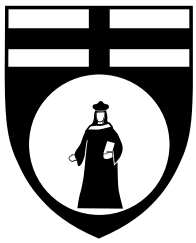

Università
di Genova

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.