UNIVERSITA' DEGLI STUDI DI GENOVA

AREA ICT

IL DIRIGENTE

VISTE le indicazioni di carattere strategico indicate nel Piano Integrato di Attività e Organizzazione PIAO 2024 – 2026 in materia di servizi informatici

VISTO l'obiettivo individuale assegnato al Dirigente dell'Area ICT per il 2024 che assegna la redazione di cinque Linee Guida i cui argomenti sono indicati al seguente Art.1.

DETERMINA

Art. 1

Per le attività di coordinamento e di gestione delle attività informatiche in Ateneo, con particolare riferimento alla integrazione delle azioni da attuare per il contrasto agli attacchi informatici, l'emanazione di cinque Linee Guida aventi per oggetto i seguenti argomenti:

1) Sicurezza informatica
2) Tecnologie da adottare
3) Utilizzo delle reti
4) Utilizzo dei client
5) Utilizzo degli apparati per la Didattica Digitale Integrati

Art.2

Le indicazioni della presente Determina Dirigenziale sono da considerarsi efficaci ed esecutive dal 1° novembre 2024.

Art. 3

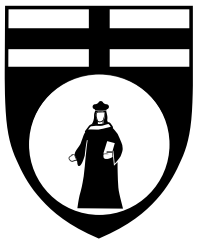
Le suddette Linee Guida saranno pubblicate sul sito di Ateneo alle pagine web dell'Area ICT, comunicate al Consiglio di amministrazione nella prima seduta utile e diffuse a tutto il personale dell'Università di Genova.

Il Dirigente dell'Area ICT

Ing. Massimo Di Spigno

Università degli Studi di Genova | P. IVA 00754150100
Area ICT

Viale Cembrano, 4, 16148 Genova
area.ICT@unige.it | PEC csita@pec.unige.it



Università
di Genova

Linea Guida ICT

Sicurezza informatica

Versione	Autori
Ottobre 2024	Stefano Orocchi (Area ICT) Massimo Di Spigno (Area ICT)

Sommario

Introduzione

L'Università degli Studi di Genova, a cui ci si riferisce in seguito come Unige, o Ateneo, nell'espletamento della sua attività istituzionale opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

Il presente documento definisce le regole e le condizioni per l'utilizzo degli strumenti informatici dell'Ateneo da parte dei dipendenti, degli studenti e di tutti coloro che, in virtù di un rapporto di lavoro, di studio, o di ricerca, a qualsiasi titolo (collaboratori, consulenti, stagisti, fornitori, studenti esterni, etc.), utilizzano strumenti informatici dell'Ateneo, nel seguito denominati Utenti.

Il presente documento deve considerarsi integrato da tutte le procedure interne adottate per argomenti specifici e casistiche, così come pubblicati sul sito dell'Ateneo e più specificatamente dell'Area ICT.

Finalità del documento

Il presente documento definisce e detta agli Utenti specifiche regole e condizioni di utilizzo degli strumenti informatici aziendali attraverso:

- definizione di regole e procedure uniformi da applicarsi in tutte le aree operative e Strutture organizzative;
- definizione di regole e procedure attinenti a specifici ambiti di applicazione;
- indicazione del corretto approccio da seguire in assenza di regole specifiche per una determinata specifica casistica;
- indicazione delle principali disposizioni normative in materia di utilizzo dei sistemi informativi e di protezione dei dati personali;
- definizione dell'ambito, delle modalità, dei limiti del monitoraggio e dei controlli attuabili dall'Ateneo nel rispetto della normativa vigente nonché delle regole e delle procedure interne.

Contesto normativo e regolamentare

Il presente regolamento è redatto sulla base dei seguenti e principali riferimenti normativi:

- Codice penale, con particolare riferimento ai reati informatici;
- L. 300/1970 (Statuto dei lavoratori) - artt. 4, 7 e 8 e successive modificazioni;
- D. Lgs. 196/2003 e s.m.i(Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per posta elettronica e Internet" di cui alla deliberazione 13/2007;
- D. Lgs. 81/2008 e s.m.i (Testo Unico sulla sicurezza);
- D.P.R 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione) e Codice di comportamento Unige;

- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR)
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1417809
- REGOLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
- DECRETO LEGISLATIVO 4 settembre 2024, n. 134 (recepimento NIS 2) - Attuazione della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio. (24G00150) (GU Serie Generale n.223 del 23-09-2024)
- Piano Implementativo Strategia Nazionale Cybersicurezza 2022-2026
- Piano Triennale per l'informatica nella PA

GLOSSARIO E DEFINIZIONI

Ai fini del presente documento si intende per:

- Amministratori di sistema: figure professionali finalizzate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009;
- Applicazioni aziendali: si considerano applicazioni aziendali:
    - Prodotti/programmi acquistati dall'Ateneo, di valenza generale, o settoriale ed in quest'ultimo caso approvati dall'Area ICT;
    - Applicazioni e servizi sviluppati ad hoc dell'Area ICT, da terze parti ma sotto il coordinamento dell'Area ICT, ovvero da altre strutture con un processo di partecipazione e approvazione da parte dell'Area ICT e che seguono le regole di gestione previste nei casi precedenti;
    - Applicazioni esterne che l'Ateneo utilizza secondo le regole di gestione e di sicurezza delle medesime a titolo di mero esempio possono essere la piattaforma NoiPA, abbonamenti a servizi informativi, portale ANAC, etc.
- Aziendali: nel corso del documento si farà spesso riferimento a risorse o dispositivi come "aziendali". Pur nella consapevolezza che l'Ateneo non è un'azienda, tale dicitura identifica più chiaramente l'organizzazione nella letteratura tecnica.
- Dispositivi o endpoint: qualunque dispositivo atto a connettersi alla rete Unige, ai suoi dati, alle applicazioni aziendali, alle risorse in genere.
- Dispositivi aziendali: dispositivi di proprietà o comunque nelle disponibilità dell'Università degli studi di Genova e messi nelle disponibilità degli utenti.
- File di log: registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato;
- GENUAnet: rete informatica gestita direttamente dall'Università di Genova divisa in rete cablata e rete WiFi eduRoam (già GenuaWiFi);
- Strumenti informatici: personal computer fissi o portatili o virtuali, stampanti locali o di rete, programmi e prodotti software in-house o in-cloud, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc);
- Utenti: personale dipendente, docenti, studenti, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni e coloro che, in virtù di un rapporto di lavoro, di studio o di collaborazione in essere a qualsiasi titolo con l'Ateneo, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione da Unige.

PRINCIPI GENERALI

Gli strumenti informatici sono assegnati agli Utenti per lo svolgimento dell'attività e devono essere utilizzati con modalità e mediante comportamenti adeguati al ruolo, ai compiti assegnati e alle responsabilità connesse, nel rispetto del Codice di comportamento dei dipendenti della pubblica amministrazione e delle normative e direttive interne e delle leggi.

Nell'esecuzione della propria attività, gli Utenti sono tenuti ad attenersi alle seguenti istruzioni generali:

a. effettuare la propria attività uniformandosi alle disposizioni dell'Ateneo e alle istruzioni ricevute;
b. custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente alle strutture preposte, secondo le modalità previste, ogni danneggiamento, smarrimento o furto;
c. mantenere la riservatezza sulle informazioni e sui dati personali di cui siano venuti a conoscenza durante lo svolgimento della propria attività;
d. in caso di cessazione dal servizio, dalla prestazione o dal rapporto con l'Ateneo, astenersi dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività, in funzione della natura di riservatezza del dato;
e. adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati;
f. garantire la corretta custodia di atti e documenti adottati da Unige.

REGOLE PER L'UTILIZZO DEI SISTEMI INFORMATICI DI ATENEO

Credenziali di autenticazione

L'accesso alle applicazioni del sistema informativo di Ateneo avviene attraverso credenziali di autenticazione centralizzate fornite e gestite dall'Area ICT (es. credenziali Unigepass, credenziali Cloud), o tramite sistemi di autenticazione esterni autorizzati dall'Area ICT (es. SPID). L'accesso a particolari dispositivi, servizi o applicazioni può avvenire tramite credenziali locali in accordo l'Area ICT (es. particolari allestimenti di laboratorio).

Le credenziali di autenticazione, da gestire nel rispetto delle regole stabilite, sono strettamente personali e non devono essere comunicate né rese disponibili ad altri soggetti.

In caso di diffusione accidentale, anche solo presunta, le password devono essere immediatamente modificate e l'incidente va immediatamente segnalato.

Il sistema di controllo degli accessi implementa regole che seguono l'evoluzione della tecnologica e delle necessità di sicurezza.

I dettagli dei requisiti richiesti per l'utilizzo dell'autenticazione sono disponibili sulle pagine del web di ateneo e più specificatamente nelle pagine dell'Area ICT.

Utilizzo di applicazioni aziendali

L'accesso alle applicazioni aziendali e il loro utilizzo devono avvenire secondo le regole del presente documento e sulla base del ruolo ricoperto dall'utente e le relative responsabilità e regole ad esse conseguenti.

L'accesso alle applicazioni aziendali deve essere finalizzato allo svolgimento del proprio ruolo in Ateneo e non presentare conflitto con esso.

Il ruolo di un Utente in Ateneo e le attività ad esso legate determinano le autorizzazioni all'accesso alle risorse aziendali. Tali autorizzazioni vengono assegnate dai sistemi informativi con l'applicazione di automatismi e richiedono quindi la costante disponibilità di dati quanto più possibile esatti nei sistemi informativi dell'Ateneo.

L'accesso alle applicazioni aziendali può avvenire tramite:

- dispositivi aziendali, allestiti da, per conto, con l'assenso dell'Area ICT.
- dispositivi di proprietà o nelle disponibilità dell'utente, caso definito anche di Bring Your Own Device (BYOD)

In ogni caso, l'accesso alle applicazioni e alle risorse aziendali segue le stesse regole e raccomandazioni per quanto concerne la sicurezza e le modalità di accesso e utilizzo, così come descritto nel presente documento.

L'Area ICT sovrintende alle corrette modalità di accesso e utilizzo delle applicazioni e risorse aziendali anche in modo delegato, provvede a dare informazione all'Ateneo dei corretti modi di utilizzo delle risorse informative aziendali, a formare gli Utenti e il personale eventualmente delegato in Ateneo.

L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni.

L'accesso alle applicazioni aziendali è legato al ruolo dell'utente in Ateneo. Al modificarsi, o al termine del ruolo dell'utente in Ateneo, la disponibilità di accesso alle risorse aziendali può cessare o andarsi a modificare, solitamente in modo automatico. L'utente è tenuto a mantenersi informato dei corretti criteri di accesso ai programmi e delle risorse di cui ha disponibilità.

Utilizzo di dispositivi aziendali

I dispositivi aziendali vengono preparati e gestiti da, per conto, con l'assenso dell'Area ICT secondo regole che evolvono con il progredire delle tecnologie e delle minacce informatiche. Ne è vietato qualunque utilizzo che danneggi le risorse aziendali (es. il dispositivo stesso, o il software, o i dati), o che sia di minaccia per la sicurezza. È consentito l'uso promiscuo, sia lavorativo, sia personale, del dispositivo, purché non contraddica alcuna altra regola del presente documento, o dell'Ateneo.

Il dispositivo è provvisto di software di sicurezza (es. antivirus, firewall, impostazioni di aggiornamento) e le configurazioni disposte o raccomandate seguono regole come descritte nel presente documento e altre linee guida opportunamente fornite dall'Area ICT.

Nei casi in cui l'Utente, o comunque altro personale opportunamente delegato, dispongano di diritti amministrativi sul dispositivo, dovranno assicurarsi in prima persona della corretta configurazione e mantenimento del dispositivo ed evitare comportamenti diversi dalle raccomandazioni.

Nei casi in cui l'utente, o comunque altro personale opportunamente delegato, abbiano autonomia di installazione/utilizzo di applicazioni, anche senza diritti amministrativi, dovranno assicurarsi in prima persona della corretta configurazione e mantenimento di esse ed evitare comportamenti diversi dalle raccomandazioni.

In caso di dubbio sul comportamento da seguire (es. l'installazione di un programma non aziendale), l'utente, o comunque altro personale opportunamente delegato, dovranno consultare il personale dell'Area ICT prima di procedere.

L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni, il ritiro del dispositivo affidato, o anche procedure legali ove necessario.

Tra i dispositivi aziendali rientrano anche i dispositivi e le risorse virtuali. Le regole di cui al presente documento valgono anche per essi per quanto applicabile.

L'accesso ai dispositivi aziendali è legato al ruolo dell'utente in Ateneo. Al modificarsi, o al termine del ruolo dell'utente in Ateneo, la disponibilità dei dispositivi aziendali può cessare o andarsi a modificare. L'utente è tenuto a informarsi dei corretti criteri di detenzione e restituzione dei dispositivi in affidamento.

Utilizzo di dispositivi non aziendali

L'accesso alle risorse aziendali può avvenire tramite dispositivi diversi da quelli aziendali, ad esempio di proprietà o nelle disponibilità dell'utente, oppure di accesso pubblico. Le norme comportamentali per l'utente restano invariate. L'utente si fa responsabile in prima persona nell'accesso alle risorse aziendali di utilizzare dispositivi sicuri, a norma di legge, secondo il regolamento di Ateneo (es. software installato aggiornato, presenza di antivirus e firewall correttamente funzionanti, nessuna minaccia locale rilevata).

L'accesso a risorse aziendali su dispositivi personali prevede un analogo trattamento in termini di assistenza all'utilizzo, ma che non si estende al dispositivo stesso, a cura invece dell'utente.

L'accesso alle applicazioni aziendali è legato al ruolo dell'utente in Ateneo. Al modificarsi, o al termine del ruolo dell'utente in Ateneo, la disponibilità di accesso alle risorse aziendali può cessare o andarsi a modificare, solitamente in modo automatico. L'utente è tenuto a mantenersi informato dei corretti criteri di accesso ai programmi e delle risorse di cui ha disponibilità e delle ripercussioni sul proprio dispositivo del venire a mancare delle risorse aziendali.

Configurazioni speciali dei dispositivi

In casi eccezionali può verificarsi la necessità di tenere in esercizio dispositivi che potrebbero violare alcune norme del presente o altri regolamenti. Un esempio può essere dato dal caso di particolari insostituibili attrezzature per l'acquisizione per i quali sussistano problemi tecnici di incompatibilità con i moderni computer. Questi casi devono essere discussi preventivamente con l'Area ICT, così di concordare un modello di allestimento che non pregiudichi la sicurezza delle risorse aziendali. Il parere dell'Area ICT in materia è vincolante.

Accesso alla rete

L'accesso alla rete internet è messo a disposizione degli utenti per le finalità di lavoro, ricerca, didattica, utili per lo svolgimento del proprio ruolo in Ateneo.

Qualsiasi operazione effettuata sulla rete interna o esterna all'ateneo (accesso a siti web per necessità inerenti e non l'attività lavorativa, salvataggio di file, partecipazione a forum, etc.) è

sotto la responsabilità dell'utente che deve mantenere un comportamento lecito e tale da non compromettere le attività e il buon nome dell'Ateneo.

Ogni Utente è tenuto a osservare le seguenti regole comportamentali:

- utilizzare la rete per fini leciti, astenendosi da qualsiasi comportamento che possa avere natura oltraggiosa e/o discriminatoria verso terzi;
- trasferire sul proprio computer (download) solo file da siti web verificati e affidabili, tenendo presente che, quando si trasferisce materiale da internet occorre prestare la massima attenzione al fine di non incorrere in violazioni di diritti di proprietà intellettuale;
- non utilizzare social network, forum, chat e simili per scambiare informazioni riservate o lesive dell'immagine dell'Ateneo e dei colleghi;
- la navigazione in rete avviene in modalità trasparente e non anonima, soprattutto se attraverso intranet o strumenti aziendali; in ogni caso è vietato accedere a siti i cui contenuti non siano adeguati all'immagine e al buon nome dell'Ateneo.

Al fine di prevenire l'accesso a siti e risorse potenzialmente nocivi, l'Area ICT adotta soluzioni di sicurezza che possono monitorare e bloccare l'accesso a risorse potenzialmente pericolose o dai contenuti illeciti. Sono adottate tecnologie anti-malware che permettono la scansione della navigazione, prevenendo lo scaricamento del contenuto malevolo.

Gi strumenti predisposti dall'Area ICT, richiedono parimenti un corretto e responsabile comportamento da parte dell'utente.

Posta elettronica

Gli utenti sono dotati di un indirizzo di posta elettronica sui sistemi di Ateneo. I sistemi di posta di Ateneo si compongono di risorse informatiche hardware e software gestite direttamente dall'Area ICT (insieme dei Server on-premise e cloud Exchange Online) a cui ci si riferirà come "posta di ateneo", o "posta Unige". L'Area ICT gestisce e supervisiona il sistema di posta garantendo il corretto flusso documentale e monitorando l'utilizzo corretto da parte degli utenti, nonché la sicurezza del sistema nel suo insieme.

In aggiunta a questi sistemi, sono presenti in ateneo sistemi di posta gestiti autonomamente da strutture/dipartimenti con l'accordo e il monitoraggio dell'Area ICT, per motivazioni funzionali e subordinatamente alla regolamentazione e supervisione dell'Area ICT.

Le modalità di attribuzione e gestione delle caselle di posta di ateneo sono regolamentate dalla policy sulla posta elettronica emanata dall'Area ICT.

Ad ogni utente viene assegnato un indirizzo di posta elettronica sulla posta di ateneo che costituisce il suo indirizzo e-mail principale di lavoro e che viene pubblicato nelle rubriche di Ateneo. Ad esso possono essere affiancati alias ritenuti funzionalmente opportuni. Tale indirizzo corrisponde solitamente anche all'UPN, login sul sistema di autenticazione di Ateneo e quindi su una molteplicità di applicazioni aziendali.

Gli indirizzi di posta, le caselle di archiviazione, quando associate, e tutti gli aspetti inerenti al sistema di posta vengono gestiti dall'Area ICT nell'osservanza della policy relativa e sulla base delle necessità di sicurezza e tecniche.

Il sistema di posta di Ateneo deve essere utilizzato esclusivamente per l'esercizio della propria attività all'interno dell'Ateneo, in funzione del proprio ruolo. È da evitarne l'utilizzo per fini personali (es. domiciliazione bollette private).

I sistemi di posta esterni alla gestione dell'Area ICT non devono essere utilizzati per lo svolgimento di attività di Unige, salvo esplicita, motivata e circostanziata autorizzazione da parte dell'Area ICT.

Sono previste caselle di posta condivise per agevolare la condivisione del lavoro di gruppo. L'assegnazione e la gestione di queste caselle segue la policy sulla posta elettronica emanata dall'Area ICT.

Nell'utilizzo della posta elettronica è necessario osservare comportamenti consoni. In particolare, si ricorda l'obbligo di:

- proteggere la privacy dell'interlocutore evitando, qualora non necessario, di inoltrare messaggi altrui senza il previo consenso dell'interessato;
- evitare l'invio, tramite le caselle di posta elettronica, di messaggi ingiuriosi, minatori, lesivi dell'immagine dell'Ateneo o che utilizzino linguaggi o immagini oscene, ingannevoli o diffamatorie;
- Prestare la massima attenzione per evitare di cadere vittima di fishing o di altri attacchi informatici, soprattutto quando di natura nota e riconoscibile;
- evitare l'invio o l'inoltro di messaggi estranei al contesto lavorativo a un gran numero di indirizzi o a liste di distribuzione interne all'Ateneo, salvo motivata e lecita necessità;
- evitare l'utilizzo dell'indirizzo e-mail per l'iscrizione e/o la partecipazione a social network, mailing list, servizi di instant messaging, forum o altri servizi pubblici su internet di interesse personale e non lavorativo;
- evitare di diffondere, all'esterno dell'Ateneo, indirizzi di posta elettronica di altri utenti, per motivi non legati all'attività lavorativa.

