 10/09/2024.

ALLEGATO 3: nota del Dirigente dell'Area Organizzazione e Sistemi Informativi – AOSI relativa agli aspetti finanziari dell'Ipotesi di CCI.

Confidando che la presente relazione illustri compiutamente l'Ipotesi di Contratto Collettivo Integrativo in oggetto, si richiede il parere obbligatorio di cui all'art. 7, comma 8, del CCNL 19.04.2018 e si resta a disposizione per qualunque ulteriore chiarimento necessario.

Restando in attesa di riscontro, porgo i più cordiali saluti.

La Direttrice generale
Beatrice Sassi

ALLEGATO 1
RELAZIONE ILLUSTRATIVA RELATIVA IPOTESI DI CONTRATTO COLLETTIVO INTEGRATIVO DELL'UNIVERSITÀ DEGLI STUDI DI SIENA RELATIVA ALL'IMPIEGO DI SISTEMI DIGITALI PER L'INCREMENTO DEI LIVELLI DI SICUREZZA INFORMATICA ANCHE NELLO SVOLGIMENTO DI LAVORO IN MODALITÀ AGILE E/O DA REMOTO.

Modulo 1 - Scheda 1.1
Illustrazione degli aspetti procedurali, sintesi del contenuto del contratto e autodichiarazioni relative agli adempimenti della legge

Data di sottoscrizione		10/09/2024
Periodo temporale di vigenza		Il CCI si applica a decorrere dalla data di sottoscrizione definitiva e fino a successivo accordo che disponga in materia
Composizione della delegazione trattante		Parte Pubblica: Prof.ssa Lara Lazzeroni, delegata del Magnifico Rettore alle relazioni sindacali Dott.ssa Beatrice Sassi, Direttrice generale pro-tempore Dirigente dell'AOSI, dott. Pierosario Lomagistro Organizzazioni sindacali ammesse alla contrattazione: RSU FLC CGIL CISL Scuola SNALS CONFSAL GILDA UNAMS Organizzazioni sindacali firmatarie: RSU FLC CGIL CISL Università SNALS CONFSAL Federazione GILDA UNAMS
Soggetti destinatari		Personale tecnico amministrativo dell'Università degli Studi di Siena
Materie trattate dal contratto integrativo (descrizione sintetica)		Impiego di sistemi digitali per l'incremento dei livelli di sicurezza informatica anche nello svolgimento di lavoro in modalità agile e/o da remoto
Rispetto dell'iter, degl	**Intervento dell'Organo di**	

	controllo interno. Allegazione della Certificazione dell'Organo di controllo interno alla Relazione illustrativa.	Non ci sono rilievi.
	Attestazione del rispetto degli obblighi di legge che in caso di inadempimento comportano la sanzione del divieto di erogazione della retribuzione accessoria	Il *Piano integrato di attività e organizzazione (PIAO) 2024-2026* è stato approvato dal C.d.A. nella seduta del 26 gennaio 2024. Nella stessa seduta, è stato approvato il Sistema di misurazione e valutazione della performance (previo parere vincolante espresso dal Nucleo di valutazione in data 19 gennaio 2024). Gli obiettivi e azioni operative - PIAO 2024-2026 e l'Allegato 4 Progetti Top down – PIAO 2024-2026 sono stati approvati dal CdA nella seduta del 23 febbraio 2024. Alcuni obiettivi e azioni operative - PIAO 2024-2026 con la rimodulazione sono stati approvati dal CdA nella seduta del 26 luglio 2024, previo parere favorevole espresso dal Nucleo di valutazione in data 18 luglio 2024. La *Relazione sulla Performance 2023* è stata approvata dal Consiglio di amministrazione del 24 maggio 2024 la Relazione sulla performance 2023 e validata dal Nucleo di valutazione nella seduta del 12 giugno 2024. Quest'ultimo nella medesima seduta ha presentato, come previsto dall'art. 14, comma 4, lettera e) del D. Lgs. 150/2009, la proposta di valutazione del Direttore generale al Consiglio di Amministrazione (CdA), sulla base del Sistema di Misurazione e Valutazione della Performance (SMVP UNISI), di cui al Titolo III dello stesso D. Lgs.. Il CdA nella seduta del 26 luglio 2023 ha approvato la proposta di valutazione del Direttore generale.
Eventuali osservazioni.		

Modulo 2 - Illustrazione dell'articolato del contratto (Attestazione della compatibilità con i vincoli derivanti da norme di legge e di contratto nazionale - altre informazioni utili)

A) *Illustrazione di quanto disposto dal contratto integrativo, in modo da fornire un quadro esaustivo della regolamentazione di ogni ambito/materia e delle norme legislative e contrattuali che legittimano la contrattazione integrativa della specifica materia trattata.*

1. PREMESSA

Agli inizi del mese di maggio 2024, l'Università degli Studi di Siena ha subito un attacco cybercriminale di tipo *ransomware* con conseguente esfiltrazione documentale tramite accessi esterni in VPN.

