Guida pratica alla sicurezza ICT per il progetto Up2U

L'ecosistema Up2U si basa sull'uso di Internet, dei sistemi cloud e sull'approccio Bring Your Own Device (BYOD). La creazione di un ambiente di apprendimento ICT sicuro e protetto per tutte le scuole coinvolte nei progetti pilota è una delle nostre priorità. Questa guida offre consigli pratici e semplici alle scuole su come ottenere tale ambiente.



Consapevolezza, responsabilità e procedure per tutta la scuola 9 consigli per insegnanti e amministratori di sistema

Istituire una Task Force per la sicurezza

Nella Task Force sulla sicurezza suggeriamo di inserire tutte le risorse umane che, all'interno della scuola, possano aiutare a identificare i rischi e creare una visione comune sulla sicurezza ICT. La collaborazione completa ad ogni livello è fondamentale.

Gestire tutti gli utenti

- Per i sistemi che gestiscono informazioni riservate, si consiglia di applicare rigide configurazioni utente. Per poter associare gli utenti ai dispositivi e contattarli in caso di necessità, è indispensabile creare un registro degli utenti.
- Usare gli account standard con privilegi limitati. Consentire l'uso di account amministrativi solo per gli utenti con competenze appropriate.
- Usare gli account amministrativi solo per eseguire operazioni che richiedono determinati privilegi.

Creare un inventario hardware e software

- Si consiglia di creare un inventario (in maniera manuale o con software automatico) dei dispositivi esistenti collegati alla rete, registrando il MAC address, l'host name, la funzione, il proprietario, l'ufficio associato, ecc.
- Potrebbe essere utile un sistema di allarme che, in caso di anomalie, rilevi i dispositivi connessi in rete e identifichi i dispositivi elettronici portatili.
- Creare un elenco del software autorizzato e un inventario del software installato.
- Effettuare scansioni regolari del sistema per rilevare software non autorizzati.

Creare una policy per la sicurezza

Una policy per la sicurezza scolastica deve affrontare, come minimo, quanto segue:

Rendere chiaro agli utenti che:

- Le risorse IT vanno utilizzate solo per scopi istituzionali
- Devono evitare di usare videogames e scaricare software illegali (MP3, film, ecc.)
- È vietato lanciare attacchi informatici su sistemi interni ed esterni

Informare regolarmente gli utenti sulle precauzioni:

- Fare attenzione alle e-mail di phishing. Alcuni indizi per individuarle sono:
  - Forte carattere di urgenza
  - Indirizzo del mittente sospetto
  - Saluti generici e firma altrettanto generica
  - Collegamenti ipertestuali contraffatti
  - Ortografia e layout (grammatica scadente)
  - Allegati sospetti
- Evitare di navigare su siti non affidabili e di cliccare su link sospetti
- Scaricare e installare software e app solo da siti affidabili
- Eliminare programmi o app non più utilizzati

Migliorare la sicurezza delle password:

- Assicurarsi che gli utenti:
  - Non rivelino mai le password, specialmente via Internet;
  - Rendano le password lunghe e complesse (almeno 12 caratteri, mescolando lettere maiuscole, numeri e simboli). È possibile creare una password lunga utilizzando una passphrase, vale a dire quattro o più parole casuali raggruppate e utilizzate come password;
  - Creino una password univoca per ogni account.
  - Non usino mai le informazioni personali come password;
  - Prendano in considerazione l'utilizzo di un gestore di password.
- Forzare periodicamente la modifica della password
- Utilizzare l'autenticazione a due fattori, se disponibile

Tenersi aggiornati!

- Mantenere aggiornato tutto il software (applicazioni e sistema), in modalità automatica se consentito.
- Tenere aggiornati anche tutti i dispositivi elettronici personali. I produttori rilasciano gli aggiornamenti man mano che scoprono vulnerabilità nei loro prodotti. Gli aggiornamenti automatici lo rendono più semplice per molti dispositivi, inclusi computer, telefoni, tablet, ma per altri dispositivi potrebbe essere necessario l'aggiornamento manuale. Installare gli aggiornamenti dai siti web dei produttori e dagli archivi di applicazioni incorporati: i siti e le applicazioni di terze parti non sono affidabili e possono infettare i dispositivi. Quando si acquistano nuovi dispositivi, valutare il mantenimento del produttore per garantire regolari aggiornamenti di supporto.
- È importante restare aggiornati sulle nuove vulnerabilità e intraprendere azioni di manutenzione regolari.
- Utilizzare strumenti di scansione delle vulnerabilità aggiornati.
- Verificare che le vulnerabilità emergenti dalle scansioni siano state risolte mediante patch o implementando contromisure appropriate o documentando e accettando un rischio ragionevole.
- Utilizzare solo software e sistemi operativi supportati (ad esempio, evitare Windows XP).
- Il vettore di attacco principale è il browser, soprattutto se non è aggiornato!

Sii consapevole!

- Controllare i log delle operazioni del server DHCP (generalmente abilitato per impostazione predefinita).
- Gestire ogni accesso alla rete registrando l'account, il timestamp, il MAC address e l'indirizzo IP.
- Eseguire periodicamente una valutazione della vulnerabilità interna e esterna per identificare preventivamente le proprie vulnerabilità prima che lo faccia qualche malintenzionato.

Implementare un programma di backup

- Eseguire backup regolari di dati critici e, a intervalli più lunghi, dell'intero sistema. Ci sono molte soluzioni cloud che possono aiutarti a farlo.
- Garantire la riservatezza dei dati nelle copie di backup mediante crittografia. La crittografia eseguita prima della trasmissione consente un backup remoto sicuro nel cloud.
- Assicurarsi che i dispositivi rimovibili contenenti backup (ad esempio, dischi rigidi esterni o pen drive USB) non siano accessibili in modo permanente dal sistema, per evitare che gli attacchi locali coinvolgano anche le copie di sicurezza.