Valgono per la posta elettronica tutti gli obblighi e le raccomandazioni inerenti al trattamento dei documenti e dei dati in genere.

Servizi di comunicazione (chat, messaggistica, videoconferenza, telefonia)

Gli strumenti di comunicazione, oltre alla posta elettronica, comprendono la chat, la telefonia, la videoconferenza e la collaborazione sui documenti. Ciascuno di questi strumenti, di natura diversa tra loro, viene gestito in maniera armonizzata dall'Area ICT, o sotto la sua supervisione.

Gli strumenti messi a disposizione dall'Ateneo e amministrati dall'Area ICT consentono lo svolgimento delle attività in Unige in osservanza delle leggi e dei regolamenti vigenti. Gli strumenti informatici in uso sono rispondenti ai requisiti stringenti in merito al trattamento dell'informazione e anche la loro amministrazione interna all'Ateneo, di cui è responsabile

l'Area ICT, permette di garantire la riservatezza dei documenti e l'osservanza dei dettami di legge tramite un lavoro di continuo monitoraggio e adeguamento. Viene scoraggiato l'utilizzo di sistemi di comunicazione diversi da quelli gestiti o raccomandati dall'Area ICT.

Durante l'utilizzo di tali strumenti è opportuno adottare comportamenti consoni, come da relativi regolamenti e rispettare le indicazioni fornite dall'Area ICT in materia di adozione degli strumenti e loro modalità di utilizzo.

Si raccomanda di utilizzare in maniera congrua lo strumento di segnalazione del proprio stato di occupazione (libero, in riunione, non disturbare, etc,) in quelle applicazioni che lo permettono (es. Teams, Outlook). Si raccomanda di osservare lo stato di disponibilità di un altro utente prima di tentare di chiamarlo, se disponibile, così da non interrompere altre attività in corso, o abusare del tempo della controparte quando fuori servizio.

Nel rispetto della normativa in materia di tutela della libertà e dignità dei lavoratori e della normativa unionale e nazionale in materia di protezione dei dati personali, sono attivi sistemi di monitoraggio delle comunicazioni che consentono di verificare mittente, destinatario, durata/data e stato. Detti sistemi sono destinati esclusivamente all'analisi del tipo di traffico ai fini di reportistica e manutenzione e le relative informazioni (dati aggregati) sono accessibili ai soli amministratori dei sistemi di comunicazione.

Nell'utilizzo sistemi di comunicazione è necessario osservare comportamenti consoni. In particolare, si ricorda l'obbligo di:

- proteggere la privacy dell'interlocutore evitando, qualora non necessario, di inoltrare messaggi altrui senza il previo consenso dell'interessato;
- assicurarsi che sia evidente a tutti i partecipanti a una comunicazione l'inizio e il termine di una registrazione;
- evitare di diffondere il contenuto di una comunicazione in maniera non concordata con gli altri interlocutori, soprattutto se in presenza di contenuti riservati o sensibili;
- evitare l'utilizzo di linguaggi ingiuriosi, minatori, lesivi dell'immagine dell'Ateneo o che utilizzino linguaggi o immagini oscene, ingannevoli o diffamatorie;
- evitare l'invio o l'inoltro di messaggi estranei al contesto lavorativo a un gran numero di persone interne o esterne all'Ateneo, salvo motivata e lecita necessità;
- evitare di diffondere, all'esterno dell'Ateneo, indirizzi di posta elettronica di altri utenti, per motivi non legati all'attività lavorativa.

Archiviazione, condivisione e servizi Cloud

L'archiviazione aziendale dell'ateneo si compone dell'insieme delle capacità di archiviazione *on-premise* e sul cloud che vanno a comporre complessivamente il sistema di archiviazione di Unige.

Rispetto alla capacità di archiviazione dei dispositivi, l'archiviazione aziendale permette una maggiore sicurezza del dato, resilienza ai guasti e possibilità di monitoraggio da parte degli amministratori di sistema. La legge obbliga l'Ateneo nel suo insieme e ogni suo utente singolarmente a custodire con cura l'informazione di cui è responsabile. Gli strumenti messi a

disposizione dall'Ateneo per la gestione documentale personale e di gruppo agevolano questo compito e sono stati individuati come adeguati a tale scopo dall'Area ICT.

I sistemi di archiviazione di Ateneo si compongono di risorse informatiche hardware e software gestite direttamente dall'Area ICT o sotto suo mandato (insieme dei file server on-premise e cloud Sharepoint Online, OneDrive, Titulus, etc.) a cui ci si riferirà come "archiviazione di ateneo".

Il sistema di archiviazione di Ateneo deve essere utilizzato esclusivamente per l'esercizio della propria attività all'interno dell'Ateneo, in funzione del proprio ruolo. È da evitarne l'utilizzo per fini personali (es. documenti personali, foto, filmati).

I sistemi documentali esterni alla gestione dell'Area ICT non devono essere utilizzati per lo svolgimento di attività di Unige, salvo esplicita, motivata e circostanziata autorizzazione da parte dell'Area ICT.

L'archiviazione di Ateneo viene gestita e monitorata dall'Area ICT che si fa carico di indicare agli utenti i modi più consoni al suo utilizzo, nell'interesse dell'Ateneo, dei lavoratori, degli utenti in generale. A tal proposito, si sottolinea la raccomandazione di tenere sincronizzati/depositati/copiati i dati di lavoro su sistemi come OneDrive, Sharepoint, Teams o Titulus, o altri raccomandati dall'Area ICT per preservarli dalla perdita in seguito a guasti ai dispositivi personali.

In caso di comprovata necessità, gli amministratori dei sistemi si faranno carico di accedere ai sistemi di archiviazione per intervenire come necessario (es. rimozione minacce informatiche, litigation hold, etc.). L'attività degli amministratori viene svolta sempre nel rispetto della normativa in materia di tutela della libertà e dignità dei lavoratori e della normativa unionale e nazionale in materia di protezione dei dati personali.

Dispositivi di memorizzazione removibili e archiviazione locale

L'utilizzo di dispositivi removibili, utili per esempio per effettuare copie di sicurezza o per il trasporto di file di grandi dimensioni, rimane sotto la responsabilità dell'utilizzatore e va considerato sulla base dell'utilizzo previsto, della natura dei dati che deve contenere e della sicurezza con cui questo possa avvenire (utilizzo di crittografia ad es.).

In modo analogo, l'utilizzo dispositivi di archiviazione e condivisione locali come nas o piccoli server di zona, va considerato sulla base delle necessità e deve avvenire solo dopo la valutazione congiunta e il consenso dell'Area ICT.

Salvo casi particolari, questi sistemi di archiviazione non sono da considerarsi sostitutivi del sistema di archiviazione di Ateneo, ma possono essere utili come integrazione.

La conservazione di questi dispositivi implica la responsabilità diretta dell'utente che deve peraltro evitare e segnalare tempestivamente qualunque possibile smarrimento e compromissione.

Archiviazione su cloud esterni

I sistemi documentali esterni alla gestione dell'Area ICT non devono essere utilizzati per lo svolgimento di attività di Unige, salvo esplicita, motivata e circostanziata autorizzazione da parte dell'Area ICT.

L'utilizzo di cloud diversi da quelli interni al sistema di archiviazione di Ateneo mette a repentaglio la qualità della custodia dei dati, in quanto non esistono un'analisi preventiva e un modello di gestione integrato con il sistema di Ateneo.

Comportamenti non consentiti

Sono vietati a tutti gli utenti i seguenti comportamenti:

- l'utilizzo abusivo di credenziali altrui, la cessione a terzi delle credenziali di utilizzo della smart card di firma digitale (o strumento equivalente), l'accesso non autorizzato a risorse informatiche di Unige e/o lo scambio di comunicazioni mediante falsa identità;
- l'installazione, sui dispositivi aziendali in dotazione, di software non coperto da licenza o, comunque, non autorizzato dall'Area ICT, o contrario ai regolamenti e alle leggi;
- l'abuso per motivi personali delle risorse informatiche dell'Ateneo;
- l'utilizzo, la distruzione, l'alterazione o la disabilitazione non autorizzata o contraria ai regolamenti di file e di ogni altra risorsa informatica;
- l'allontanamento dai dispositivi senza il loro blocco o l'adozione delle opportune misure di sicurezza;
- la modifica delle configurazioni delle risorse informatiche di Ateneo senza l'autorizzazione dell'Area ICT;
- l'utilizzo di strumenti volti a eludere i sistemi di protezione.

Protezione contro furti e danneggiamenti

Tutti i dispositivi aziendali, soprattutto se mobili, devono essere custoditi in luogo sicuro, adottando le opportune precauzioni contro il furto delle strumentazioni informatiche e/o dei dati in essi contenuti. L'Utente è tenuto a informare immediatamente il dirigente responsabile, l'Area ICT e, qualora vi sia la possibilità di una violazione di dati personali, altresì il DPO di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso, fermi restando gli obblighi di denuncia alle autorità competenti.

Comportamento in caso di assenza programmata

Il personale dell'Area ICT, salvo per previste motivazioni di sicurezza, tecniche, o legali, non accede ai dati e ai profili dell'utente assente senza il suo consenso, né autorizza terzi all'accesso.

Pertanto, in caso di assenza programmata, al fine di garantire la continuità di servizio, all'utente è richiesto di rendere disponibili i documenti su cui sta lavorando all'ufficio di riferimento, tramite l'utilizzo delle risorse di archiviazione condivisa di Ateneo. Potrà essere utile attivare i meccanismi di risposta automatica, disponibili nelle applicazioni e dispositivi aziendali (risposte automatiche di Outlook e Teams, segreterie telefoniche) per permettere il corretto instradamento dell'attività ai colleghi.

AMBITI DI RICERCA E DIDATTICA

Le attività di ricerca e di didattica si svolgono all'interno dei regolamenti di Ateneo e delle leggi in vigore. Valgono in generale tutte regole e le raccomandazioni contenute nel presente documento e nell'insieme delle regole di Ateneo.

Le attività di ricerca e didattica si svolgono per loro natura con un elevato grado di autonomia degli utenti coinvolti e possono richiedere una maggiore varietà di configurazioni di dispositivi e di applicativi rispetto a quelli normalmente disponibili per le attività di ufficio. L'utilizzo di configurazioni, applicazioni, modalità di utilizzo diverse da quelle già considerate consone per l'attività in Ateneo richiede una consultazione preventiva del personale dell'Area ICT, secondo i normali canali di assistenza, per l'individuazione della maniera più consona di soddisfacimento della necessità (Es. una ricerca sui virus informatici potrebbe richiedere il corretto isolamento dell'ambiente di test e l'esclusione dell'accesso alla rete di produzione).

L'accesso a dati del sistema informativo di Unige, soprattutto se contenenti dati personali, l'utilizzo di applicazioni con uscita o condivisione di dati dal sistema informativo di Unige, l'iscrizione degli Utenti Unige a servizi non gestiti internamente, sono tutti esempi di attività che necessitano di consultazione preventiva dell'Area ICT.

L'Area ICT si fa carico di esaminare le necessità e cercare soluzioni che preservino in primo luogo la sicurezza dell'utente e la funzionalità dell'infrastruttura informatica di Ateneo. I casi più comuni possono essere coperti dall'osservanza di semplici indicazioni sul sito di Ateneo e più specificatamente dell'Area ICT.

La consultazione, se invece necessaria, deve avere luogo nella fase precedente alla presa di accordi con terzi o di indagine economica. Il parere dell'Area ICT in merito è vincolante. L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni, o anche procedure legali ove necessario.

CONTROLLO E MONITORAGGIO

L'Area ICT imposta la propria azione di monitoraggio e controllo sui sistemi informatici di Ateneo messi a disposizione per lo svolgimento delle attività nel rispetto della normativa vigente e sul presupposto di un utilizzo responsabile degli stessi da parte degli Utenti, adottando in ogni caso le soluzioni tecnologiche idonee a garantire i profili di sicurezza dei sistemi informativi e dei dati gestiti.

A tal fine, l'Area ICT utilizza sistemi automatizzati per il monitoraggio centralizzato che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la funzionalità e la sicurezza degli apparati informatici di Ateneo e delle informazioni ivi contenute.

I file di log relativi all'utilizzo della infrastruttura informatica sono registrati e conservati per le suddette finalità di funzionalità e sicurezza, in conformità alla normativa vigente e alle disposizioni adottate al riguardo dall'Area ICT. Nel caso di eventi anomali e/o pregiudizievoli per la sicurezza informatica, i file di log file e i dati di monitoraggio relativi possono essere esaminati dagli amministratori di sistema per l'individuazione del problema tecnico e l'adozione delle necessarie misure conseguenziali. In ogni caso, tutti i controlli di funzionalità e monitoraggio avvengono nel rispetto di quanto previsto dal CAD, dalle norme in materia di tutela della libertà e dignità dei lavoratori, della normativa unionale e nazionale in materia di protezione dei dati personali.

Gli amministratori di sistema, nel caso in cui rilevino anomalie o configurazioni non corrette dei dispositivi, possono provvedere a isolare immediatamente l'origine dell'anomalia o del malfunzionamento anche senza preavvisare l'Utente, per salvaguardare la sicurezza e l'integrità dei sistemi informativi di Unige. In tal caso, verrà data successiva informativa all'Utente sui motivi dell'avvenuto intervento da parte degli amministratori di sistema. Le predette attività sono svolte nel rispetto dei principi di gradualità, pertinenza e non eccedenza stabiliti dal Garante per la protezione dei dati personali nonché dei diritti e delle libertà fondamentali dei lavoratori, sempre mediante funzionalità consentite dalla normativa vigente.

RUOLI E RIFERIMENTI

Organizzazione e referenti

L'Area ICT si articola internamente in servizi e settori in modo da potere rispondere adeguatamente alle necessità informatiche dell'Ateneo.

Nell'ambito della propria attività si avvale della collaborazione di referenti qualificati individuati nelle strutture interne all'Ateneo e/o dipendenti di aziende e/o professionisti esterni a Unige, a cui l'Area ICT può delegare ruoli amministrativi e di riferimento. Nell'ambito di questo rapporto, tali figure comunque agiscono e rispondono delle proprie azioni come afferenti all'Area ICT.

Ruolo degli amministratori

Gli Amministratori dell'Area ICT svolgono le attività necessarie per garantire la salvaguardia del sistema informativo e delle applicazioni conformemente alle politiche e alle istruzioni impartite dall'Ateneo e nel rispetto della normativa vigente con particolare riferimento alla protezione dei dati personali. Qualora si renda necessario procedere a operazioni finalizzate al ripristino della funzionalità del Sistema informativo comportanti l'accesso a cartelle, file o archivi di altri Utenti, gli Amministratori sono tenuti ad avvisare gli interessati, limitando il proprio intervento a quanto strettamente necessario.

ASSISTENZA, INFORMAZIONE, FORMAZIONE

Gli utenti possono ottenere assistenza e informazioni tramite i canali previsti dall'Ateneo per le varie casistiche, così come pubblicato sulle pagine dell'Ateneo e più specificatamente dell'Area ICT. I canali preferenziali da cui partire con una richiesta di assistenza o di informazioni, salvo per casi specifici e diversamente indicati, sono l'Help Desk dell'Area ICT e i tecnici locali di riferimento (tecnici di dipartimento, presidii). La richiesta di assistenza o di informazioni verrà instradata internamente nella maniera più consona, al fine di fornire una risposta adeguata nel minor tempo possibile e un corretto trattamento del caso.

Gli utenti non devono cercare di contattare direttamente un supporto specialistico interno all'Area ICT, se non specificatamente indicato dal personale di supporto, né possono scegliere di essere assistiti da specifiche persone.

L'assistenza informatica dell'Ateneo copre le risorse e gli strumenti informatici di Unige, ma non quelle esterne ad esso, o comunque fuori dalla propria gestione. Esempio: può essere offerta assistenza per la configurazione della posta elettronica di ateneo, ma non per l'allestimento del computer di proprietà dell'utente. Il limite dell'intervento viene di volta in volta definito e chiarito dal personale di supporto tecnico di Unige.

Supporto all'acquisizione di risorse informatiche

L'Area ICT fornisce supporto all'acquisizione di risorse informatiche a diversi livelli, a seconda della destinazione e della finalità dell'oggetto e del successivo modello di gestione. Il livello di coinvolgimento dell'Area ICT può variare a seconda delle necessità e prevede che l'acquisto venga indirizzato per soddisfare sia le necessità tecniche immediate, sia quelle di gestione successiva. Di particolare rilevanza, nel caso dell'hardware, è la progettazione del successivo ciclo di gestione dell'oggetto. Nel caso del software, l'Area ICT si premura soprattutto di

assicurare l'individuazione del corretto applicativo, l'inserimento del software nel modello di gestione, la compatibilità con le risorse informatiche di Ateneo, la sicurezza.

La consultazione, quando necessaria, deve avere luogo nella fase di analisi del bisogno, precedente alla presa di accordi con terzi o di indagine economica. Il parere dell'Area ICT in merito è vincolante. L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente o sull'ufficio possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni.

Tutte le acquisizioni di risorse informatiche dell'amministrazione centrale richiedono il coinvolgimento dell'Area ICT dal primo momento (es. uffici, stampanti, telefonia, reti, software).

Tutte le acquisizioni di risorse informatiche rivolte al pubblico o agli studenti richiedono il coinvolgimento dell'Area ICT dal primo momento (es. aule informatiche, sale conferenze, sia hardware che software).

Tutte le acquisizioni di risorse informatiche che prevedano un coinvolgimento dell'Area ICT nella gestione richiedono il coinvolgimento dell'Area ICT dal primo momento (es. dipartimenti carenti di personale tecnico informatico e assistiti dall'Area ICT, software da integrare con le risorse informatiche di Ateneo o con l'infrastruttura di autenticazione).

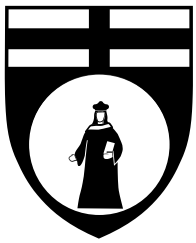
Per le acquisizioni di particolari tipi di apparecchiature o software le Strutture Fondamentali possono avvalersi della consulenza dell'Area ICT (es. Workstation particolarmente potenti, infrastrutture hardware e software complesse e necessitanti integrazione)

Per i dispositivi ad uso personale più comuni, si consiglia comunque una consultazione del personale tecnico locale (es. portatile personale pagato su fondi di ateneo, non per acquisti privati).

Gli acquisti di dispositivi personali da parte degli studenti non prevedono un'assistenza specifica dell'Area ICT, ma l'eventuale stipula di convenzioni richiede il coinvolgimento dell'Area ICT dal primo momento (es. sconti da particolari fornitori).

Formazione

L'Utente ha diritto ad essere formato all'utilizzo delle risorse informatiche in uso in Ateneo. L'Area ICT provvede a questo fabbisogno tramite la progettazione di corsi erogati con risorse interne ed esterne all'Ateneo. Periodicamente provvede all'erogazione di corsi ai nuovi utenti e aggiornamenti per gli utenti già presenti. In alcuni casi, l'Area ICT può richiedere l'erogazione di corsi fuori dalla pianificazione, per motivata urgenza, e corsi obbligatori per categorie di utenti, per necessità di sicurezza o di funzionamento.



Università
di Genova

Linea Guida ICT

Tecnologie da adottare

Versione	Autori
Ottobre 2024	Paolo Moresco (Area ICT) Stefano Orocchi (Area ICT) Marco Ferrante (Area ICT) Massimo Di Spigno (Area ICT)

Sommario

Introduzione

L'Università degli Studi di Genova, a cui ci si riferisce in seguito come Unige, o Ateneo, nell'espletamento della sua attività istituzionale opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

Il presente documento definisce le regole e le condizioni per l'utilizzo degli strumenti informatici dell'Ateno da parte dei dipendenti, degli studenti e di tutti coloro che, in virtù di un rapporto di lavoro, di studio, o di ricerca, a qualsiasi titolo (collaboratori, consulenti, stagisti, fornitori, studenti esterni, etc.), utilizzano strumenti informatici dell'Ateno, nel seguito denominati Utenti.