A seguito dell'evento si è reso necessario predisporre un **programma di interventi** finalizzati ad elevare la postura di sicurezza dell'Ateneo e della sua architettura informatica. Il programma dei primi interventi proposti dall'Area Organizzazione e Sistemi Informativi è stato approvato dagli Organi (Senato Accademico del 16 luglio 2024, rep. n.126/2024, prot. n. 148834 del 18/07/2024, e del Consiglio di Amministrazione del 26/07/2024, rep. 215/2024, prot. n. 158058 del 29/07/2024) ed è allegato sub. All. 1) all'Ipotesi di accordo oggetto della presente relazione.

In particolare, e per quanto rileva ai fini dell'accordo, l'attacco informatico e le operazioni di messa in sicurezza hanno comportato l'interdizione all'uso dei sistemi in accesso da remoto attraverso collegamento VPN (Virtual Private Network)[1].
L'accesso alla VPN ha tuttavia rappresentato, e rappresenta, una delle possibili modalità con le quali rendere la prestazione lavorativa durante il lavoro da remoto e si rende pertanto necessario regolamentarne l'utilizzo in sicurezza.

In generale il programma di interventi per elevare la postura di sicurezza dell'Ateneo prevede diversi livelli di sicurezza a seconda delle risorse a cui si deve accedere.

Al primo livello è previsto l'accesso mediante autenticazione a due fattori. A questo livello sarà possibile accedere alle risorse bibliografiche che l'Ateneo mette a disposizione sulla Rete di Ateneo e al Voip; l'utenza tipica è potenzialmente da individuare nell'intera comunità universitaria che necessita di accedere solo a dette risorse.

Un livello di sicurezza maggiore è previsto per coloro che accedono a risorse più "sensibili", quali ad esempio i Desktop virtuali oppure i pc fisici collocati nei locali dell'amministrazione, oppure ancora i file memorizzati sulle cosiddette "cartelle condivise".

[1] Una VPN è un servizio che crea una connessione sicura e privata su Internet criptando i dati che vengono scambiati e rendendoli inaccessibili a chiunque tenti di spiarli.

Per questi accessi è necessario che sul dispositivo che accede alla Rete sia installato il software **Forticlient ZTNA Edition** che, oltre a richiedere l'autenticazione e due fattori, consente l'accesso alla VPN **solo se** il dispositivo su cui è installato risponde ai requisiti di sicurezza richiesti dall'Ateneo.

2. I CONTENUTI DELL'IPOTESI DI CCI

Nelle premesse all'accordo viene dato conto delle motivazioni e del periodo di sperimentazione a seguito dei quali si è giunti all'individuazione del programma di sicurezza Software FortiClient ZTNA Edition; viene inoltre dato conto del percorso di condivisione con le rappresentanze e sigle sindacali a conclusione del quale si è giunti alla sottoscrizione dell'Ipotesi di Contratto collettivo integrativo.
Nella stesura dell'Accordo, con particolare riferimento ai contenuti tecnici, la Parte pubblica si è avvalsa delle conoscenze e competenze tecniche della Area Organizzazione e Sistemi Informativi, il cui Dirigente ha pertanto sottoscritto l'Accordo sindacale.

Sono previste **due fasce di implementazione del sistema di sicurezza**:

- una di primo livello, presidiata da un sistema di accesso con autenticazione a due fattori e per la quale è sufficiente la presenza di "**FortiClient VPN**" (versione base e a licenza d'uso gratuito, già attualmente in uso). Tale primo livello di sicurezza consente l'accesso, tramite una VPN "limitata", alle sole risorse bibliografiche elettroniche dell'Ateneo. È altresì possibile, mediante lo stesso "FortiClient VPN" rispondere tramite computer, tablet o smartphone alle telefonate degli utenti effettuate verso il numero fisso dell'ufficio.
- una di secondo livello, per consentire l'accesso tramite la VPN al proprio *desktop* virtuale o pc fisico, in cui alla autenticazione a due fattori si aggiunge l'installazione nel pc di uno specifico Agente-Software denominato "**FortiClient ZTNA Edition**". Tale ipotesi consente anche a coloro che accedono da remoto di collegarsi virtualmente al *desktop* dell'ufficio integrato con il client VoIP associato al proprio numero telefonico dell'ufficio. La connessione VPN viene permessa dopo aver verificato che:
    1. l'utente abbia attivato l'autenticazione a due fattori;
    2. il sistema operativo della postazione remota sia correntemente supportato dal produttore (come ad es., ad oggi, con Windows 10 o superiore);
    3. sia presente un software antivirus attivo e aggiornato.