Il presente documento deve considerarsi integrato da tutte le procedure interne adottate per argomenti specifici e casistiche, così come pubblicati sul sito dell'Ateneo e più specificatamente dell'Area ICT.

Finalità del documento

Il presente documento definisce e detta agli Utenti specifiche regole e condizioni di utilizzo degli strumenti informatici aziendali attraverso:

- definizione di regole e procedure uniformi da applicarsi in tutte le aree operative e Strutture organizzative;
- definizione di regole e procedure attinenti a specifici ambiti di applicazione;
- indicazione del corretto approccio da seguire in assenza di regole specifiche per una determinata specifica casistica;
- indicazione delle principali disposizioni normative in materia di utilizzo dei sistemi informativi e di protezione dei dati personali;
- definizione dell'ambito, delle modalità, dei limiti del monitoraggio e dei controlli attuabili dall'Ateneo nel rispetto della normativa vigente nonché delle regole e delle procedure interne.

Contesto normativo e regolamentare

Il presente regolamento è redatto sulla base dei seguenti e principali riferimenti normativi:

- Codice penale, con particolare riferimento ai reati informatici;
- L. 300/1970 (Statuto dei lavoratori) - artt. 4, 7 e 8 e successive modificazioni;
- D. Lgs. 196/2003 e s.m.i(Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per posta elettronica e Internet" di cui alla deliberazione 13/2007;
- D. Lgs. 81/2008 e s.m.i (Testo Unico sulla sicurezza);
- D.P.R 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione) e Codice di comportamento Unige;
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR)

- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1417809
- REGOLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
- DECRETO LEGISLATIVO 4 settembre 2024, n. 134 (recepimento NIS 2) - Attuazione della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio. (24G00150) (GU Serie Generale n.223 del 23-09-2024)
- Piano Implementativo Strategia Nazionale Cybersicurezza 2022-2026
- Piano Triennale per l'informatica nella PA
- Legge 9 gennaio 2004, n. 4 (Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilita' agli strumenti informatici
- Direttiva (UE) 2019/882 del parlamento europeo e del consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi
- Normativa sull'accessibilità reperibile presso AgID https://www.agid.gov.it/it/design-servizi/accessibilita/normativa

GLOSSARIO E DEFINIZIONI

Ai fini del presente documento si intende per:

- Amministratori di sistema: figure professionali finalizzate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009;
- Applicazioni aziendali: si considerano applicazioni aziendali:
    - Prodotti/programmi acquistati dall'Ateneo, di valenza generale, o settoriale ed in quest'ultimo caso approvati dall'Area ICT;
    - Applicazioni e servizi sviluppati ad hoc dell'Area ICT, da terze parti ma sotto il coordinamento dell'Area ICT, ovvero da altre strutture con un processo di partecipazione e approvazione da parte dell'Area ICT e che seguono le regole di gestione previste nei casi precedenti;
    - Applicazioni esterne che l'Ateneo utilizza secondo le regole di gestione e di sicurezza delle medesime a titolo di mero esempio possono essere la piattaforma NoiPA, abbonamenti a servizi informativi, portale ANAC, etc.
- Aziendali: nel corso del documento si farà spesso riferimento a risorse o dispositivi come "aziendali". Pur nella consapevolezza che l'Ateneo non è un'azienda, tale dicitura identifica più chiaramente l'organizzazione nella letteratura tecnica.
- Dispositivi o endpoint: qualunque dispositivo atto a connettersi alla rete Unige, ai suoi dati, alle applicazioni aziendali, alle risorse in genere.
- Dispositivi aziendali: dispositivi di proprietà o comunque nelle disponibilità dell'Università degli studi di Genova e messi nelle disponibilità degli utenti.
- File di log: registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato;
- GENUAnet: rete informatica gestita direttamente dall'Università di Genova divisa in rete cablata e rete WiFi eduRoam (già GenuaWiFi);
- Strumenti informatici: personal computer fissi o portatili o virtuali, stampanti locali o di rete, programmi e prodotti software in-house o in-cloud, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc);
- Utenti: personale dipendente, docenti, studenti, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni e coloro che, in virtù di un rapporto di lavoro, di studio o di collaborazione in essere a qualsiasi titolo con l'Ateneo, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione da Unige.

PRINCIPI GENERALI

L'Ateneo si avvale di tutte le moderne tecnologie necessarie allo svolgimento delle sue attività, provvedendo a regolamentarne l'introduzione, tenendo conto dell'ambito di applicazione, della finalità dell'introduzione, delle risorse disponibili alla corretta gestione.

Gli ambiti di applicazione possono in prima analisi includere produttività personale, produttività generale o di gruppi di lavoro, collaborazione con altre organizzazioni, ricerca, didattica.

Tutte le attività si svolgono all'interno dei regolamenti di Ateneo e delle leggi in vigore. Valgono in generale tutte regole e le raccomandazioni contenute nel presente documento e nell'insieme delle regole di Ateneo.

Le attività di ricerca e didattica si svolgono per loro natura con un elevato grado di autonomia degli utenti coinvolti e possono richiedere l'impiego di una maggiore varietà di tecnologie rispetto a quelle normalmente disponibili per le attività di ufficio. Valgono per esse regole specifiche che ne permettono lo svolgimento armonizzato nella maniera più ampia.

Nell'esecuzione della propria attività, gli Utenti sono tenuti ad attenersi alle seguenti istruzioni generali:

a. effettuare la propria attività uniformandosi alle disposizioni dell'Ateneo e alle istruzioni ricevute;
b. custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente alle strutture preposte, secondo le modalità previste, ogni danneggiamento, smarrimento o furto;
c. mantenere la riservatezza sulle informazioni e sui dati personali di cui siano venuti a conoscenza durante lo svolgimento della propria attività;
d. in caso di cessazione dal servizio, dalla prestazione o dal rapporto con l'Ateneo, astenersi dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività, in funzione della natura di riservatezza del dato;
e. adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati;
f. garantire la corretta custodia di atti e documenti adottati da Unige;
g. promuovere la piena integrazione delle persone con disabilità.

REGOLE PER L'INTRODUZIONE DI NUOVE TECNOLOGIE NEI SISTEMI INFORMATICI DI ATENEO

Ambito di applicazione

Le linee guida presenti disciplinano e indirizzano nell'adozione di tecnologie di natura e impatto estremamente diversificati ed eterogenei. L'introduzione di nuove tecnologie può consistere nelle seguenti fattispecie, la cui lista è a titolo di esemplificazione e non è da considerarsi esaustiva:

- Introduzione di ambienti cloud di uso generale (es. Microsoft 365)
- Introduzione di applicazioni di uso diffuso (es. Titulus, Autocad, Matlab, LimeSurvey, software e servizi per la didattica)
- Allestimento di sistemi di archiviazione centralizzati, hardware o cloud (es. datacenter, anche locali, Sharepoint)
- Introduzione di sistemi di comunicazione hardware e software (es. sistema telefonico, Teams)
- Introduzione di sistemi di gestione di dispositivi, di utenti o di dati (es. Intune, AD DS, Defender)
- Allestimento di ambienti in appoggio allo smartworking (es. Teams rooms)
- Allestimento di ambienti di didattica e collaborazione (es. aule didattiche, aule informatiche)
- Introduzione di sistemi di rielaborazione dell'informazione (es. ChatGPT)

Viene disciplinata o indirizzata qualunque tecnologia, hardware o software, che abbia un ampio impatto nell'attività dell'organizzazione, oppure che vada a lambire ambiti particolarmente sensibili, tra i quali si annoverano:

- sicurezza informatica in genere
- identità e riservatezza
- accessibilità e usabilità
- storage e basi di dati centrali in produzione
- storage e basi di dati sotto il controllo diretto degli utenti
- sistemi di telecomunicazione e trasferimento dei dati

Ruolo dell'Area ICT

L'Area ICT si fa carico di proporre proattivamente l'allestimento di nuove tecnologie informatiche, oltre che di raccoglierne le richieste da parte dell'utenza, valutarne l'applicabilità, produrre una strategia di introduzione, ovvero soluzioni sostitutive.

Compito dell'Area ICT è di armonizzare l'introduzione delle tecnologie a tutti i livelli, dai portali di uso generale alle applicazioni ad uso personale, consentendo l'interoperabilità delle tecnologie e prevenendo situazioni di malfunzionamento e abuso.

L'Area ICT fornisce supporto all'acquisizione di risorse informatiche a diversi livelli, a seconda della destinazione e della finalità dell'oggetto e del successivo modello di gestione. Il livello di coinvolgimento dell'Area ICT può variare a seconda delle necessità e prevede che l'acquisto venga indirizzato per soddisfare sia le necessità tecniche immediate, sia quelle di gestione successiva.

Di particolare rilevanza, nel caso dell'hardware, è la progettazione del successivo ciclo di gestione dell'oggetto. Nel caso del software, l'Area ICT si premura soprattutto di assicurare l'individuazione del corretto applicativo, l'inserimento del software nel modello di gestione, la compatibilità con le risorse informatiche di Ateneo, la sicurezza.

La valutazione delle nuove tecnologie avviene in considerazione di diversi principi e regole che richiedono un opportuno equilibrio.

- Qualora venga valutata l'introduzione di una nuova tecnologia destinata a soddisfare una necessità già coperta da una tecnologia in essere in modo equivalente, si tende a preferire quest'ultima e a reindirizzare l'utenza sul suo adeguato utilizzo.
- Qualora venga valutata l'introduzione di una nuova tecnologia con performance apprezzabilmente superiori a una precedente, si tende a preferire l'introduzione della nuova tecnologia, compatibilmente con le possibilità di pianificazione e le risorse disponibili.
- Vengono preferite tecnologie la cui introduzione possa essere inquadrata in un piano integrato di allestimento a lungo termine, in osservanza degli obblighi di legge, dei regolamenti, degli indirizzi della governance, delle strategie già pianificate.
- Vengono preferite tecnologie di ampia diffusione, ampia e chiara documentazione, massima interoperabilità, possibilità di supporto efficiente e scalabile, economicità di acquisto e gestione.
- Vengono considerati gli aspetti legali riconducibili alla tecnologia, alla sua origine, anche geografica, alla sua rispondenza alle leggi e ai regolamenti in vigore nell'organizzazione, in Italia, in Europa.
- Vengono preferite modalità di acquisizione che permettano una stima economica chiara e conveniente in fase di acquisto, di rinnovo, di ampliamento del contratto, oltre che una pianificazione chiara e sostenibile dell'impegno di manutenzione e adeguamento durante tutto il periodo di disponibilità.
- Vengono considerati già in fase preliminare gli aspetti economici e logistici legati all'intero ciclo di vita della tecnologia.

La consultazione, quando necessaria, deve avere luogo nella fase di analisi del bisogno, precedente alla presa di accordi con terzi o di indagine economica. Il parere dell'Area ICT in merito è vincolante. L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente o sull'ufficio possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni, o anche procedure legali ove necessario.

Tutte le acquisizioni di risorse informatiche dell'amministrazione centrale richiedono il coinvolgimento dell'Area ICT dal primo momento (es. uffici, stampanti, telefonia, reti, software).

Tutte le acquisizioni di risorse informatiche rivolte al pubblico o agli studenti richiedono il coinvolgimento dell'Area ICT dal primo momento (es. aule informatiche, sale conferenze, sia hardware che software).

Tutte le acquisizioni di risorse informatiche che prevedano un coinvolgimento dell'Area ICT nella gestione richiedono il coinvolgimento dell'Area ICT dal primo momento (es. dipartimenti carenti di personale tecnico informatico e assistiti dall'Area ICT, software da integrare con le risorse informatiche di Ateneo o con l'infrastruttura di autenticazione).

Tecnologie ad uso diffuso

L'introduzione di nuove tecnologie ad uso diffuso può rendersi necessaria per diversi motivi, tra i quali:

- Adempimento a obblighi di legge, regolamenti, raccomandazioni, siano essi di provenienza nazionale o europea
- Compatibilità con standard di fatto, tecnologie di ampia diffusione, interoperabilità
- Considerazioni legate alla convenienza economica od operativa
- Accoglimento di necessità percepite come diffuse nella comunità accademica
- Promozione dell'integrazione delle persone con disabilità
- Raggiungimento di obbiettivi dettati dalla governance, da gruppi di utenti, da individui

La proposta di introdurre nuove tecnologie ad uso diffuso può avvenire per iniziativa dell'Area ICT, in seguito al monitoraggio delle necessità degli utenti, oppure in seguito a un indirizzo da parte degli organi di governo dell'Ateneo.

L'Area ICT si fa carico di raccogliere le proposte di nuove tecnologie da parte degli utenti, valutarle, portarle all'opportuna sede di discussione, renderle attuabili se necessario e opportuno.

Le richieste di interlocuzione possono essere fatte pervenire attraverso i canali informativi dell'Area ICT, ossia i referenti nei dipartimenti e nelle strutture, il personale di presidio sul territorio, i recapiti dell'assistenza.

Tecnologie finalizzate alla produttività di gruppi di persone

L'introduzione di nuove tecnologie finalizzata alla produttività di gruppi di persone può rendersi necessaria per diversi motivi, tra i quali:

- Soddisfacimento di necessità oggettive nel flusso di lavoro
- Considerazioni legate alla convenienza economica od operativa
- Adempimento a obblighi di legge, regolamenti, raccomandazioni, siano essi di provenienza nazionale o europea
- Compatibilità con standard di fatto, tecnologie di ampia diffusione, interoperabilità
- Integrazione delle persone con disabilità
- Raggiungimento di obbiettivi dettati dalla governance, da gruppi di utenti, da individui

La proposta di introdurre nuove tecnologie finalizzate alla produttività di gruppi di persone può avvenire, solitamente, su iniziativa di una struttura, o di uno specifico gruppo di lavoro, ma non è escluso che avvenga per iniziativa dell'Area ICT, in seguito al monitoraggio delle necessità degli utenti, in seguito a un indirizzo da parte degli organi di governo dell'Ateneo.

L'Area ICT si fa carico di raccogliere le proposte di nuove tecnologie da parte degli utenti, valutarle, portarle all'opportuna sede di discussione, renderle attuabili se necessario e opportuno, dare indicazione delle corrette modalità quando il gruppo di interessati possa procedere in autonomia.

Le richieste di interlocuzione possono essere fatte pervenire attraverso i canali informativi dell'Area ICT, ossia, preferenzialmente, tramite i referenti nei dipartimenti e nelle strutture, o il personale di presidio sul territorio, ma anche tramite i recapiti dell'assistenza, soprattutto quando si tratti di necessità di gruppi di lavoro trasversali o geograficamente distribuiti.

Tecnologie finalizzate alla produttività personale

L'introduzione di nuove tecnologie finalizzate alla produttività personale può rendersi necessaria per diversi motivi, tra i quali:

- Soddisfacimento di necessità oggettive nel flusso di lavoro
- Considerazioni legate alla convenienza economica od operativa
- Adempimento a obblighi di legge, regolamenti, raccomandazioni, siano essi di provenienza nazionale o europea
- Compatibilità con standard di fatto, tecnologie di ampia diffusione, interoperabilità
- Integrazione delle persone con disabilità
- Raggiungimento di obbiettivi dettati dalla governance, da gruppi di utenti, da individui

Nel rispetto delle indicazioni nel presente documento, delle altre linee guida, delle leggi, dei regolamenti, delle raccomandazioni, degli indirizzi dei suoi superiori, l'utente può procedere autonomamente nell'adozione di una nuova tecnologia. Quando reputato necessario o preferibile, l'utente può richiedere di avvalersi dell'assistenza del personale tecnico di riferimento.

L'Area ICT fornisce supporto all'adozione di nuove tecnologie a diversi livelli, a seconda della destinazione e della finalità dell'oggetto e del successivo modello di gestione. Il livello di coinvolgimento dell'Area ICT può variare a seconda delle necessità e prevede che l'adozione venga indirizzata per soddisfare sia le necessità tecniche immediate, sia quelle di gestione successiva. Di particolare rilevanza, nel caso dell'hardware, è la progettazione del successivo ciclo di gestione dell'oggetto. Nel caso del software, l'Area ICT si premura soprattutto di assicurare l'individuazione del corretto applicativo, l'inserimento del software nel modello di gestione, la compatibilità con le risorse informatiche di Ateneo, la sicurezza.

La consultazione, quando necessaria, deve avere luogo nella fase di analisi del bisogno, precedente alla presa di accordi con terzi o di indagine economica. Il parere dell'Area ICT in merito è vincolante. L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente o sull'ufficio possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni.

Obblighi per il proponente

Nel proporre l'adozione di nuove tecnologie, siano esse di uso diffuso, limitato a un gruppo di utenti, o ad uso personale, è fatto obbligo per il proponente di verificare un insieme di caratteristiche.

- Verificare l'esistenza di altri prodotti già in uso all'Ateneo capaci di soddisfare le esigenze specifiche.
- Illustrare chiaramente i benefici attesi.
- Verificare le condizioni di licensing, preferendo i sistemi più manutenibili, centralizzabili
- Verificare con attenzione la provenienza, le condizioni contrattuali e le modalità d'uso per evitare problemi di natura legale o di incongruenza con l'utilizzo previsto

- Porre attenzione alle informazioni di cui è richiesta la condivisione. Frequentemente le applicazioni richiedono la condivisione di informazioni di natura personale o dell'organizzazione, del cui trattamento l'utente si fa responsabile in prima persona.
- Effettuare in collaborazione dell'Area ICT di criteri di valutazione ex-post dell'utilità del prodotto/servizio, possibilmente con una valutazione costo/utente ritenuta accettabile, e un chiaro percorso di dismissione.
- Valutazione del rispetto dei requisiti di accessibilità e usabilità, o chiara valutazione dei motivi di esclusione dai requisiti.

L'Area ICT fornisce supporto in questa attività di indagine con vari livelli di coinvolgimento, a seconda delle necessità.

Didattica e Ricerca

Le attività di ricerca e di didattica si svolgono all'interno dei regolamenti di Ateneo e delle leggi in vigore. Valgono in generale tutte regole e le raccomandazioni contenute nel presente documento e nell'insieme delle regole di Ateneo.

Le attività di ricerca e didattica si svolgono per loro natura con un elevato grado di autonomia degli utenti coinvolti e possono richiedere un maggiore dispiegamento di tecnologie, anche sperimentali, nonché una varietà di configurazioni di dispositivi e di applicativi rispetto a quelli normalmente disponibili per le attività di ufficio. L'utilizzo di tecnologie, configurazioni, applicazioni, modalità di utilizzo diverse da quelle già considerate consone per l'attività in Ateneo richiede una consultazione preventiva dell'Area ICT per l'individuazione della maniera più consona di soddisfacimento della necessità (Esempio: una ricerca sui virus informatici potrebbe richiedere il corretto isolamento dell'ambiente di test e l'esclusione dell'accesso alla rete di produzione).

Viene preferita una separazione forte tra l'ambiente adibito alla ricerca, i suoi dati e il suo funzionamento e l'ambiente di produzione, in un'ottica di non ingerenza dei dati e delle attività quando sussista rischio per la sicurezza o per il corretto andamento di una delle due attività.

Viene preferita una integrazione gestionale tra le tecnologie utilizzate nell'ambito della didattica e quello di produzione, per favorirne la gestione centrale da parte dell'Area ICT e, l'integrazione all'interno delle attività ordinarie dell'Ateneo e in generale il principio di "una sola volta (*once only)*".

L'accesso a dati del sistema informativo di Unige, soprattutto se contenenti dati personali, l'utilizzo di applicazioni con uscita o condivisione di dati dal sistema informativo di Unige, l'iscrizione degli Utenti Unige a servizi non gestiti internamente, sono tutti esempi di attività che necessitano di consultazione preventiva dell'Area ICT.

È necessario prevedere già in fase di stesura dei progetti di ricerca gli strumenti e i servizi ICT di cui si necessiti, consultando il personale dell'Area ICT per esaminare le necessità e cercare soluzioni che preservino in primo luogo la sicurezza dell'utente e la funzionalità dell'infrastruttura informatica di Ateneo. I casi più comuni possono essere coperti dall'osservanza di semplici indicazioni sul sito di Ateneo e più specificatamente dell'Area ICT.

La consultazione deve avere luogo nella fase precedente alla presa di accordi con terzi o di indagine economica, in particolare se il progetto prevede la gestione di lungo periodo di prodotti, archivi o applicazioni. Il parere dell'Area ICT in merito è vincolante. L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e

delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni, o anche procedure legali ove necessario.

Collaborazione con altre organizzazioni

L'attività dell'Università di Genova, per la natura della sua missione, è caratterizzata da un costante scambio informativo e tecnologico con altre organizzazioni.
L'interscambiabilità tra i sistemi viene agevolata per quanto possibile dall'attività dell'Area ICT, la quale si fa carico di esaminare le necessità e cercare soluzioni che preservino in primo luogo la sicurezza dell'utente e la funzionalità dell'infrastruttura informatica di Ateneo, nei limiti delle risorse a sua disposizione.
L'accesso reciproco tra i sistemi informatici dell'Ateneo e delle organizzazioni esterne è sottoposto alle restrizioni dovute alle legislazioni e ai regolamenti vigenti.
Le necessità più comuni possono essere coperte dall'osservanza di semplici indicazioni sul sito di Ateneo e più specificatamente dell'Area ICT.
La consultazione, se invece necessaria, deve avere luogo nella fase precedente alla presa di accordi con terzi o di indagine economica. Il parere dell'Area ICT in merito è vincolante. L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni, o anche procedure legali ove necessario.

AUTONOMIA DELL'UTENTE, CONTROLLO E MONITORAGGIO

La sempre maggiore varietà e complessità delle tecnologie a disposizione degli utenti e la necessità di procedure snelle di acquisizione delle stesse portano l'Area ICT alla definizione di procedure che garantiscano la massima autonomia e flessibilità per l'utente, pur garantendo la sicurezza delle identità e dei dati.

Dove possibile, vengono incentivati sistemi di controllo automatizzato della disponibilità di applicazioni che consentano agli utenti di procedere in autonomia all'allestimento di quanto necessario allo svolgimento della propria attività, pur coadiuvando l'impegno sul fronte della sicurezza. Esempi di queste tecnologie consistono in:

- adozione di store aziendali gestiti (cataloghi di applicazioni)
- controlli sul consenso alla condivisione dei dati
- catalogazione dell'informazione
- politiche di controllo gestito delle configurazioni dei dispositivi e delle applicazioni
- monitoraggio del flusso informativo

Il dispiegamento delle suddette tecnologie e il loro corretto impiego da parte degli utenti vengono documentati sul sito di Ateneo e più specificatamente dell'Area ICT.

L'Area ICT imposta la propria azione di monitoraggio e controllo sui sistemi informatici di Ateneo messi a disposizione per lo svolgimento delle attività nel rispetto della normativa vigente e sul presupposto di un utilizzo responsabile degli stessi da parte degli Utenti, adottando in ogni caso

le soluzioni tecnologiche idonee a garantire i profili di sicurezza dei sistemi informativi e dei dati gestiti.

A tal fine, l'Area ICT utilizza sistemi automatizzati per il monitoraggio centralizzato che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la funzionalità e la sicurezza degli apparati informatici di Ateneo e delle informazioni ivi contenute.

Gli amministratori di sistema, nel caso in cui rilevino anomalie o configurazioni non corrette dei dispositivi, possono provvedere a isolare immediatamente l'origine dell'anomalia o del malfunzionamento anche senza preavvisare l'Utente, per salvaguardare la sicurezza e l'integrità dei sistemi informativi di Unige. In tal caso, verrà data successiva informativa all'Utente sui motivi dell'avvenuto intervento da parte degli amministratori di sistema. Le già menzionate attività sono svolte nel rispetto dei principi di gradualità, pertinenza e non eccedenza stabiliti dal Garante per la protezione dei dati personali nonché dei diritti e delle libertà fondamentali dei lavoratori, sempre mediante funzionalità consentite dalla normativa vigente.

Università di Genova

Linea Guida ICT

Utilizzo delle reti

Versione	Autori
Ottobre 2024	Agnese Arosio (Area ICT) Giorgio Bertorello (Area ICT) Claudio Di Martino (Area ICT) Francesco Fronda (Area ICT) Massimo Ivaldi (Area ICT) Gianni Verduci (Area ICT) Massimo Di Spigno (Area ICT)

Sommario

Introduzione

L'Università degli Studi di Genova, a cui ci si riferisce in seguito come Unige, o Ateneo, nell'espletamento della sua attività istituzionale opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

Il presente documento deve considerarsi integrato da tutte le procedure interne adottate per argomenti specifici e casistiche, così come pubblicati sul sito dell'Ateneo e più specificatamente dell'Area ICT.

Finalità del documento

Il presente documento è da considerarsi parte integrante delle "Linee guida per la sicurezza e l'utilizzo delle risorse informatiche dell'Ateneo": più specificatamente in questo elaborato si vogliono definire specifiche regole e condizioni di utilizzo della Rete Dati e del Sistema Telefonico di Ateneo.

Contesto normativo e regolamentare

Il presente regolamento è redatto sulla base dei seguenti e principali riferimenti normativi:

- Regolamento dell'Università degli Studi di Genova per la realizzazione e la gestione della rete dati
  https://ict.unige.it/sites/ict.unige.it/files/pagine/Regolamento-reti_0.pdf
- Norme Tecniche Attuative del Regolamento per la realizzazione e la gestione della rete dati
  https://ict.unige.it/sites/ict.unige.it/files/pagine/NormeTecnicheAttuative.pdf
- Acceptable User Policy (AUP) di GARR
  https://www.garr.it/it/regole-di-utilizzo-della-rete-aup

GLOSSARIO E DEFINIZIONI

Ai fini del presente documento si intende per:

- **ACN** https://www.acn.gov.it :
  E' l'Agenzia per la Cybersicurezza Nazionale, istituita dal Decreto-legge n.82 del 14 giugno 2021 che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.
  L'Agenzia per la cybersicurezza nazionale (ACN) è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza.
  L'Agenzia ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico. Si occupa di prevenire e mitigare il maggior numero di attacchi cibernetici e di favorire il raggiungimento dell'autonomia tecnologica.

- **AP**
  Acronico di Access Point (Punto di Accesso), identifica l'apparato/dispositivo che eroga le reti wireless GenuaWiFI/Eduroam, diffondendo il segnale radio in un determinato raggio d'azione.

- **AUP** (Acceptable Use Policy) di GARR https://www.garr.it/it/regole-di-utilizzo-della-rete-aup :
  Sono le regole di corretto utilizzo e comportamento emanate dal Consortium GARR, alle quali sono soggetti gli enti autorizzati ad accedere alla Rete GARR.

- **Client**
  In generale, termine che definisce la postazione di lavoro dell'utente. Si tratta del dispositivo terminale, che è interconnesso alla rete dati (sia cabalata che wireless).

- **CSIRT Italia** https://www.csirt.gov.it :
  E'istituito presso l'Agenzia per la Cybersicurezza Nazionale (ACN). I compiti del CSIRT sono definiti dal Decreto Legislativo 18 maggio 2018, n. 65 e dal Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 art. 4. Essi includono:
  - il monitoraggio degli incidenti a livello nazionale;
  - l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
  - l'intervento in caso di incidente;
  - l'analisi dinamica dei rischi e degli incidenti;
  - la sensibilizzazione situazionale;
  - la partecipazione alla rete dei CSIRT.

- Il CSIRT stabilisce relazioni di cooperazione con il settore privato.
  Per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi comuni o standardizzate nei settori delle procedure di trattamento degli incidenti e dei rischi e sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

- **Eduroam** (*EDUcation ROAMing*) https://eduroam.org :
  E'il servizio internazionale di roaming wireless per persone che lavorano nella ricerca e nell'istruzione superiore.
  Fornisce a ricercatori, insegnanti e studenti accesso facile e sicuro alla rete quando visitano istituzioni diverse da quella in cui lavorano. L'autenticazione degli utenti è eseguita dalla loro istituzione di origine, usando le stesse credenziali fornite da essa, mentre l'autorizzazione all'accesso a Internet e ad altre risorse è gestita dall'istituzione ospite. Non è richiesto alcun pagamento per l'utilizzo di eduroam. Il servizio è fornito a livello locale dalle istituzioni partecipanti (università, istituti di ricerca ecc.), mentre a livello nazionale è organizzato dagli operatori del paese.

- **GARR** https://www.garr.it :
  E' la rete nazionale ad altissima capacità dedicata alla comunità dell'istruzione, della ricerca e della cultura. Il suo principale obiettivo è quello di fornire connettività ad alte prestazioni e di sviluppare servizi innovativi per le attività quotidiane di docenti, ricercatori e studenti e per la collaborazione a livello internazionale.
  La rete GARR è progettata e gestita dal Consortium GARR, un'associazione senza fini di lucro fondata sotto l'egida del Ministero dell'Istruzione, dell'Università e della Ricerca. Gli enti soci sono CNR, ENEA, INAF, INGN, INGV e tutte le università italiane rappresentate dalla Fondazione CRUI.

- **GenuaNET**:
  E'il sistema integrato di reti dell'Università degli Studi di Genova ed è composto da:
  - rete geografica: realizza l'interconnessione dei poli genovesi e dei poli distaccati dell'Università di Genova e comprende collegamenti verso l'esterno dell'Ateneo; per poli si intendono edifici o gruppi di edifici nei quali sono dislocate strutture universitarie;
  - reti comprensoriali: all'interno di un polo, realizzano l'interconnessione fra le reti locali e la rete geografica;
  - reti locali: realizzano le interconnessioni interne alle strutture universitarie;
  - rete wireless di Ateneo (GENUAwi-fi)

- **GENUAwi-fi**:
  E'la rete componente GENUAnet realizzata con tecnologia wireless, gestita in modo centralizzato e utilizzabile da coloro che dispongono delle credenziali personali UniGePASS; complementa la rete cablata (wired);

- **Indirizzo IP**
  E' una sequenza numerica, che identifica una interfaccia di rete, connessa ad una rete che implementa i protocolli TCP/IP.

- **Indirizzo IP privato**
  Identifica una interfaccia di rete utilizzando un indirizzamento non raggiungibile direttamente da Internet.

- **Proxy server**
  Server che viene utilizzato come intermediario tra le richieste di un client e il server

finale destinatario delle richieste. È impiegato all'interno di reti complesse con diverse finalità, per migliorare la sicurezza e l'efficienza nell'erogazione dei servizi.

- **UniGePass** https://ict.unige.it/UniGePASS :
  E'il sistema di autenticazione di Ateneo, che consente agli utenti di accedere alla rete e alla maggior parte dei servizi informatici mediante le credenziali personali UniGePASS, attualmente costituite da nome utente, password ed eventuale secondo fattore di autenticazione (2FA).

PRINCIPI GENERALI

GenuaNet è la rete telematica dell'Ateneo che ha lo scopo di collegare tutte le aree ove sono ubicate le sedi dedicate alla didattica, alla ricerca e agli uffici amministrativi, distribuite sia in ambito cittadino che in quello regionale. La sua architettura è complessa e comprende sia la rete geografica che quelle di comprensorio, le reti locali e quelle wireless.

Utilizzando la rete GenuaNET e la connessione di GenuaNET a internet tramite la rete GARR, è possibile per i suoi utenti collegarsi alla rete e interagire per gli scopi più diversi, come, per es., la consultazione di archivi e banche dati, la partecipazione a corsi o conferenze on-line, l'utilizzo di risorse computazionali, lo scambio di informazioni, utilizzando sistemi di interconnessione moderni e all'avanguardia.

La complessità, l'estensione e la pervasività della rete pongono inoltre sfide importanti per l'implementazione di adeguati livelli di sicurezza (relativi a riservatezza, integrità e disponibilità) sia della rete stessa che delle risorse accessibili per suo tramite.

L'Area ICT dell'Ateneo ha nel tempo sviluppato, adottato e consolidato strategie al fine di favorire e semplificare le attività di messa in sicurezza della rete stessa, dei servizi erogati in rete, come pure dei dati custoditi sui sistemi ad essa collegati, avvallate anche dalle good practices diventate di implementazione comune.

A titolo esemplificativo (e non esaustivo) indichiamo tra le strategie adottate:

- Azioni per minimizzare la superficie esposta a potenziali attacchi:
  - Conoscere approfonditamente i servizi di rete pubblicati e i sistemi ad essa collegati
  - Evitare l'esposizione non mediata dei servizi e dei sistemi
  - Consentire l'accesso ad ogni specifica risorsa di rete solo alle postazioni/utenze che ne hanno effettiva necessità

- Azioni per ridurre l'impatto di eventuali guasti o malfunzionamenti di componenti HW o SW:
  - Ridondare tutte le componenti HW e SW per non avere singoli punti di fallimento
  - Aggiornare e manutenere accuratamente, puntualmente e costantemente tutte le componenti HW e SW che costituiscono l'infrastruttura dei servizi di rete

- Azioni atte a validare tutti gli accessi in maniera motivata, non per default:
  - Adottare tecniche di autenticazione e autorizzazione all'accesso solide ed efficaci
  - Autorizzare all'accesso sulla base di ruoli e funzioni

- Studio delle minacce più comuni e di quelle emergenti per mantenere un costante ed aggiornato livello di conoscenza e di consapevolezza delle problematiche associate e per una adeguata adozione di misure e strategie di contenimento del rischio ad esse connesse

- Attività di monitoraggio delle risorse nelle reti interne alle Strutture

- Adozione di piani di formazione e aggiornamento di tutti gli utenti

L'applicazione delle strategie sopra elencate e il costante aggiornamento delle azioni di mitigazione dei rischi finora adottate, ha portato l'Area ICT a sviluppare le regole sotto riportate a cui si dovrà fare esplicito riferimento a seconda delle aree di intervento o di interesse.

REGOLE PER L'UTILIZZO DELLA RETE CABLATA

Disposizioni generali

I dispositivi di qualunque natura utilizzati dalle Aree, dai Centri, dalle Scuole, dai Dipartimenti e dal personale e gli utenti relativi, possono essere collegati alla LAN della struttura di appartenenza, rispettando le seguenti norme:

- la Rete può essere usata esclusivamente per le attività istituzionali;
- l'accesso alla Rete di Ateneo dovrà, comunque e in qualsiasi caso, essere conforme alle regole stabilite dall'Ateneo e dalle AUP del GARR;
- la gestione delle interconnessioni comuni ad altri Enti è condotta dall'Area ICT insieme ai rispettivi gestori degli Enti stessi, secondo protocolli definiti da accordi specifici;
- nessuna Struttura può attivare connessioni autonome dalle proprie reti locali di struttura con quelle di altre Strutture, se non concordate ed approvate preventivamente dall'Area ICT;
- per avere un chiaro controllo dei flussi comunicativi, anche internamente ad ogni Struttura deve essere mantenuta una topologia logica e fisica di rete che non presenti interconnessioni che realizzino magliature, di fatto moltiplicando i percorsi possibili;
- ogni Struttura che, a protezione della propria rete locale, abbia necessità di impiegare firewall, è tenuta a comunicare e concordare con l'Area ICT la configurazione degli stessi, prima della relativa implementazione, in modo da poter armonizzare le policy implementate con quelle di Ateneo e delle altre Strutture e assicurare l'accesso ai servizi di Ateneo dalle postazioni locali;
- tutti i sistemi collegati alla rete devono essere identificati, conosciuti e riconducibili ad almeno un referente responsabile che sia contattabile in caso di necessità e ne devono essere registrati gli indirizzi IP assegnati, interno alla Struttura oppure di riferimento nel polo territoriale di competenza;
- l'auto assegnazione da parte dell'utente di indirizzi IP è espressamente vietata;
- tutti gli utenti a cui viene fornito accesso alla Rete devono essere identificati e identificabili;
- l'accesso a Internet da postazioni accessibili al pubblico può essere effettuato solo tramite accreditamento con credenziali personali e deve essere trattato a norma di legge.

Inoltre:

- l'accesso alle risorse della rete è personale e non può essere condiviso o ceduto;
- la responsabilità del contenuto dei materiali prodotti e diffusi attraverso la rete è delle persone che li producono e diffondono;
- gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso;
- gli utenti sono responsabili delle attività svolte sui dispositivi che possano compromettere la piena funzionalità e sicurezza della rete e dei sistemi ad essa collegati.

Regole per l'implementazione della Rete Cablata: segmentazione

Al fine di rispettare i criteri generali sopra indicati, come regola tecnica principe da seguire nell'implementazione di reti cablate si richiede di effettuare la cosiddetta "segmentazione" (possibilmente fisica) della rete, prevedendo l'assegnazione di indirizzi privati in segmenti di rete classificati.

In particolare, si raccomanda di prevedere almeno:

- un segmento ben identificato e destinato ai dispositivi classificati "insicuri" (guest, non amministrati direttamente, non rispondente agli standard di sicurezza individuati, ecc.);
- un segmento destinato ai dispositivi approvati e quindi indicato come "sicuro";
- una serie di sottoreti opportunamente suddivise, isolate e protette riservate ai servizi erogati.

La corretta classificazione dei segmenti di rete consente una gestione più semplice, ordinata e coordinata delle regole che determinano i flussi di comunicazione validati e ammessi all'interno della rete GenuaNET e verso internet.

Nel rispetto della suddetta classificazione, sarà quindi possibile collegare un dispositivo in rete, attraverso apposite prese allestite nei locali, purché, per le Scuole, i Dipartimenti e i Centri, venga richiesto preventivamente all'Area ICT, attraverso richiesta al Presidio Territoriale di competenza, la verifica preventiva della fattibilità, interfacciandosi con il Settore Rete Dati e Fonia, attraverso il canale messo a disposizione dall'indirizzo e-mail di servizio retifonia@unige.it .

È altresì possibile utilizzare la rete cablata per collegare PC personali, purché vengano rispettati i requisiti di sicurezza forniti dall'Area ICT e la collocazione nei segmenti di rete classificati a tal scopo.

Per tale motivo è necessario, per i Dipartimenti e i Centri, fare riferimento alle indicazioni dei propri referenti ICT, che potranno interfacciarsi con i Presidi di Facility Management, e per l'Amministrazione Centrale e i Servizi Tecnici, fare riferimento diretto ai Presidi stessi.

Se le caratteristiche dei dispositivi saranno tali da rispettare i requisiti di sicurezza indicati, sia dal punto di vista software che hardware, la postazione potrà essere considerata idonea per la configurazione in rete che prevederà in ogni caso l'assegnazione di un indirizzo IP privato e l'impiego del proxy server per il controllo del traffico.