L'Agente-Software "FortiClient ZTNA Edition" per le modalità e le funzioni per le quali viene usato non rientra strettamente nelle previsioni dell'art. 4, comma 1, della l. n. 300/70 e, piuttosto, costituisce uno strumento di lavoro tale per cui trova applicazione la fattispecie di cui al secondo comma dell'art. 4 della l. n. 300/70.

Tuttavia l'Amministrazione ha ritenuto opportuno, per maggiore trasparenza e condivisione con personale, RSU e OO.SS., addivenire ad un accordo che possa anche valere, a tutti gli effetti, ai sensi dell'art. 4 comma 1, l. 300/70[2], in virtù del quale:

[2] L'art. 51 del D. Lgs. n. 165/2001, al comma 2, prevede che "*La legge 20 maggio 1970, n. 300, e successive modifiche e integrazioni, si applica alle pubbliche amministrazioni a prescindere dal numero dei dipendenti*".

"*1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali (…) In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro (…) 2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze*.", le parti addivengono alla presente intesa.

Conseguentemente le Parti Pubblica, rappresentata dalla Delegata del Rettore, prof.ssa Lara Lazzeroni, dalla Direttrice Generale, dott.ssa Beatrice Sassi, dal Dirigente dell'AOSI, dott. Pierosario Lomagistro, e la Parte Sindacale (Rappresentanza Sindacale Unitaria di Ateneo e le seguenti Rappresentanze sindacali: FLC-CGIL, CISL SCUOLA, SNALS CONFALS, Federazione GILDA UNAMS), hanno convenuto di sottoscrivere il giorno 10/09/2024 l'Ipotesi di CCI in materia di impiego, ex art. 4, L. n. 300/1970, di sistemi utili a eseguire la prestazione lavorativa e in grado di garantire una maggiore sicurezza informatica dell'intera Rete di Ateneo consistenti nell'utilizzo del software "FortiClient ZTNA Edition[3]".

3. INSTALLAZIONE DELL'AGENTE SOFTWARE

L'accordo regolamento le modalità di installazione dell'Agente. Trattandosi di un Software necessario a rendere la prestazione lavorativa o comunque necessario, secondo il principio di minimizzazione, a verificare la presenza dei requisiti minimi di sicurezza indispensabili per rendere una prestazione lavorativa in sicurezza e nell'adempimento degli accordi stabiliti nell'ambito degli accordi individuali per il lavoro da remoto, l'installazione di tale Agente-Software dovrà avvenire da parte di coloro la cui prestazione lavorativa si svolga in modalità remota e quindi con uso di pc non collegati direttamente alla Rete di Ateneo, che abbiano necessità di accedere al proprio *desktop* virtuale o pc fisico.

Ciascun lavoratore o lavoratrice interessato/a, quale condizione necessaria allo svolgimento della prestazione da remoto, è dunque tenuto/a a presentare apposita richiesta di abilitazione all'accesso in VPN di secondo livello, controfirmata dal/dalla proprio/a Responsabile, mediante la compilazione di un apposito modulo (All. 2 all'Ipotesi di CCI) contenente la dichiarazione del lavoratore/lavoratrice con cui si impegna a scaricare l'Agente-software di sicurezza informatica indicato nell'accordo sindacale.

In via di prima applicazione:

a. Il personale interessato è invitato, nei 10 giorni di tempo dalla sottoscrizione definitiva dell'accordo sindacale o dall'invito scritto del Responsabile, a presentare richiesta di accreditamento alla VPN di secondo livello;
b. Il personale interessato avrà poi 7 giorni di tempo per scaricare l'Agente-software sullo strumento impiegato per l'esecuzione della prestazione da remoto, decorrente dalla data di invio delle credenziali e/o istruzioni per scaricare l'Agente da parte dei tecnici informatici.

[3] La cui scheda tecnica è allegata all'Ipotesi di CCI.

L'autorizzazione ha valenza annuale e si rinnova automaticamente qualora non ricorrano variazioni organizzative; in tali casi, la cessazione della necessità di accedere da remoto tramite VPN viene comunicata via mail dall'interessato/a alla AOSI previo confronto/consenso con il diretto Responsabile. In caso di cessazione nell'utilizzo della VPN o dal servizio, la comunicazione è necessaria al fine di rendere eventualmente trasferibile la licenza.

La connessione VPN viene permessa al personale interessato solo dopo aver verificato, da parte del sistema Agente stesso (e non più in autonomia dal singolo lavoratore/lavoratrice, e a propria cura) che la postazione di lavoro rispetti tutti i requisiti indicati nella "Misure minime di sicurezza ICT per le pubbliche amministrazioni" emanate dall'AGID (Agenzia per l'Italia Digitale)".