Procedure per la realizzazione ex novo/rinnovo/ della Rete Cablata

In caso non fossero presenti prese di rete in numero sufficiente nei locali in cui è richiesto l'utilizzo, è necessario attenersi alle seguenti indicazioni:

1. in caso di progettazione di nuovi edifici e nelle ristrutturazioni di edifici o di porzioni di essi l'Ateneo prevede, finanzia e realizza tramite l'Area ICT la connessione in rete locale di ogni postazione telematica di lavoro o di studio (cablaggio standard) di ciascuna Struttura, comprese le apparecchiature di rete: l'Area ICT provvede, pertanto, a realizzare il cablaggio "verticale" di dorsale a proprio carico, fornendo connettività ai piani degli edifici;

2. in caso di impianti esistenti, ma non più a norma oppure obsoleti e nel caso in cui una rete locale di Struttura risulti non più adeguata alle necessità della Struttura stessa

- i Centri, le Scuole e i Dipartimenti possono estendere il cablaggio "orizzontale" in completa autonomia, a proprio carico, purché la modalità sia compatibile con le caratteristiche dell'infrastruttura di rete; in questo caso, le Strutture che intendono procedere a nuove realizzazioni o a modifiche delle proprie reti locali sono tenute a presentare preventivamente all'Area ICT il progetto, redatto da un professionista abilitato, delle opere che intendono realizzare, fornendo le caratteristiche degli apparati e l'opportuna documentazione aggiuntiva, completa delle specifiche metriche dell'impianto;

su richiesta della Struttura o su proposta dell'Area ICT, il rifacimento e/o l'aggiornamento del cablaggio può essere realizzato a cura e spese dell'Ateneo attraverso l'Area ICT, nel rispetto della propria pianificazione e programmazione temporale oppure a cura e spese della Struttura, con le modalità sopra descritte. Potrà essere prevista una suddivisione della spesa. Gli interventi sono effettuati rispettando le seguenti modalità:

a) la Struttura che intende richiedere all'Amministrazione l'esecuzione di opere di cui al punto 2, deve inviare una circostanziata richiesta indirizzata al Pro-Rettore per gli aspetti informatici;
b) le priorità degli interventi sono definite dal Pro-Rettore per gli aspetti informatici, sentita la Commissione ICT;
c) gli aggiornamenti o ampliamenti devono tenere conto dello stato dell'arte della tecnologia delle reti;
d) l'Ateneo assegna annualmente all'Area ICT, che ne potrà disporre con piena autonomia, uno specifico budget per piccoli interventi di estrema urgenza;
e) gli interventi di manutenzione straordinaria e le nuove esecuzione di non modesta entità, devono essere pianificati e programmati in sede di bilancio di previsione (periodo settembre – dicembre);
f) rispetto ai progetti presentati dalle Strutture, l'Area ICT fornisce un parere tecnico scritto vincolante, indicando anche l'eventuale partecipazione finanziaria da parte dell'Ateneo;
g) la Struttura può anticipare la quota di finanziamento di competenza del Bilancio Universitario, previa approvazione scritta di quest'ultima, oppure sostenere interamente la spesa a titolo definitivo;
h) ai fini dell'ammissibilità del progetto, gli apparati di rete da installare a cura delle Strutture devono essere conformi agli standard di gestione remota ed accessibili in remoto, in caso di necessità, anche dai tecnici dell'Area ICT.
i) al termine di ogni modifica di una rete locale di struttura, il Responsabile della Struttura deve consegnare all'Area ICT copia della documentazione comprensiva di:

- certificazione del cablaggio in base alla normativa nazionale ed internazionale vigente;
- parametri di configurazione degli apparati installati;
- eventuali password non privilegiate delle apparecchiature di rete installate, che permettano il monitoraggio in caso di problemi ed emergenze;
- pianta aggiornata che riporti la topologia fisica e logica della rete locale della struttura.

  In assenza di suddetti elementi, l'Area ICT non configurerà, nei nodi delle dorsali di rete di Ateneo, alcuna connessione con gli apparati di rete della Struttura oggetto della modifica; la rete di struttura rimarrà quindi non connessa alla rete di Ateneo;

j) nel caso in cui l'impianto in oggetto risultasse già collegato alla rete di Ateneo, pur non avendone i requisiti, l'Area ICT non fornirà alcun tipo di supporto e si riserva la facoltà di disconnettere la porzione d'impianto, eventualmente anche senza preavviso, in caso essa possa pregiudicare il funzionamento o la sicurezza della rete Genuanet;
k) la gestione dell'infrastruttura di Rete è attribuita alla Struttura finale e sarà da essa condotta avvalendosi dei referenti tecnici informatici della Struttura, funzionalmente dipendenti dall'Area ICT (come da atto organizzativo in vigore dal 1/1/2024), oppure affidando le attività a un manutentore esterno che può intervenire interfacciandosi e concordando le modalità di gestione con l'Area ICT.

Regole per la configurazione delle postazioni di lavoro: client e servizi di rete

Nel sistema di reti di Ateneo viene garantito il supporto della famiglia di protocolli TCP/IP.

L'Area ICT definisce il piano di indirizzamento IP e assegna segmenti di indirizzi IP privati (validi per le comunicazioni interne e utilizzabili per l'accesso internet via gateway/proxy) e segmenti di indirizzi IP pubblici, da utilizzare esclusivamente per la pubblicazione di servizi che devono essere consultabili da internet. In questo caso, sarà necessario presentare un progetto di fattibilità da sottoporre all'Area ICT.

Al fine di favorire e semplificare le attività di messa in sicurezza dei servizi erogati in rete, come pure dei dati custoditi sui sistemi ad essa collegati, nel tempo si sono adottate e consolidate nell'uso alcune strategie, avvallate anche dalle good practices diventate di implementazione comune e finalizzate a minimizzare la superficie esposta a potenziali attacchi.

Per tale ragione, si rende necessario:

- Conoscere approfonditamente i servizi di rete pubblicati e i sistemi ad essi collegati;
- Evitare l'esposizione non mediata dei servizi e dei sistemi;
- Consentire l'accesso alle risorse di rete solo alle postazioni/utenze che ne hanno necessità.

Le postazioni di rete vengono configurate secondo la seguente logica di assegnazione indirizzi IP:

- Indirizzi IP privati: 10.186.0.0/16 utilizzati da tutte le strutture per le postazioni aperte al pubblico (biblioteche, laboratori, ecc.), per le postazioni utilizzate solo per la navigazione su Internet attraverso proxy di Ateneo e che non devono accedere alle applicazioni Intranet, in generale per i segmenti classificati "insicuri" o di "servizio"
- Indirizzi IP privati: 10.187.0.0/16 utilizzati da tutte le strutture, per le postazioni accessibili solo al personale, amministrate secondo i criteri definiti dall'Area ICT e che devono poter accedere alle applicazioni Intranet, in generale solo ai segmenti classificati "sicuri"

È essenziale attribuire i range di indirizzi privati assegnati alla Struttura, sulla base della classificazione e della destinazione d'uso, ad esempio:

- Range 10.187.X.0/24 "sicuro" destinato a uffici amministrativi e macchine fisse dei docenti, a seconda del tipo di utilizzo;

- Range 10.186.Y.0/24 “insicuro” destinato ad uso laboratori e macchine fisse dei docenti a seconda del tipo di utilizzo;
- Range 10.186.Z.0/24 “insicuro” destinato ad aule informatiche;
- Range 10.186.X.0/24 “servizio” destinato a servizi di Struttura (es. terminali controllo accessi, sistema CCTV, ecc....)
- Altre casistiche, da concordare con l’Area ICT, in caso di necessità.

È inoltre raccomandato evitare di configurare sulla stessa rete IP dispositivi con destinazioni d’uso diversi (es. PC amministrativi con PC laboratori/aula).

Le Strutture Fondamentali possono pertanto precedere autonomamente all’attribuzione degli indirizzi ad esse preventivamente assegnati dall’Area ICT, attraverso il proprio referente ICT di Struttura o, in mancanza, del tecnico informatico del Presidio di competenza;

Viene di norma assegnato alle Strutture anche un range limitato di indirizzi IP pubblici 130.251.0.0/16, che deve essere utilizzato esclusivamente per le postazioni che forniscono un servizio diretto e censito verso Internet.
E’ infatti necessario, nel caso di impiego d’indirizzamento pubblico, registrare il tipo di servizio che il client eroga verso l’esterno di Genuanet, comunicandolo all’Area ICT (v. paragrafo “Procedura di registrazione server”).

Regole per la registrazione di Applicazioni e servizi sulla rete

Le applicazioni in rete devono, in qualsiasi ambito, rispettare l'RFC 1855 "Netiquette Guide Lines", l'Acceptable Use Policy della rete GARR ed ogni altra legge, norma o regolamento relativo alla particolare rete utilizzata.
Le strutture sono tenute a comunicare all’Area ICT l'eventuale presenza di server il cui uso non è confinato localmente al segmento di rete di appartenenza e a presentare preventivamente un documento che illustri eventuali servizi on-line che intendono realizzare o modificare, completo delle specifiche relative a protocolli, criteri di accesso e autenticazione. Al contempo dovranno essere indicati i referenti responsabili del mantenimento in sicurezza e gestione dello stesso, da contattare in caso di anomalie riscontrate e/o segnalate. In caso di decadenza o avvicendamento di tali referenti è necessario darne comunicazione tempestiva all’Area ICT
Questa comunicazione consente all’Area ICT di adottare, eventualmente, misure mirate a garantire ai servizi priorità nel ripristino, di assegnare maggiore banda per le comunicazioni, prevedere meccanismi di monitoraggio, protezione e prevenzione, di differenziare le politiche di accesso a e da tali servizi.

Regole Generali Rete Wireless

L’intero Ateneo è coperto dall’infrastruttura di rete wi-fi gestita dall’Area ICT, che eroga i servizi Eduroam e GenuaWiFI.

Le reti wireless per loro natura non sono confinate e localizzate precisamente e rendono più difficile l'individuazione fisica dell'origine del traffico generato, per cui occorre porre particolare attenzione ai criteri con cui esse vengono realizzate affinché si armonizzino nella gestione con le reti cablate

In generale non è ammesso l'utilizzo di dispositivi wireless di tipo indipendente (stand-alone) per estendere la rete cablata autonomamente. Nel caso in cui la Struttura decida di installare un proprio sistema wireless, l'implementazione deve quindi essere di tipo infrastrutturale, garantire standard implementativi di livello almeno pari a quello realizzato per GenuaWIFI e il progetto deve essere validato dall'Area ICT per i rischi e gli eventuali impatti sulla sicurezza della rete GenuaNET nel suo complesso

In questo caso, l'attività è soggetta alle seguenti norme:

• per l'installazione di un access-point wireless è richiesta la presentazione preventiva di un progetto operativo all'Area ICT: il parere favorevole di quest'ultima è vincolante per il collegamento alla Rete;

• il processo di identificazione, autenticazione e accesso, compresa la conservazione a norma di legge dei dati relativi, è a carico della Struttura;

• devono essere rimossi, o adeguatamente riconfigurati a cura della struttura, gli access point non autorizzati o comunque configurati in modo improprio.

In caso contrario, l'Area ICT si riserva la facoltà di disconnettere le porzioni di infrastruttura non conformi a quanto sopra.

Procedura per autorizzazione presenza AP wireless, non appartenenti all'infrastruttura dell'Area ICT, nelle sedi dell'Università di Genova

Il Decreto del 16 agosto 2005 (G.U. N.190 del 17/8/2005) richiede all'Università di consentire l'uso delle reti wireless a dipendenti, studenti e coloro che in modo occasionale possono utilizzare la connessione ad Internet solo previa autenticazione con credenziali personali. La connessione, attraverso un qualsiasi media trasmissivo di un access point wireless, alla Rete costituisce un ampliamento della rete informatica che sottostà al presente regolamento. È pertanto necessario che la struttura interessata all'attivazione o al mantenimento in funzione di un qualsiasi AP wireless, anche se non esplicitamente connesso alla Rete dati, invii preventivamente all'Area ICT una richiesta sottoscritta dal responsabile, analogamente alla procedura seguita per le reti cablate.

Sono inoltre richieste le seguenti misure minime:

1. Devono essere operative tutte le misure necessarie per l'autenticazione dell'utente con credenziali personali e la memorizzazione degli accessi (log) secondo le modalità di legge.
2. Devono essere attribuiti indirizzi IP privati e deve essere consentita la navigazione solo attraverso proxy.
3. La navigazione su Internet deve essere consentita solo previa accettazione di liberatoria da parte dell'utente per il salvataggio dei log del proxy, sottoposti a trattamento dati in conformità con il GDPR.
4. Access Point e postazioni wireless devono costituire una rete separata (fisica o virtuale) del comprensorio/campus rispetto alle LAN di struttura.
5. Gli Access Point ad accesso libero che non richiedono alcuna forma di autenticazione da parte dell'utente devono essere adeguatamente riconfigurati a cura della struttura o rimossi.

6. Non è necessario che la comunicazione via etere venga criptata, purché l'utente venga messo a conoscenza dei rischi nel caso di utilizzo di protocolli insicuri attraverso un'informativa.

L'Area ICT effettua periodicamente il monitoraggio proattivo delle reti wireless. Gli AP che causano interferenze e gli AP non autorizzati potranno essere rimossi, previa comunicazione ai responsabili di Struttura.

Utilizzo infrastruttura wireless EDUROAM e GenuaWiFI

Eduroam (Education Roaming) è la rete wireless prioritaria dell'Ateneo che ha come scopo principale quello di fornire la connettività radio nei punti di aggregazione studentesca più significativi e in tutte le aule.

Gli utenti di un'istituzione aderente a EduRoam, come l'Università di Genova, che visitano un altro istituto aderente sono in grado di utilizzarne la rete locale wireless (WLAN) usando le stesse credenziali (nome utente e password) che userebbero nella propria istituzione d'appartenenza, senza la necessità di ulteriori formalità presso l'istituto ospitante.

Per accedere a Eduroam è preferibile seguire la procedura di configurazione guidata, disponibile alla pagina seguente:

http://ict.unige.it/wi-fi-istruzioniconfigurazione

La rete locale GenuaWifi è pensata per quegli utenti che utilizzano raramente la rete wireless di Ateneo e per gli ospiti che non dispongono di credenziali Eduroam.

Per la configurazione si può fare riferimento alla pagina seguente:

http://ict.unige.it/wifi-istruzioniconfigurazione#configurazione

Per richiesta assistenza, suggerimenti o chiarimenti, è possibile inviare una mail al seguente indirizzo:

helpwifi@unige.it

Sono presenti risposte alle domande più frequenti, al seguente URL:

https://ict.unige.it/wifi-faq

Regole Generali Telefonia di Ateneo

Il Sistema Telefonico di Ateneo è gestito internamente dall'Area ICT, che provvede ad assegnare, modificare e rimuovere utenze.

Allo stato attuale le utenze attive sono circa 6000, a cui vengono sommati i servizi IVR (acronimo di Risposte Vocali Interattive).

All'interno delle Strutture e dei Centri, sono presenti tecnologie miste, per il collegamento telefonico: possono essere di tipo VOIP (apparecchi connessi alla rete dati a cui è possibile collegare "in serie" una postazione PC), oppure di tipo analogico (apparecchi che sfruttano l'impianto tradizionale a doppino).

Una Struttura che ha intenzione di richiedere una nuova linea telefonica e/o un eventuale apparecchio, può inoltrare istanza scritta all'indirizzo retifonia@unige.it

Tale richiesta può essere effettuata dalle seguenti figure di riferimento:

- Dirigente dell'Area o Caposervizio in caso di richiesta proveniente da un'Area dell'Amministrazione Centrale.
- Direttore di Scuola/Dipartimento, Responsabile Amministrativo di Scuola/Dipartimento o Coordinatore Tecnico in caso di richiesta proveniente dalle Strutture Fondamentali;

Premesso che gli apparecchi telefonici VoIP non devono mai essere scollegati, **eventuali apparecchi non più utilizzati devono essere tempestivamente restituiti all'Area ICT,** che provvederà all'eventuale riassegnazione.
In caso di richiesta di assegnazione di una nuova linea collegata ad un nuovo telefono VoIP, da parte di una Struttura, l'Area ICT effettuerà un monitoraggio presso la stessa Struttura per rilevare eventuali apparecchi scollegati dalla rete. Ne verificherà l'eventuale inutilizzo presso la Struttura stessa, invitandola a rinnovarne l'impiego in caso di necessità.

La modalità d'uso delle linee è descritta al seguente URL:

https://ict.unige.it/telefonia#toc-modalit-du-lVQ6E4lz

Gli apparecchi telefonici VOIP sono, a tutti gli effetti, dispositivi di rete del costo commerciale superiore a 100 € e rientrano nella casistica evidenziata nel precedente paragrafo delle Disposizioni Generali; pertanto, l'utente che ne entra in possesso è tenuto a compilare il modulo presente alla pagina seguente:

https://ict.unige.it/telefonia

sotto la voce:

Modulo di assegnazione apparecchio telefonico VoIP (personale in possesso di credenziali Office 365 UNIGE attive).

L'utente diventa a tutti gli effetti responsabile dell'apparecchio affidato ed è tenuto a comunicare all'Area ICT, attraverso l'indirizzo e-mail retifonia@unige.it , eventuali necessità di spostamento dell'apparecchio, che potrà rimanere assegnato, anche in caso di trasferimento ad altro ufficio, anche di Strutture diverse.

In caso di smarrimento o furto, l'assegnatario provvederà ad effettuare regolare denuncia alle Forze dell'Ordine e a far pervenire a retifonia@unige.it copia della stessa.

Manutenzione delle postazioni telefoniche

In analogia con quanto definito per la rete dati, la manutenzione dell'infrastruttura telefonica è a carico dell'Area ICT nella distribuzione verticale ai piani degli edifici.

In caso di realizzazione nuove postazioni di lavoro e di ripristino guasti nell'infrastruttura "orizzontale", la Struttura ha piena autonomia di intervento.

Può rivolgersi ad imprese specializzate, che possano realizzare ed intervenire sul cablaggio, certificandone la qualità dell'impianto.

Procedura per la segnalazione guasti telefonici e richieste generiche sulla telefonia

La manutenzione degli apparecchi che presentano problemi, è affidata alla Società con cui l'Ateneo ha stipulato l'accordo quadro.

È possibile aprire una chiamata, utilizzando l'apposito numero verde dedicato; tutto il personale può chiamare il numero verde, in caso di necessità.

Tutte le indicazioni sono fornite alla seguente pagina:

https://ict.unige.it/segnalazioneguastitelefonici

Per tutte le altre richieste di ordine generico (attivazione nuova linea, richieste di attivazione deviazione, dismissione telefono, ecc....), è possibile rivolgersi all'indirizzo:

retifonia@unige.it

Tali richieste possono essere avanzate da Direttori di Struttura, Responsabili amministrativi, Referenti di Edificio.

E' possibile richiede deviazioni di chiamata da linea telefonica fissa, verso altra linea esterna, purché la richiesta rientri nelle casistiche riportate al seguente URL:

https://ict.unige.it/info-deviazioni

Nell'ottica di una razionalizzazione e valorizzazione delle risorse e delle attrezzature messe a disposizione dall'Ateneo nonché di una riduzione della spesa in materia di telefonia fissa e mobile, si richiamano di seguito alcune informazioni e alcune richieste.

- Le chiamate da interno fisso ad interno fisso (senza deviazione verso numeri esterni) non generano costi;
- Le chiamate da interno fisso a numero esterno generano un costo a consumo che varia se la destinazione è urbana, nazionale, cellulare, internazionale;
- Le chiamate da interno fisso ad interno fisso con deviazione su cellulare generano un costo a consumo come in 2);
- Le chiamate fra cellulari di servizio appartenenti allo stesso contratto sono comprese nel canone (Amministrazione centrale e Strutture fondamentali hanno contratti differenti); in ogni caso nel canone mensile sono compresi anche dei minuti di conversazione a pagamento;
- Le chiamate vocali attraverso Teams non generano costi.

Per quanto sopra siamo tutti invitati a chiamare le persone non presenti alla propria postazione di lavoro (cioè in prossimità dell'apparecchio telefonico fisso) attraverso Microsoft Teams che si raccomanda di attivare in orario di lavoro, oppure, se non è possibile usare Teams, usando il cellulare di servizio chiamando altro cellulare di servizio.