4. RAGIONI E SCOPO RELATIVI ALL'UTILIZZO DELL'AGENTE-SOFTWARE "FORTICLIENT ZTNA EDITION"

Nell'Accordo è specificato che l'Università è autorizzata ad impiegare l'Agente-Software "FortiClient ZTNA Edition" al solo ed esclusivo scopo di verificare che gli apparecchi digitali che accedano alla VPN di secondo livello abbiano:

a) attivato l'autenticazione a due fattori;
b) un sistema operativo della postazione remota correntemente supportato dal produttore;
c) un software antivirus attivo e aggiornato.

5. MODALITÀ DI FUNZIONAMENTO DELL'AGENTE SOFTWARE

L'accordo descrive le modalità di funzionamento dell'Agente e in apposito allegato è presente il Manuale operativo del sistema Agente. Il personale riceverà apposita informativa sulle modalità di installazione.
Qualora vengano apportate modifiche e/o integrazioni che non alterino in modo significativo l'ambito di operatività del sistema Agente-Software "FortiClient ZTNA Edition", in relazione alle tutele contenute nell'Accordo, l'Amministrazione potrà limitarsi a fornire la relativa informativa preventiva a RSU e OO.SS.
È in ogni caso previsto che sarà oggetto di verifica congiunta delle Parti lo stato di attuazione dell'Accordo nonché la condivisione, al bisogno, di eventuali specifiche problematiche legate alla sicurezza.
L'Università degli Studi di Siena assicura, anche con la sottoscrizione dell'Accordo, che non vi sarà alcun controllo sulle attività svolte da remoto da parte dei lavoratori e delle lavoratrici e sul contenuto delle apparecchiature utilizzate per l'esecuzione della prestazione lavorativa.

6. PERIODO DI CONSERVAZIONE DI DATI E DELLE INFORMAZIONI ACQUISITI DAL SOFTWARE "FORTICLIENT ZTNA EDITION"

I dati e le informazioni (tra cui quelli ad esempio relativi ai LOG di accesso alla VPN), saranno detenuti dall'Amministrazione per un massimo di giorni 15, periodo ritenuto una misura minima necessaria ed indispensabile per tenere traccia di eventuali anomalie che potrebbero compromettere la sicurezza della Rete e dell'Ateneo, nel rispetto di quanto indicato anche dall'autorità Garante per la Privacy. In ogni caso, ai sensi dell'art. 5 del GDPR, ", i dati personali trattati sono *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*".

7. TUTELE RELATIVE ALL'UTILIZZO DELL'AGENTE E AL TRATTAMENTO DEI DATI

L'accordo esplicita le finalità di utilizzo dell'Agente-Software "FortiClient ZTNA Edition" nel rispetto dei principi di cui all'art. 5, Reg. UE 2016/679.
Tutti i dati raccolti saranno trattati soltanto dall'Università degli Studi di Siena, mentre il fornitore dell'Agente-Software non vi avrà alcun accesso e comunque non li tratterà in nessun modo.
Il trattamento dei dati personali relativo all'utilizzo dell'Agente-Software "FortiClient ZTNA Edition", avverrà in conformità alle disposizioni dell'art. 4 e alle altre disposizioni della l. 300/1970 (stat. lav.), del Reg. UE 2016/679 (GDPR), del Codice in materia di protezione dei dati personali di cui al D. Lgs n. 196/2003 e ss. mod. e int., nonché degli inerenti provvedimenti ed atti interpretativi e di indirizzo e della legislazione in materia applicabile e del Regolamento sul trattamento dei dati personali di Ateneo.
Le modalità di trattamento saranno oggetto di specifica informativa agli interessati (da fornire prima dell'inizio del trattamento).

8. ASPETTI INERENTI ALLA QUANTIFICAZIONE DEI COSTI E ALLA RELATIVA COPERTURA FINANZIARIA

Relativamente agli aspetti inerenti alla quantificazione dei costi relativi all'installazione dell'Agente e alla correlata copertura finanziaria, si rinvia alla specifica relazione del Dirigente dell'Area Organizzazione e Sistemi Informativi, dott. Pierosario Lomagistro (Prot. n. 177290 del 09/09/2024).
L'acquisto di licenze dell'Agente-Software avviene a spese dell'Amministrazione, per tutte le macchine di proprietà dell'Amministrazione impiegate per l'accesso alla VPN di secondo livello non direttamente collegate alla Rete di Ateneo e comunque per quelle apparecchiature informatiche che i lavoratori e le lavoratrici utilizzeranno per la prestazione da remoto, quand'anche di loro proprietà.

Nel rimanere a disposizione per eventuali necessità di chiarimenti o di ulteriori informazioni, si inviano cordiali saluti.

La Direttrice generale
Beatrice Sassi

La Responsabile della Divisione personale tecnico amministrativo
Laura Goracci