Regole per l'accesso alla Rete GenuaNET dall'esterno

L'Ateneo, tramite l'Area ICT, mette a disposizione del personale docente, tecnico-amministrativo nonché degli studenti strumenti e modalità per l'accesso ai servizi di Ateneo dall'esterno della Rete UNIGE.
Uno degli strumenti per realizzare una connessione sicura da qualsiasi punto della rete internet verso l'interno della rete universitaria è la VPN (Virtual Private Network) con fattori multipli di autenticazione: con questo strumento si ha la possibilità di accedere alle risorse informatiche

dell'Università da una sottorete classificata per tale scopo e appropriatamente monitorata e controllata mediante policy di sicurezza.

Qualora una Struttura intenda intraprendere soluzioni autonome di fornitura di accesso remoto, il responsabile della stessa deve darne preventiva comunicazione scritta all'Area ICT, garantendo l'adozione di tutte le misure atte a prevenire intrusioni e/o utilizzi illeciti e a conservare a norma di legge i dati relativi alle connessioni, sempre in conformità con le AUP di GARR e presentando un progetto che deve essere validato dall'Area ICT per i rischi e gli eventuali impatti sulla sicurezza della rete GenuaNET nel suo complesso.
L'utilizzo della VPN è la soluzione prioritaria anche per consentire le connessioni di entità terze (ditte ed Enti che collaborano a vario titolo con l'Ateneo), verso GenuaNet.
Non è consentito utilizzare i software per l'accesso e il controllo remoto delle postazioni (es. Anydesk, Teamviewer, Supremo, ecc...), che compromettono la sicurezza dell'infrastruttura, "bypassando" le difese perimetrali della rete Genuanet.
Eventualmente, le entità terze possono essere fornite di credenziali ad hoc per l'utilizzo della VPN UNIGE, previa comunicazione all'Area ICT attraverso i comuni canali.
Tali credenziali saranno nominative, per un utilizzo non continuativo e di scadenza concordata.

Le informazioni generali, relative all'utilizzo della VPN sono riportate al link:

https://ict.unige.it/accesso-vpn

Il software da utilizzare è FORTICLIENT VPN, che consente di instaurare una connessione diretta alla Rete possid'Ateneo, impiegando le proprie credenziali UNIGEPass.

Tutte le indicazioni per installare il software necessario, sono reperibili al seguente URL:

https://ict.unige.it/istruzioni-vpn

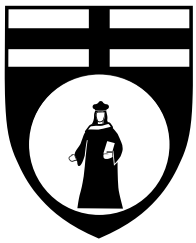
In caso di necessità, come per la parte wi-fi, viene di seguito riportato il link da cui consultare risposte alle domande più frequenti:

https://ict.unige.it/faq-vpn

Per ogni altro chiarimento, non rientrante nella casistica, è possibile scrivere una e-mail all'indirizzo:

assistenza@unige.it

Qualunque necessità non prevista dalle presenti linee guida, deve essere esposta e discussa preventivamente con l'Area ICT, attraverso i canali già definiti sopra.



Università
di Genova

Linea Guida ICT

Utilizzo dei client

Versione	Autori
Ottobre 2024	Paolo Moresco (Area ICT) Stefano Orocchi (Area ICT) Massimo Di Spigno (Area ICT)

Sommario

Introduzione

L'Università degli Studi di Genova, a cui ci si riferisce in seguito come Unige, o Ateneo, nell'espletamento della sua attività istituzionale opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

Il presente documento definisce le regole e le condizioni per l'utilizzo degli strumenti informatici dell'Ateneo da parte dei dipendenti, degli studenti e di tutti coloro che, in virtù di un rapporto di lavoro, di studio, o di ricerca, a qualsiasi titolo (collaboratori, consulenti, stagisti, fornitori, studenti esterni, etc.), utilizzano strumenti informatici dell'Ateneo, nel seguito denominati Utenti.

Il presente documento deve considerarsi integrato da tutte le procedure interne adottate per argomenti specifici e casistiche, così come pubblicati sul sito dell'Ateneo e più specificatamente dell'Area ICT.

Finalità del documento

Il presente documento è da considerarsi approfondimento delle "*Linee guida per la sicurezza e l'utilizzo delle risorse informatiche dell'Ateneo*". Definisce e detta agli Utenti specifiche regole e condizioni di utilizzo dei dispositivi aziendali attraverso:

- definizione di regole e procedure uniformi da applicarsi in tutte le aree operative;
- indicazione delle procedure operative per l'accesso alle risorse aziendali tramite l'utilizzo dei dispositivi (client) aziendali da parte degli utenti
- indicazione delle procedure operative per l'accesso alle risorse aziendali tramite l'utilizzo di dispositivi (client) non aziendali da parte degli utenti
- indicazione delle principali disposizioni normative in materia di utilizzo dei sistemi informativi e di protezione dei dati personali;
- definizione dell'ambito, delle modalità e dei limiti del monitoraggio e dei controlli attuabili dall'Ateneo nel rispetto della normativa vigente nonché delle regole e delle procedure interne.

Contesto normativo e regolamentare

Il presente regolamento è redatto sulla base dei seguenti e principali riferimenti normativi:

- Codice penale, con particolare riferimento ai reati informatici;
- L. 300/1970 (Statuto dei lavoratori) - artt. 4, 7 e 8 e successive modificazioni;
- D. Lgs. 196/2003 e s.m.i(Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per posta elettronica e Internet" di cui alla deliberazione 13/2007;
- D. Lgs. 81/2008 e s.m.i (Testo Unico sulla sicurezza);

- D.P.R 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione) e Codice di comportamento Unige;
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR)
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1417809
- REGOLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
- DECRETO LEGISLATIVO 4 settembre 2024, n. 134 (recepimento NIS 2) - Attuazione della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio. (24G00150) (GU Serie Generale n.223 del 23-09-2024)
- Piano Implementativo Strategia Nazionale Cybersicurezza 2022-2026
- Piano Triennale per l'informatica nella PA

GLOSSARIO E DEFINIZIONI

Ai fini del presente documento si intende per:

- Amministratori di sistema: figure professionali finalizzate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009;
- Applicazioni aziendali: si considerano applicazioni aziendali:
    - Prodotti/programmi acquistati dall'Ateneo, di valenza generale, o settoriale ed in quest'ultimo caso approvati dall'Area ICT;
    - Applicazioni e servizi sviluppati ad hoc dell'Area ICT, da terze parti ma sotto il coordinamento dell'Area ICT, ovvero da altre strutture con un processo di partecipazione e approvazione da parte dell'Area ICT e che seguono le regole di gestione previste nei casi precedenti;
    - Applicazioni esterne che l'Ateneo utilizza secondo le regole di gestione e di sicurezza delle medesime a titolo di mero esempio possono essere la piattaforma NoiPA, abbonamenti a servizi informativi, portale ANAC, etc.
- Aziendali: nel corso del documento si farà spesso riferimento a risorse o dispositivi come "aziendali". Pur nella consapevolezza che l'Ateneo non è un'azienda, tale dicitura identifica più chiaramente l'organizzazione nella letteratura tecnica.
- Dispositivi o endpoint: qualunque dispositivo atto a connettersi alla rete Unige, ai suoi dati, alle applicazioni aziendali, alle risorse in genere.
- Dispositivi aziendali: dispositivi di proprietà o comunque nelle disponibilità dell'Università degli studi di Genova e messi nelle disponibilità degli utenti.
- File di log: registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato;
- GENUAnet: rete informatica gestita direttamente dall'Università di Genova divisa in rete cablata e rete WiFi eduRoam (già GenuaWiFi);
- Strumenti informatici: personal computer fissi o portatili o virtuali, stampanti locali o di rete, programmi e prodotti software in-house o in-cloud, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc);
- Utenti: personale dipendente, docenti, studenti, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni e coloro che, in virtù di un rapporto di lavoro, di studio o di collaborazione in essere a qualsiasi titolo con l'Ateneo, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione da Unige.

PRINCIPI GENERALI

Gli strumenti informatici sono assegnati agli Utenti per lo svolgimento dell'attività e devono essere utilizzati con modalità e mediante comportamenti adeguati al ruolo, ai compiti assegnati e alle responsabilità connesse, nel rispetto del Codice di comportamento dei dipendenti della pubblica amministrazione e delle normative e direttive interne e delle leggi.

Nell'esecuzione della propria attività, gli Utenti sono tenuti ad attenersi alle seguenti istruzioni generali:

a. effettuare la propria attività uniformandosi alle disposizioni dell'Ateneo e alle istruzioni ricevute;
b. custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente alle strutture preposte, secondo le modalità previste, ogni danneggiamento, smarrimento o furto;
c. mantenere la riservatezza sulle informazioni e sui dati personali di cui siano venuti a conoscenza durante lo svolgimento della propria attività;
d. in caso di cessazione dal servizio, dalla prestazione o dal rapporto con l'Ateneo, astenersi dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività, in funzione della natura di riservatezza del dato;
e. adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati;
f. garantire la corretta custodia di atti e documenti adottati da Unige.

Regole per l'utilizzo dei dispositivi informatici in Ateneo

Dispositivi aziendali e personali

Vengono considerati aziendali tutti quei dispositivi di proprietà o comunque nelle disponibilità dell'Università degli studi di Genova e messi nelle disponibilità degli utenti. Al di fuori di questi, sono invece considerati personali i dispositivi di proprietà o comunque nelle disponibilità degli utenti.

L'Università degli Studi di Genova gestisce l'intero ciclo di vita dei dispositivi aziendali.

L'Università degli Studi di Genova gestisce l'accesso e il ciclo di vita delle risorse messe a disposizione degli utenti e accedute tramite dispositivi sia aziendali che personali.

Utilizzo di dispositivi aziendali

I dispositivi aziendali vengono preparati e gestiti da, per conto, con l'assenso dell'Area ICT secondo regole che evolvono con il progredire delle tecnologie e delle minacce informatiche. Ne è vietato qualunque utilizzo che danneggi le risorse aziendali (il dispositivo stesso, il software, i dati, etc.), o che sia di minaccia per la sicurezza. È consentito l'uso promiscuo, sia lavorativo, sia personale, del dispositivo, purché non contraddica alcuna altra regola del presente documento, o dell'Ateneo.

Il dispositivo è provvisto di software di sicurezza (es. antivirus, firewall, impostazioni di aggiornamento) e le configurazioni disposte o raccomandate seguono regole come descritte nel presente documento e in altre istruzioni opportunamente fornite dall'Area ICT.

Nei casi in cui l'Utente, o comunque altro personale opportunamente delegato, dispongano di diritti amministrativi sul dispositivo, dovranno assicurarsi in prima persona della corretta configurazione e mantenimento del dispositivo ed evitare comportamenti diversi dalle raccomandazioni.

Nei casi in cui l'utente, o comunque altro personale opportunamente delegato, abbiano autonomia di installazione/utilizzo di applicazioni, anche senza diritti amministrativi, dovranno assicurarsi in prima persona della corretta configurazione e mantenimento di esse ed evitare comportamenti diversi dalle raccomandazioni.

In caso di dubbio sul comportamento da seguire (es. l'installazione di un programma non aziendale), l'utente, o comunque altro personale opportunamente delegato, dovranno consultare il personale tecnico di riferimento prima di procedere.

L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni, il ritiro del dispositivo affidato, o anche procedure legali ove necessario.

Tra i dispositivi aziendali rientrano anche i dispositivi e le risorse virtuali. Le regole di cui al presente documento valgono anche per essi per quanto applicabile.

L'accesso ai dispositivi aziendali è legato al ruolo dell'utente in Ateneo. Al modificarsi, o al termine del ruolo dell'utente in Ateneo, la disponibilità dei dispositivi aziendali può cessare o andarsi a modificare. L'utente è tenuto a informarsi dei corretti criteri di detenzione e restituzione dei dispositivi in affidamento.

Installazione e configurazione dei dispositivi aziendali

I dispositivi aziendali possono essere installati e configurati in maniera manuale o, più facilmente, automatizzata da parte o per conto del personale dell'Area ICT, in collaborazione con essi, o anche in maniera autonoma da parte dell'utente.

L'Area ICT mette a disposizione meccanismi automatici che facilitano l'installazione e configurazione dei dispositivi, permettendone la gestione automatizzata del ciclo di vita, della gestione dell'allestimento, della sicurezza.

L'Area ICT provvede a indicare le procedure più corrette nei vari casi, tenendo conto delle necessità di operatività degli utenti, delle necessità delle strutture di appartenenza, della fattibilità nei casi specifici, dei tempi e dei modi più appropriati.

I dispositivi aziendali vengono connessi alle risorse aziendali tramite un meccanismo detto di "join". Detto meccanismo permette gestione e monitoraggio continuo da parte degli amministratori di sistema, centrali o locali, nonché l'automazione del supporto e della messa a disposizione delle risorse agli utenti.

Le procedure di Join dei dispositivi sono possibili sia per gli amministratori, centrali o locali, sia per gli Utenti e sono descritte nelle istruzioni operative nelle pagine del sito dell'Università di Genova, più specificatamente nelle pagine dell'Area ICT.

I dispositivi joined permettono a qualunque utente dell'Ateneo di accedere localmente ottenendo un ambiente di lavoro isolato da quello di altri utenti. Documenti, impostazioni personali, password memorizzate, sono locali all'utente specifico e non sono accessibili da altri utenti del dispositivo.

Una volta connessi alla rete aziendale, i dispositivi joined ricevono configurazioni, applicazioni e dati direttamente dal sistema centrale, così come predisposto dagli amministratori centrali e locali, in preparazione delle necessità degli utenti a cui essi sono destinati. Eventuali configurazioni aggiuntive o personalizzazioni necessarie allo svolgimento della propria attività possono essere richieste al personale di supporto.

Il modello di gestione dei dispositivi varia a seconda della struttura di afferenza e delle necessità operative specifiche. I dispositivi possono essere allestiti con differenti applicazioni, impostazioni di sicurezza, vincoli di accesso, etc. Come esempio, un portatile destinato ad attività di ricerca può necessitare che l'utente abbia massima autonomia e diritti amministrativi per l'installazione di applicazioni, un terminale di una portineria può prevedere un allestimento "Office" standard con diritti limitati agli utenti, un computer di un'aula informatica può necessitare di una configurazione completamente customizzata con diritti molto elaborati per gli utenti.

La modalità di allestimento e gestione viene decisa dal personale dell'Area ICT, in collaborazione con gli amministratori locali eventualmente presenti, sentite le esigenze specifiche del personale e delle strutture di riferimento, nell'ottica del migliore equilibrio tra tutte le esigenze in gioco.

Gli utenti devono riferirsi al personale di supporto informatico per indicazioni sulla corretta procedura da utilizzare e sulla specifica modalità e grado di autonomia nelle operazioni che riguardano i dispositivi a loro affidati.

Accesso ai dispositivi aziendali

L'accesso ai dispositivi di Ateneo avviene attraverso credenziali di autenticazione centralizzate fornite e gestite dall'Area ICT (es. credenziali di dominio, credenziali Cloud). L'accesso a particolari dispositivi, servizi o applicazioni (es. in alcuni laboratori, oppure su aule virtuali) può avvenire tramite credenziali locali in accordo con l'Area ICT.

I dettagli dei requisiti per l'accesso alle credenziali di autenticazione e il loro corretto utilizzo sono disponibili sulle pagine del web di ateneo e più specificatamente nelle pagine dell'Area ICT.

Una volta eseguito l'accesso al dispositivo aziendale, l'utente ottiene l'accesso ai dati e alle applicazioni nelle sue disponibilità in maniera automatica o comunque agevolata, tramite un meccanismo di single sign-on.

La richiesta di autenticazione durante l'utilizzo dei dispositivi viene minimizzata tramite meccanismi di caching sicuro. Attività di particolare delicatezza (es. cambio password), oppure in situazioni specifiche (accesso da rete inusuale) possono richiedere all'utente una conferma dell'autenticazione rafforzata, ad esempio tramite l'utilizzo di un authenticator o di un codice di verifica.

Installazione di applicazioni sui dispositivi aziendali

I dispositivi aziendali possono essere "assegnati" a un utente, oppure "condivisi".

Un dispositivo assegnato permette all'utente assegnatario di svolgere operazioni di configurazione del software in maggiore autonomia rispetto ad altri utenti, pur in assenza di diritti amministrativi. Sono solitamente assegnati a utenti specifici i computer degli uffici. Nei casi in cui oltre all'assegnazione sia prevista l'attribuzione di diritti amministrativi agli utenti, tali utenti sono ritenuti corresponsabili della gestione del dispositivo nella misura dei diritti in loro possesso.

Un dispositivo condiviso permette l'accesso ottimizzato da parte di più utenti senza che alcuno di essi ne abbia una specifica attribuzione e diritti di amministrazione. Sono solitamente di questo tipo i computer delle aule didattiche e degli uffici ad alto avvicendamento di personale. La gestione del dispositivo è solitamente a carico dello staff dell'Area ICT o di personale da essi delegato.

Le applicazioni possono essere messe a disposizione degli utenti tramite:

- installazione automatica sul dispositivo, da o per conto degli amministratori dell'Area ICT
- installazione disponibile sul dispositivo, tramite gli store di applicazioni indicati, da o per conto degli amministratori delle configurazioni dell'Area ICT
- installazione disponibile all'utente, tramite gli store di applicazioni indicati, da o per conto degli amministratori delle configurazioni dell'Area ICT

- installazione autonoma da parte dell'utente, nel caso in cui egli sia stato reso amministratore del dispositivo, oppure nel caso di applicazioni legate al solo profilo dell'utente.

Eventuali necessità di adeguamento del set di applicazioni a disposizione, o discrepanze rispetto alle configurazioni attese vanno segnalate al personale di supporto informatico di riferimento perché venga valutata una correzione.

In ogni caso, l'accesso alle applicazioni e alle risorse aziendali segue le stesse regole e raccomandazioni per quanto concerne la sicurezza e le modalità di accesso e utilizzo.

Qualora l'utente venga reso autonomo nell'amministrazione del dispositivo, egli è corresponsabile della corretta gestione di esso e della sua rispondenza ai regolamenti e alle indicazioni dell'Area ICT nella misura dei diritti a sua disposizione.

Gestione e monitoraggio dei dispositivi aziendali

I dispositivi aziendali vengono gestiti e monitorati centralmente dall'Area ICT tramite strumenti che permettono l'analisi continuativa dello loro stato di funzionamento. La gestione e il monitoraggio possono essere delegati a personale operante per conto dell'Area ICT (es. referenti tecnici informatici, operatori economici esterni, referenti di laboratorio) per competenza.

I dispositivi vengono monitorati in diversi aspetti, tra i quali:

g. accesso alla rete e alle risorse aziendali
h. conformità delle configurazioni di sicurezza,
i. conformità dell'allestimento hardware e software,
j. eventi di malfunzionamento,
k. violazioni di sicurezza

Qualora ne ravveda la necessità, oppure su richiesta degli utenti, il personale dell'Area ICT o da esso incaricato può intervenire in presenza o da remoto per verificare, modificare, correggere l'impostazione del dispositivo.

Il personale dell'Area ICT o da esso incaricato ha cura di avvisare gli utenti interessati quando l'intervento preveda un impatto sul normale svolgimento del lavoro sul dispositivo, oppure richieda la collaborazione dell'utente. L'intervento viene pianificato con l'ottica della migliore mediazione possibile tra urgenza, sicurezza, fattibilità, costo, impatto sull'attività. Vengono privilegiati interventi trasparenti agli utenti, da remoto, a minimo impatto. Quando questo non sia possibile o conveniente, viene chiesto il coinvolgimento dell'utente che è tenuto alla massima collaborazione e osservanza delle indicazioni fornite.

Gestione dell'impatto energetico

La configurazione dei dispositivi aziendali tiene conto dell'impatto sull'ambiente di un allestimento estremamente vasto e articolato. L'Ateneo utilizza una molteplicità di dispositivi di diversa natura, generazione, finalità, quindi con necessità di impiego estremamente diversificate.

L'Area ICT progetta l'allestimento dei sistemi informatici tenendo conto di una molteplicità di problematiche, tra le quali quelle tecniche, di produzione, gestionali, economiche, energetiche.

Tramite l'impiego delle tecnologie e delle risorse a disposizione, l'Area ICT impiega e raccomanda le corrette tecnologie, impostazioni e procedure per minimizzare il carbon footprint, pur mantenendo efficienti i sistemi di monitoraggio della sicurezza e minimizzando l'impatto sull'attività dell'utente.

L'Area ICT sottolinea tra l'altro la necessità di dotarsi di attrezzature moderne, energeticamente ottimizzate, tramite la sostituzione pianificata e continuativa dei dispositivi più datati con altri di nuova generazione.

Utilizzo di dispositivi non aziendali

L'accesso alle risorse aziendali può avvenire tramite dispositivi diversi da quelli aziendali, ad esempio di proprietà o nelle disponibilità dell'utente, oppure di accesso pubblico. Le norme comportamentali per l'utente restano invariate. L'utente si fa responsabile in prima persona nell'accesso alle risorse aziendali di utilizzare dispositivi sicuri, a norma di legge, secondo il regolamento di Ateneo (es. software installato aggiornato, presenza di antivirus e firewall correttamente funzionanti, nessuna minaccia locale rilevata).

L'accesso a risorse aziendali su dispositivi personali prevede un analogo trattamento in termini di assistenza all'utilizzo, ma che non si estende al dispositivo stesso, a cura invece dell'utente.

L'accesso alle applicazioni aziendali è legato al ruolo dell'utente in Ateneo. Al modificarsi, o al termine del ruolo dell'utente in Ateneo, la disponibilità di accesso alle risorse aziendali può cessare o andarsi a modificare, solitamente in modo automatico. L'utente è tenuto a mantenersi informato dei corretti criteri di accesso ai programmi e delle risorse di cui ha disponibilità e delle ripercussioni sul proprio dispositivo del venire a mancare delle risorse aziendali.

Installazione e configurazione dei dispositivi personali

L'installazione dei dispositivi personali è a carico dell'utente nelle cui disponibilità è posto il dispositivo. In nessun caso può venire richiesto al personale dell'Università di Genova di intervenire in tale fase.

I dispositivi personali possono essere utilizzati per l'accesso alle risorse informatiche dell'Università di Genova da parte degli utenti autorizzati. Perché questo avvenga è richiesto che l'utente allestisca il dispositivo e mantenga conforme alle regole e alle procedure indicate dalle linee guida e dai regolamenti dell'Università di Genova.

Il personale di supporto dell'Area ICT e il personale di supporto locale provvedono a indicare le procedure più corrette per fare si che un dispositivo personale possa essere considerato adeguato a connettersi alle risorse aziendali in sicurezza.

Un dispositivo personale che accede alle risorse informatiche dell'Università di Genova può essere "registrato" tra i dispositivi che accedono all'organizzazione. La procedura di registrazione avviene normalmente durante il primo accesso autenticato dell'utente alle risorse.

In seguito alla registrazione del dispositivo, il dispositivo può essere interrogato dai sistemi di sicurezza informatica di Unige per la verifica automatica delle regole di compliance, a seguito delle quali l'utente ha accesso ai dati e alle applicazioni messe a disposizione

dall'organizzazione. I controlli di compliance possono essere eseguiti automaticamente dai sistemi informatici in maniera periodica, in seguito a particolari eventi, su richiesta degli amministratori. Gli utenti devono riferirsi al personale di supporto informatico per indicazioni sulla corretta procedura da utilizzare e sulla specifica modalità e grado di autonomia nelle operazioni che riguardano l'accesso alle risorse a loro disponibili.

Accesso ai dispositivi personali

Le modalità di accesso ai dispositivi personali dipendono dagli utenti nelle cui disponibilità sono i dispositivi. Solitamente l'accesso al dispositivo avviene tramite un account pubblico, oppure locale, comunque non dell'Università di Genova. In seguito all'accesso al dispositivo, l'utente avente diritto ha facoltà di utilizzare le credenziali dell'Ateneo per l'accesso alle risorse aziendali.

Perché i dispositivi vengano utilizzati per l'accesso alle risorse dell'Università di Genova è però necessario che l'accesso avvenga in maniera sicura, secondo le raccomandazioni del personale dell'Ateneo, i regolamenti e le leggi che governano la materia. I dispositivi devono essere aggiornati, dotati di software di protezione adeguato e manutenuti con procedure regolari e adeguate. I requisiti necessari sono dinamici come dinamica è l'evoluzione delle tecnologie legate alla protezione informatica. Tali requisiti sono documentati sulle pagine dell'Università di Genova e più specificatamente nelle pagine dell'Area ICT.

Qualora i sistemi informatici dell'Ateneo ravvisino il venire a mancare della compliance del dispositivo, l'accesso alle risorse aziendali può essere negato, ai dati, alle applicazioni, a qualunque risorsa nelle disponibilità dell'Ateneo. Gli utenti devono riferirsi al personale di supporto informatico per indicazioni sulla corretta procedura da utilizzare e sulla specifica modalità e grado di autonomia nelle operazioni che riguardano l'accesso alle risorse a loro disponibili.

Installazione di applicazioni sui dispositivi personali

L'Università di Genova mette a disposizione dei suoi utenti le applicazioni aziendali necessarie al corretto svolgimento delle attività lavorative o di didattica. L'accesso alle applicazioni aziendali e il loro utilizzo devono avvenire secondo le regole del presente documento e sulla base del ruolo ricoperto dall'utente e le relative responsabilità e regole ad esse conseguenti.

Il ruolo di un Utente in Ateneo e le attività ad esso legate determinano le autorizzazioni all'accesso alle risorse aziendali. Tali autorizzazioni vengono assegnate dai sistemi informativi con l'applicazione di automatismi e richiedono quindi la costante disponibilità di dati quanto più possibile esatti nei sistemi informativi dell'Ateneo.

L'Area ICT sovrintende ai corretti accesso e utilizzo delle applicazioni e risorse aziendali anche in modo delegato, provvede a dare informazione all'Ateneo dei corretti modi di utilizzo delle risorse informative aziendali, a formare gli Utenti e il personale eventualmente delegato in Ateneo.

L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi

sull'utente possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni, o anche procedure legali ove necessario.

Le applicazioni possono essere messe a disposizione degli utenti tramite:

- installazione disponibile sul dispositivo, tramite gli store di applicazioni indicati, da o per conto degli amministratori delle configurazioni dell'Area ICT
- installazione disponibile all'utente, tramite gli store di applicazioni indicati, da o per conto degli amministratori delle configurazioni dell'Area ICT
- installazione autonoma da parte dell'utente, nelle cui disponibilità è il dispositivo.

Eventuali necessità di adeguamento del set di applicazioni a disposizione, o discrepanze rispetto alle configurazioni attese vanno segnalate al personale di supporto informatico di riferimento perché venga valutata una correzione.

In ogni caso, l'accesso alle applicazioni e alle risorse aziendali segue le stesse regole e raccomandazioni per quanto concerne la sicurezza e le modalità di accesso e utilizzo.

Gestione e monitoraggio dei dispositivi personali

I dispositivi personali non vengono gestiti e monitorati centralmente dall'Area ICT, bensì dall'utente nelle cui disponibilità è il dispositivo.

Le applicazioni aziendali e l'accesso ai dati e alle risorse informatiche in genere messe a disposizione dall'Ateneo vengono monitorate dall'Area ICT tramite strumenti che permettono l'analisi continuativa dello loro stato di funzionamento. La gestione e il monitoraggio possono essere delegati a personale operante per conto dell'Area ICT, come i referenti informatici di zona, per competenza.

Le risorse aziendali accedute vengono monitorate in diversi aspetti, tra i quali:

l. accesso alla rete e alle risorse aziendali
m. conformità delle configurazioni di sicurezza,
n. conformità dell'allestimento hardware e software,
o. eventi di malfunzionamento,
p. violazioni di sicurezza

Qualora ne ravveda la necessità, oppure su richiesta degli utenti, il personale dell'Area ICT o da esso incaricato può intervenire in presenza o da remoto per verificare, modificare, correggere le modalità di funzionamento delle risorse messe a disposizione. Tali interventi sono sempre contestuali alle risorse aziendali e non prevedono un allargamento del supporto al dispositivo personale nella sua interezza o comunque in aspetti non direttamente legati alle risorse dell'organizzazione.

Il personale dell'Area ICT o da esso incaricato ha cura di avvisare gli utenti interessati quando sia necessario un intervento su un dispositivo di un utente che impatti sul normale funzionamento del dispositivo, oppure richieda la collaborazione dell'utente. L'intervento viene pianificato con l'ottica della migliore mediazione possibile tra urgenza, sicurezza, fattibilità, costo, impatto sull'attività. Vengono privilegiati interventi trasparenti agli utenti, automatizzati, a minimo impatto. Quando questo non sia possibile o conveniente, viene chiesto il

coinvolgimento dell'utente che è tenuto alla massima collaborazione e osservanza delle indicazioni fornite.

Configurazioni speciali dei dispositivi

In casi eccezionali può verificarsi la necessità di tenere in esercizio dispositivi che potrebbero violare alcune norme del presente o altri regolamenti. Un esempio può essere dato dal caso di particolari insostituibili attrezzature per l'acquisizione per i quali sussistano problemi tecnici di incompatibilità con i moderni computer. Altro esempio può essere quello della necessità di allestimento di un laboratorio di ricerca che richieda particolari configurazioni di sicurezza.

Questi casi devono essere discussi preventivamente con il personale dell'Area ICT, così da individuare un modello di allestimento che possa permettere l'operatività pur non pregiudicando la sicurezza delle risorse aziendali. Il parere dell'Area ICT in materia è vincolante.

Utilizzo dei dati e delle risorse sui dispositivi

L'archiviazione aziendale dell'ateneo si compone dell'insieme delle capacità di archiviazione on-premise e sul cloud che vanno a comporre complessivamente il sistema di archiviazione di Unige.

Rispetto alla capacità di archiviazione dei dispositivi, l'archiviazione aziendale permette una maggiore sicurezza del dato, resilienza ai guasti e possibilità di monitoraggio da parte degli amministratori di sistema. La legge obbliga l'Ateneo nel suo insieme e ogni suo utente singolarmente a custodire con cura l'informazione di cui è responsabile. Gli strumenti messi a disposizione dall'Ateneo per la gestione documentale personale e di gruppo agevolano questo compito e sono stati individuati come adeguati a tale scopo dall'Area ICT.

I sistemi di archiviazione di Ateneo si compongono di risorse informatiche hardware e software gestite direttamente dall'Area ICT o sotto suo mandato (insieme dei file server on-premise e cloud Sharepoint Online, OneDrive, Titulus, etc.) a cui ci si riferirà come "archiviazione di ateneo".

Il sistema di archiviazione di Ateneo deve essere utilizzato esclusivamente per l'esercizio della propria attività all'interno dell'Ateneo, in funzione del proprio ruolo. È da evitarne l'utilizzo per fini personali (es. documenti personali, foto, filmati).

I sistemi documentali esterni alla gestione dell'Area ICT non devono essere utilizzati per lo svolgimento di attività di Unige, salvo esplicita, motivata e circostanziata autorizzazione da parte dell'Area ICT.

L'archiviazione di Ateneo viene gestita e monitorata dall'Area ICT che si fa carico di indicare agli utenti i modi più consoni al suo utilizzo, nell'interesse dell'Ateneo, dei lavoratori, degli utenti in generale. A tal proposito, si sottolinea la raccomandazione di tenere sincronizzati/depositati/copiati i dati di lavoro su sistemi come OneDrive, Sharepoint, Teams o Titulus, o altri raccomandati dall'Area ICT per preservarli dalla perdita in seguito a guasti ai dispositivi personali.

In caso di comprovata necessità, gli amministratori dei sistemi si fanno carico di accedere ai sistemi di archiviazione per intervenire come necessario (es. rimozione minacce informatiche, litigation hold, etc.). L'attività degli amministratori viene svolta sempre nel rispetto della normativa in materia di tutela della libertà e dignità dei lavoratori e della normativa unionale e nazionale in materia di protezione dei dati personali.

Archiviazione cloud e locale

Il corretto utilizzo degli spazi di archiviazione sul cloud di ateneo permette il recupero del dato in caso di errore anche critico del dispositivo dell'utente, preservando l'informazione che può continuare ad essere disponibile tramite altri dispositivi e permettendo la continuazione dell'attività.

I sistemi di archiviazione dell'Ateneo sul cloud permettono di essere acceduti in modo sicuro dai dispositivi tramite la connessione con protocolli moderni e permettono meccanismi di sincronizzazione, totale o parziale, dei dati sui dispositivi. Il loro impiego permette all'utente una esperienza di utilizzo analoga a quella tradizionale con i vantaggi di sicurezza e resilienza del dato delle moderne tecnologie.

L'utilizzo di tali risorse deve essere ritenuto preferenziale per l'archiviazione finale dei documenti, quando essi siano in uno stato di lavorazione avanzata, o quando necessitino di una stesura collaborativa o di condivisione. Viene deprecato l'utilizzo dell'archiviazione di rete di Ateneo per l'immagazzinamento di bozze iniziali, o archivi di documenti di dubbia utilità.

L'immagazzinamento dei dati sui dispositivi a disposizione dell'utente, siano essi aziendali o personali, non garantisce la corretta salvaguardia delle informazioni.

Supporto alla pianificazione e all'impiego delle risorse di archiviazione

Le modalità di utilizzo dello spazio di archiviazione vengono pianificate dall'Area ICT sulla base di una continua ricerca di equilibrio tra le esigenze operative degli utenti, le necessità di sicurezza e gestione, gli obblighi di legge e la disponibilità di risorse. L'Area ICT fornisce agli utenti e alle strutture indicazioni di indirizzo e regole precise per il corretto impiego delle risorse a disposizione.

Gli utenti possono ottenere assistenza, informazioni e formazione tramite i canali previsti dall'Ateneo per le varie casistiche, così come pubblicato sulle pagine dell'Ateneo e più specificatamente dell'Area ICT. In caso di dubbio sul comportamento da seguire (es. un grosso archivio di dati specifico di una determinata attività), l'utente, o comunque altro personale opportunamente delegato, dovranno consultare il personale dell'Area ICT prima di procedere.

Supporto tecnico

L'Area ICT, attivata dal 1° gennaio 2024, si articola internamente in servizi e settori, come le altre Aree Dirigenziali, in modo da potere rispondere al meglio alle necessità informatiche generali dell'Ateneo.

Per svolgere la propria attività si avvale della collaborazione di referenti tecnici informatici che, seppure incardinati nelle Strutture Fondamentali, dipendono funzionalmente dalla stessa Area ICT (come da Atto Organizzativo dal 1/1/2024), nel contesto informatico. Questa, inoltre, può

avvalersi di aziende e di professionisti esterni a Unige per sopperire all'occorrenza, la carenza di risorse interne. In ogni caso il personale dell'Area ICT resta il referente principale verso l'utente.

Presìdi informatici sul territorio

Come per gli aspetti edilizi e le attività negoziale, anche per le esigenze informatiche la nuova organizzazione ha previsto, per ciascuno dei 5 Poli Territoriali, un supporto informatico costituito al momento da una sola persona. Tale figura, in progressione, potrà costituire un riferimento tecnico per le esigenze del Polo, soprattutto dove il tecnico informatico di Struttura non è presente oppure nelle situazioni in cui occorrono competenze specifiche non presenti localmente. Il referente informatico dell'Area ICT presso il Polo di facility management può intervenire di persona oppure scalare sul competente Servizio/Settore dell'Area ICT che può avvalersi anche di supporti esterni. I presìdi territoriali dell'Area ICT svolgono tra gli altri i seguenti compiti:

- sono interlocutori principali sia per i referenti tecnici informatici in dipendenza funzionale con Area ICT, per i direttori di struttura e per i responsabili amministrativi;
- monitorano e coordinano l'andamento delle attività informatiche congiunte delle strutture con l'Area ICT e suggeriscono interventi evolutivi o correttivi in base alle linee guida, alle normative e alle indicazioni dell'Area ICT;
- costituiscono il secondo livello di assistenza a cui i referenti tecnici informatici, che svolgono assistenza di primo livello, si possono rivolgere.

Amministrazione centrale

Il supporto alle Aree dell'amministrazione centrale è fornito dall'Area ICT con personale del presidio competente o con personale in modo diretto o tramite personale gestito dall'Area ICT.

Strutture Fondamentali

Fatto salvo quanto definito per l'amministrazione centrale, in generale le Strutture Fondamentali sono dotate di almeno un referente tecnico informatico, dipendente funzionalmente dall'Area ICT, i cui compiti sono esplicitati in seguito. Se opportuno, un referente può essere assegnato anche per il servizio di più Strutture o a supporto di postazioni isolate dell'Amministrazione centrale quando logisticamente conveniente.

Nei casi in cui una Struttura non si possa avvalere di un referente tecnico informatico verrà supportata dall'Area ICT, se possibile attraverso il presidio competente, che procederà primariamente a mettere in sicurezza i sistemi informativi. In attesa che si possa disporre di un referente di Struttura, l'Area ICT provvederà in funzione delle risorse interne/esterne disponibili.

In assenza di criteri differenti, i referenti informatici di Struttura vengono individuati su indicazione del direttore della struttura, anche su impulso del coordinatore tecnico dove presente.

Il direttore della struttura nell'ambito delle proprie funzioni:

- è garante, all'interno della propria struttura, dell'applicazione delle misure di sicurezza definite dalla normativa vigente, dalle Linee Guida e dalle prescrizioni dell'Ateneo (Area ICT);
- appronta le misure derivanti dalle scelte politiche, tecnologiche e organizzative definite in Ateneo;
- segnala uno o più referenti informatici per la propria Struttura, in maniera adeguata all'impegno richiesto;
- predispone le condizioni organizzative, logistiche e amministrative affinché i propri collaboratori informatici possano svolgere efficacemente il proprio compito, agevolando la loro formazione e il loro aggiornamento;
- rende note le Linee Guida, la normativa nazionale e le indicazioni ANC (già AGID) agli utenti della propria Struttura e, se necessario, stabilisce ulteriori disposizioni per i servizi con validità interna alla struttura, conformemente ai regolamenti d'Ateneo e a quanto stabilito dalla normativa vigente;
- nel caso di variazioni organizzative, comunica tempestivamente all'Area ICT eventuali variazioni inerenti i referenti informatici;
- rende disponibili in modo pianificato all'Area ICT, tutte le informazioni relative all'organizzazione della gestione dei servizi informatici erogati dalla Struttura, in particolare i riferimenti delle persone con funzioni di amministratore di sistema, reti, database, le modalità di trattamento dei dati dell'organizzazione che competano la Struttura.

Il referente informatico funzionalmente dipendente da Area ICT tra i suoi compiti:

- riferisce al proprio Responsabile di Struttura eventuali attività, in essere o da adottare, per mettere in sicurezza la propria struttura, anche in riferimento a eventuali collaborazioni con l'Area ICT;
- opera secondo le direttive e le procedure stabilite dall'Area ICT. per quanto concerne il corretto uso e funzionamento dei sistemi informativi d'Ateneo, delle infrastrutture tecnologiche e l'implementazione di adeguate misure di sicurezza informatica;
- controlla, sotto il profilo tecnico, ogni Sistema in Rete e i Servizi relativi alle strutture di sua competenza e si riferisce all'Area ICT per ogni violazione o sospetto di violazione della sicurezza informatica e/o alle Linee Guida o ai regolamenti;
- adotta compatibilmente le misure idonee per prevenire l'utilizzo illecito della rete e dei servizi di rete salvaguardando opportunamente le reti locali, i server e le postazioni di lavoro ed effettuando il monitoraggio delle proprie reti locali;
- si interfaccia con l'Area ICT, regolando con essa i flussi di comunicazione con la propria Struttura;
- comunica all'Area ICT tutte le informazioni relative all'infrastruttura e all'architettura dei servizi informatici erogati dalla Struttura;
- risolve tempestivamente gli incidenti di sicurezza dall'Area ICT nei tempi previsti dai Regolamenti GARR e secondo le modalità indicate dall'Area ICT;
- qualora nell'ambito delle ordinarie attività di gestione dei sistemi informativi di competenza, rilevi file illegali o dal contenuto palesemente non istituzionale provvede a darne segnalazione al proprio Responsabile di Struttura.

L'Area ICT partecipa alla formazione degli utenti dell'Ateneo in materia di corretto utilizzo delle risorse informatiche e in particolare i referenti tecnici delle strutture, così da renderli in grado di operare secondo le modalità e le tecnologie messe a disposizione dall'Area ICT.

L’Area ICT monitora il buon funzionamento del supporto informatico presente in ogni Struttura e valuta l’adeguatezza del servizio offerto, anche in collaborazione con le Strutture interessate.

Università di Genova

Linea Guida ICT

Utilizzo degli apparati per la Didattica Digitale Integrata (DDI)

Versione	Autori
Ottobre 2024	Daniele Fabbrini (Area ICT) Paolo Moresco (Area ICT) Laura Guida (Area ICT) Massimo Di Spigno (Area ICT)

Sommario

Introduzione

L'Università degli Studi di Genova, a cui ci si riferisce in seguito come Unige, o Ateneo, nell'espletamento della sua attività istituzionale opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

Il presente documento definisce le regole e le condizioni per l'utilizzo degli strumenti informatici dell'Ateno da parte dei dipendenti, degli studenti e di tutti coloro che, in virtù di un rapporto di lavoro, di studio, o di ricerca, a qualsiasi titolo (collaboratori, consulenti, stagisti, fornitori, studenti esterni, etc.), utilizzano strumenti informatici dell'Ateno, nel seguito denominati Utenti.

Il presente documento deve considerarsi integrato da tutte le procedure interne adottate per argomenti specifici e casistiche, così come pubblicati sul sito dell'Ateneo e più specificatamente dell'Area ICT.

Finalità del documento

Queste linee guida hanno l'obiettivo di indicare **ruoli e procedure** per fruire di tutti gli spazi comuni di Ateneo in uso sia agli studenti che al personale docente e tecnico amministrativo (aule, laboratori, sale conferenze). La modalità ibrida di lavoro in presenza o da remoto è punto centrale della didattica digitale integrata, e a tal proposito è da considerare un obiettivo primario, non solo di singole azioni ma altresì a livello progettuale, che non coinvolge solo le aule, ma anche spazi comuni e modalità di lavoro ordinario. Sono rivolte in particolare a chi ha un ruolo attivo nella progettazione, nella manutenzione, nel funzionamento degli spazi comuni e al corpo docente come agente attivo della didattica. Verranno valutate eventuali proposte migliorative anche del corpo studentesco.

Introduzione di contesto: cos'è la Didattica Digitale Integrata

Per fronteggiare l'emergenza sanitaria che colpì il mondo a partire dal 2020, la didattica inizialmente si aprì alla possibilità tecnologica di svolgere le lezioni in modalità remota, mentre, in un secondo tempo, iniziò a esplorare gli strumenti tecnologici utilizzati per la didattica online, comprendendone opportunità e vantaggi.

Il concetto di didattica digitale integrata (DDI) integra i concetti di didattica in presenza e a distanza, delineando un percorso di progettazione e consolidamento degli strumenti tecnologici, permettendo di coglierne pienamente tutti i vantaggi.

Il documento di riferimento per tale progettazione sono **le linee guida per la didattica digitale integrata**, parte integrante del Decreto ministeriale 39/2020. Riepiloghiamo qui alcuni passaggi chiave:

- Nota dipartimentale del 17 marzo 2020: è consentito lo svolgimento di attività didattiche a distanza.

- Decreto legge 8 aprile 2020: è stabilito l'obbligo per il personale docente e dirigenti scolastici di assicurare lo svolgimento dell'attività di didattica a distanza attraverso l'ausilio degli strumenti tecnologici disponibili.
- Il Decreto legge 19 marzo 2020: assegna dei fondi per migliorare la didattica.

Dopo la fase iniziale della pandemia, che ha funzionato come trigger per progettare una didattica a 360°, è ora possibile delineare un quadro più completo dei vantaggi e delle sfide di una buona didattica digitale integrata. Tutti i vantaggi della didattica digitale integrata si possono considerare applicabili anche alle modalità di lavoro:

- **Superamento dello spazio fisico:** la lezione è progettata per essere fruita indifferentemente dal luogo fisico in cui studenti e docenti si trovano.
- **Superamento del proprio gruppo o ecosistema**: è possibile far partecipare o collegare persone che non fanno parte dell'ambiente di studio o lavoro, con un enorme abbattimento dei costi e maggiore possibilità di interazione che in passato.
- **Superamento degli strumenti fisici** attraverso strumenti della "realtà **aumentata":** con questo concetto ci si riferisce alla possibilità di ampliare alcune percezioni della realtà, cogliendo elementi diversi da quelli che sono direttamente in discussione. Ne sono un esempio video che possono essere proiettati, QR code che possono condurre ad altri documenti, testi o percorsi.
- **Superamento dei vincoli temporali:** la lezione e molti dei suoi strumenti possono essere fruiti anche in modalità asincrona.

Per fare in modo che queste potenzialità siano un vantaggio per tutti, è necessario porre l'accento anche su altri aspetti:

a. **La didattica deve saper comunicare efficacemente per coinvolgere tutte le persone collegate allo spazio di lavoro**. Si rimanda alla sezione approfondimenti per questo aspetto.
b. Le nuove tecnologie che verranno introdotte, come l'intelligenza artificiale nella domotica, nella didattica, nello studio e nella ricerca, devono essere introdotte pensando a dei progetti che siano in grado di aprirsi all'innovazione come opportunità, ma anche all'equità nell'accesso alle **tecnologie e all'accessibilità**.
c. Come le linee guida ministeriali non mancano di sottolineare, devono essere garantite **la privacy** e l'accessibilità ai documenti anche quando si lavora in modo ibrido.

GLOSSARIO E DEFINIZIONI

Ai fini del presente documento si intende per:

- Amministratori di sistema: figure professionali finalizzate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009;
- Applicazioni aziendali: si considerano applicazioni aziendali:
    - Prodotti/programmi acquistati dall'Ateneo, di valenza generale, o settoriale ed in quest'ultimo caso approvati dall'Area ICT;
    - Applicazioni e servizi sviluppati ad hoc dell'Area ICT, da terze parti ma sotto il coordinamento dell'Area ICT, ovvero da altre strutture con un processo di partecipazione e approvazione da parte dell'Area ICT e che seguono le regole di gestione previste nei casi precedenti;
    - Applicazioni esterne che l'Ateneo utilizza secondo le regole di gestione e di sicurezza delle medesime a titolo di mero esempio possono essere la piattaforma NoiPA, abbonamenti a servizi informativi, portale ANAC, etc.
- Aziendali: nel corso del documento si farà spesso riferimento a risorse o dispositivi come "aziendali". Pur nella consapevolezza che l'Ateneo non è un'azienda, tale dicitura identifica più chiaramente l'organizzazione nella letteratura tecnica.
- Dispositivi o endpoint: qualunque dispositivo atto a connettersi alla rete Unige, ai suoi dati, alle applicazioni aziendali, alle risorse in genere.
- Dispositivi aziendali: dispositivi di proprietà o comunque nelle disponibilità dell'Università degli studi di Genova e messi nelle disponibilità degli utenti.
- File di log: registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato;
- GENUAnet: rete informatica gestita direttamente dall'Università di Genova divisa in rete cablata e rete WiFi eduRoam (già GenuaWiFi);
- Strumenti informatici: personal computer fissi o portatili o virtuali, stampanti locali o di rete, programmi e prodotti software in-house o in-cloud, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc);
- Utenti: personale dipendente, docenti, studenti, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni e coloro che, in virtù di un rapporto di lavoro, di studio o di collaborazione in essere a qualsiasi titolo con l'Ateneo, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione da Unige.

Descrizione dettagliata degli spazi comuni attualmente presenti in Ateneo

L'università, come la quasi totalità delle istituzioni e un numero elevatissimo di aziende, a partire dal 2020 ha introdotto all'interno dei propri ambienti di didattica e lavoro gli strumenti tecnologici necessari per la didattica digitale integrata e le modalità di lavoro agile e telelavoro. Per la descrizione dettagliata delle tipologie di aule attualmente presenti in Ateneo, si rimanda alla pagina nel sito dei Servizi dei servizi informatici di Ateneo, che costituisce parte integrante di queste linee guida.

Alcuni punti per la realizzazione della didattica digitale integrata sono stati introdotti e rimarranno punti fermi di ogni futura configurazione:

- Piattaforma software e hardware che garantisca la possibilità di collegarsi agli eventi che si svolgano nell'aula anche in modalità remota se previsto dai relatori.
- Presenza rete wi-fi
- Facilitazione del lavoro in coworking utilizzando piattaforme software che lo permettano

Sistemi di gestione delle Aule

La messa in servizio e la manutenzione dei sistemi di gestione delle aule è di esclusiva competenza dell'Area ICT. Quest'area può, tuttavia, delegare parte delle attività a ditte esterne, selezionate attraverso bandi pubblici. In questi bandi vengono dettagliatamente definiti i ruoli, gli obblighi, i vincoli e le funzioni assegnate alle ditte aggiudicatrici.

È importante sottolineare che nessun soggetto diverso dall'Area ICT è autorizzato a dotarsi di software o attrezzature necessarie per la gestione degli spazi comuni dell'Ateneo senza consultare l'Area ICT, il cui parere è vincolante. Questo garantisce una coerenza e un coordinamento centralizzato nella gestione delle risorse tecnologiche dell'Ateneo. I software attualmente utilizzati potranno essere cambiati se necessario con altri, mantenendone le funzioni e i ruoli descritti in questo documento.

Attualmente, per gestire gli spazi, l'Ateneo si è dotato di diversi software dedicati a specifiche attività:

- **Easy Academy/Easy Room**: Gestisce gli orari delle lezioni e le prenotazioni delle aule.
- **Webmonitor**: Gestisce l'inventario degli spazi e del materiale tecnico presente all'interno di essi.
- **GVE di Extron**: Gestisce nelle aule allestite con questa tecnologia le apparecchiature presenti, anche in modalità remota.

Easyacademy Easyroom

È un software proprietario acquistato dall'Ateneo per gestire gli orari delle lezioni e garantirne la massima diffusione agli studenti. Il software gestisce anche la rilevazione delle presenze

durante le lezioni ed è disponibile anche come applicazione per iOS e Android. Un portale specifico del software, denominato **"Easyroom"**, gestisce la prenotazione delle aule.

Il software è disponibile alla pagina https://easyacademy.unige.it/

Nel portale per ogni aula è indicato il numero di postazioni.

Per la prenotazione delle aule, gli utenti possono inoltrare delle richieste attraverso una pagina pubblica. Nell'applicazione, o da browser, è possibile visualizzare l'occupazione delle aule e, per gli studenti e i docenti, gli orari delle lezioni. C'è anche una sezione dedicata alla ricerca degli eventi in corso. La piattaforma è multilingua.

Il ciclo di prenotazione degli spazi è semplificato per i fruitori, poiché tutte le richieste vengono gestite attraverso il portale Easy Academy. Per le indicazioni relative agli eventi, consultare la pagina Prenota uno spazio | UniGe | Università di Genova

Per gestire **le prenotazioni**, ogni struttura o dipartimento ha individuato un referente per gli spazi comuni (referente Easy Academy), in grado di accettare le prenotazioni. Il portale, in ogni momento, può visualizzare ai fruitori lo stato delle stesse. I nomi dei referenti Easy Academy non sono pubblici, se non per scelta dei dipartimenti/strutture che rendono visibili i nominativi nei loro siti web. I referenti Easy Academy possono essere visualizzati nel portale Webmonitor, il cui accesso è riservato ai referenti tecnici di ogni dipartimento o struttura.

Webmonitor Unige Classroom

Parallelamente al progetto di adeguamento degli spazi di cui alla pagina "aule", l'Ateneo ha implementato un sistema per gestire l'inventario delle aule e degli spazi comuni. Il software, denominato **"Unige Classroom",** contiene l'elenco di tutte le aule didattiche di Ateneo, divise per edificio.

Per ogni aula sono riportati alcuni dati provenienti da altre fonti (ad esempio, la capienza delle aule), oltre a quelli di inventario delle dotazioni, che sono gestite direttamente nel software. Nello specifico sono riportati:

- La capienza delle aule/locali
- Il codice Ref building, che identifica in modo preciso ogni locale di Ateneo e viene utilizzato in vari ambiti in cui è necessario utilizzare le planimetrie (sicurezza, gestione di contratti per la manutenzione anche tecnica degli edifici)
- **L'indicazione del manutentore dell'aula, il referente tecnico e il referente Easy Academy**
- La dotazione tecnica presente, con l'indicazione dei Mac Address delle apparecchiature informatiche e degli indirizzi IP, ove necessario
- Il tipo di connessione del proiettore
- Altri dati (presenza Wi-Fi, cattedre, lavagna, accessibilità e predisposizione per studenti disabili)

GVE (Extron Global viewer enterprise)

Contiene un pannello di gestione di tutte le aule attrezzate con tecnologia Extron. Il pannello permette di eseguire operazioni analoghe a quelle che possono essere svolte all'interno dell'aula, anche in remoto. Citiamo a titolo di esempio:

- Accensione, spegnimento, riavvio dell'aula o di singole attrezzature, come, per esempio, il proiettore
- Visualizzazione e monitoraggio dello stato di funzionamento dell'aula nel suo complesso o di singole attrezzature

Alcune operazioni di aggiornamento sono gestite dalla ditta che effettua la manutenzione delle attrezzature, altre, come lo spegnimento, possono essere effettuate dai referenti tecnici delle strutture/dipartimenti.

Definizione dettagliata di tutti di tutti i ruoli coinvolti nella manutenzione delle aule

Per la gestione delle aule e degli spazi comuni, l'organizzazione e i ruoli rispecchiano la strutturazione interna dell'Ateneo. L'Area ICT organizza, progetta, realizza e gestisce il sistema informativo digitale dell'Ateneo, fornendo supporto alle Strutture Fondamentali attraverso i 5 Poli di Facility Management.

Nella gestione delle aule e degli spazi comuni, i **REFERENTI ICT DEI POLI TERRITORIALI** hanno il fondamentale compito di fare da punto di congiunzione tra l'Area e i referenti locali delle strutture e dei dipartimenti che, a vario titolo, si occupano degli spazi comuni. Il compito del referente dell'Area ICT del polo territoriale è di coordinamento. Supporta, ma non sostituisce, i referenti tecnici locali per la manutenzione delle aule, per l'uso dei software di gestione sopra menzionati, e per gestire le richieste di assistenza con le modalità descritte nei contratti di manutenzione. Come parte dell'Area ICT, contribuisce con essa all'introduzione delle nuove tecnologie all'interno delle aule e alla formazione su questi strumenti.

I referenti ICT dei poli territoriali sono reperibili agli indirizzi email indicati alla pagina seguente: Richieste di assistenza tecnica | Servizi informatici di Ateneo (unige.it) e afferiscono al settore servizi per i poli territoriali che rimane il riferimento principale per ogni chiarimento sugli aspetti funzionali.

Il canale privilegiato attraverso cui l'Area ICT comunica con i referenti informatici è il Teams **Assistenza referenti tecnici**. I referenti tecnici che dovessero richiedere di farne parte devono mandare un'email a assistenza@unige.it.

REFERENTE INFORMATICO è l'informatico deputato alla manutenzione delle aule. In particolare, gestisce:

- La manutenzione del PC docente e, eventualmente, altri PC presenti nelle aule, se informatiche. L'Area ICT, pur nella massima collaborazione per la ricerca delle migliori soluzioni, può imporre o richiedere ai referenti informatici di adottare soluzioni tecnologiche compatibili con gli standard di sicurezza, le tecnologie, e le configurazioni delle macchine, in modo da muoversi in una direzione comune, anche rispetto agli obiettivi di Ateneo e alla possibilità di gestione delle apparecchiature.

- La cura e la richiesta di sostituzione dei consumabili.
- L'apertura delle richieste di assistenza.

Si precisa che, per le aule inserite in progetti di manutenzione di Ateneo, è necessario seguire le modalità di assistenza in essi contenute. In caso di dubbi, ci si può rivolgere ai referenti ICT dei poli territoriali per avere chiarimenti.

REFERENTE EASY ACADEMY è la persona che, all'interno di ogni struttura, si occupa di gestire le richieste di prenotazione delle aule che vengono inserite su Easy Academy. Le aule in cui si tengono corsi di studio sono prenotate in automatico sulla base dei calendari didattici.

MANUTENTORE AULA viene indicato quando la manutenzione dell'aula è affidata a un soggetto diverso dal referente tecnico informatico interno della struttura in cui si trova l'aula. Se non indicato, si intende che corrisponda al referente informatico.

Richiesta di modifica allestimento hardware/software

Docenti, studenti attraverso i rappresentanti presso i consigli di corsi di studio, direttori delle strutture e il personale tecnico amministrativo possono aprire delle richieste di modifica allestimento strutturale o di allestimento hardware e software delle aule.

Citando brevemente l' Atto di Organizzazione Amministrativa e Tecnica vigente dal 1.5.2024.pdf (unige.it) all'interno di ogni polo territoriale si trovano:

- manutenzione edilizia e impiantistica, servizio fornito dall'Area Tecnica;
- negoziale, servizio fornito dall'Area Negoziale;
- ICT, servizio fornito dall'Area ICT.

Se la modifica riguarda il primo punto, si può contattare la figura apicale di gestione della struttura per la quale si fa la richiesta (Direttore della Scuola, del Dipartimento, Responsabile Amministrativo, o il Dirigente per le Aree, che prenderà accordi con il referente del polo in materia edilizia).

Se la modifica riguarda la dotazione ICT, hardware o software, va contattato il referente informatico nelle Strutture Fondamentali, o direttamente il referente ICT del polo nell'Amministrazione Centrale. Alcuni spazi comuni sono inseriti in piani di manutenzione e allestimento con modalità specifiche di gestione delle richieste.

Il riferimento per ogni dubbio informativo su questi aspetti attualmente è il Settore servizi per i poli territoriali cui afferiscono i referenti informatici dell'Area ICT dei Poli territoriali di facility management e che è da considerare unico riferimento per questo tipo di richieste.

Il referente informatico deve fare le seguenti valutazioni, in accordo con il settore sopra menzionato:

Compatibilità con i sistemi informativi già adottati in Ateneo.

Obiettivi che si vogliono raggiungere con il nuovo acquisto, in termini di efficacia, efficienza e economicità.

Per i software, va inoltre valutata con certezza:

- La presenza di eventuali altre strutture che hanno adoperato quel software.
- I costi.
- Gli obiettivi che si vogliono raggiungere e la presenza di eventuali software similari in Ateneo.
- Il numero di persone o postazioni su cui si desidera installare quel software, per poter valutare con certezza il tipo di licenza da adottare.

Si ritiene di sottolineare questi aspetti, in quanto una valutazione superficiale può comportare sanzioni in sede di valutazione dell'Ateneo. Inoltre, rimanendo sugli aspetti tecnici:

- Un software incompatibile con altre tecnologie adottate (autenticazione, piattaforme informative, sistemi) può complicare il funzionamento e risultare scomodo da configurare e complicato per l'utente.
- Può risultare antieconomico.

Chiediamo quindi una maggiore attenzione, in accordo con l'Area ICT, per evitare in futuro problemi spiacevoli di difficile gestione e, soprattutto, complicazioni per gli utenti, che ne sono i fruitori finali.