- Attenzione all'inserimento di dispositivi USB sconosciuti nei sistemi scolastici. Potrebbero contenere un malware nascosto!
- Una policy affidabile di backup dei dati può salvarti se sei colpito da ransomware.

Creare una procedura per la gestione degli incidenti

Ogni scuola dovrebbe avere un piano di risposta agli incidenti informatici. Se le persone sanno cosa fare in caso di problemi, il loro impatto può essere ridotto al minimo.
Dopo l'incidente, dovresti documentare ciò che è successo e condividere tutte le informazioni, per prevenire casi simili in futuro.

Adottare le Acceptable Use Policy

Ogni utente della rete deve firmare una Acceptable Use Policy per la sicurezza ICT.
Le scuole possono rifarsi ai modelli e alle linee guida presenti sul sito web della rete WMnet (www.wmnet.org.uk).

The innovation action leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 732049 - Up2U

CC BY SA

Un sistema ICT sicuro

Personalizzazione della configurazione della rete e dei sistemi

Come proteggere la rete

- Configurare il router in modo appropriato (filtri antispoofing, filtri che consentono l'accesso solo ai servizi istituzionali).
- Segmentare la rete in sottoreti separate, applicando, in relazione al contesto, le politiche più rigorose:
  - Sottorete DMZ esposta a Internet (DNS, server Web, server di posta)
  - Sottorete per Management e Amministrazione
  - Sottorete per didattica e laboratori
  - Sottorete per studenti e ospiti (BYOD: smartphone, tablet, notebook)
  - Sottorete per stampanti, videosorveglianza, automazione degli edifici, dispositivi IoT, ecc.
- Installare almeno un firewall di rete che blocchi le connessioni in entrata a tutte le sottoreti (esclusa DMZ), eventualmente anche con la funzione di NAT.
- Attenuare gli attacchi effettuati tramite e-mail analizzando i messaggi prima che raggiungano la casella del destinatario. A tale scopo, configura il software antispam e antivirus sul server di posta.
- Installa una soluzione di filtraggio web per proteggere gli utenti da siti dannosi durante la navigazione.
- Abilitare la sicurezza wireless:
  - Utilizzare il più potente protocollo di crittografia disponibile (WPA2/WPA3)
  - Cambiare la password predefinita di amministratore del router
  - Modificare il Service Set Identifier (SSID) predefinito
  - Disabilitare il WiFi Protected Setup (WPS)
  - Ridurre la potenza del segnale wireless
  - Spegnere la rete quando non in uso (o configurare un'accensione programmata della rete wireless)
  - Disabilitare l'Universal Plug and Play (UPnP)
  - Mantenere tutti i router e i dispositivi di rete aggiornati all'ultima versione del firmware
  - Disabilitare la gestione remota
  - Monitorare i tentativi di connessione di dispositivi sconosciuti.



Firewall

I firewall forniscono protezione contro gli aggressori esterni preservando i computer o la rete da traffico di rete malevolo o non necessario.



I firewall possono anche impedire al software dannoso di accedere ai computer o a una rete tramite Internet.

I firewall possono essere configurati in modo da bloccare i dati da determinati indirizzi di rete, applicazioni o porte consentendo al tempo stesso l'accesso ai dati rilevanti e necessari.

I firewall richiedono professionisti qualificati per supportare la loro configurazione e manutenzione. La maggior parte dei prodotti firewall viene preconfigurata ed è pronta per l'uso. Poiché ciascun firewall è diverso, è necessario leggere e comprendere la documentazione fornita per determinare se le impostazioni del firewall predefinito sono sufficienti per le proprie esigenze.

I firewall non garantiscono che il tuo computer non venga attaccato.

I firewall aiutano principalmente a proteggere dal traffico dannoso, non dai programmi dannosi (ad es. malware) e potrebbero non proteggerti se accidentalmente installi o esegui malware sul computer. Tuttavia, l'utilizzo di un firewall insieme ad altre misure protettive (ad es. software antivirus e pratiche informatiche sicure) rafforzerà la resistenza agli attacchi.



Come proteggere i sistemi

Definire e implementare le configurazioni standard e le politiche di protezione dei sistemi:

- Disinstallare software non necessari
- Disabilitare i servizi non necessari
- Condividere solo le risorse hardware necessarie e proteggerle
- Impedire le modifiche alla configurazione o l'installazione del software da parte di utenti non amministratori
- Impostare correttamente le configurazioni software e hardware predefinite (molti prodotti hanno una configurazione predefinita troppo aperta)
- Configurare client e server per utilizzare solo protocolli crittografati: SSH, HTTPS, IMAP e SMTP su SSL/TLS
- Installare localmente il software antivirus (e verificarne l'aggiornamento automatico)
- Installare localmente firewall e sistema di prevenzione delle intrusioni (IPS)
- Installare un Web Application Firewall (WAF) sul server Web
- Disabilitare l'esecuzione automatica dei contenuti quando si collegano dispositivi rimovibili
- Disabilitare l'esecuzione automatica di contenuti dinamici (ad esempio macro) nei file
- Disattivare l'apertura automatica delle e-mail
- Disabilitare l'anteprima automatica del contenuto del file
- Prima di connettere un nuovo dispositivo alla rete, sostituire le credenziali amministrative predefinite



The innovation action leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 732049 - Up2U

CC BY SA

Cos'è un'identità digitale?

L'identità digitale è la rappresentazione virtuale dell'identità reale che può essere utilizzata durante le interazioni elettroniche con persone o macchine.



Cosa sono l'autenticazione e l'autorizzazione?

❖ Autenticazione

L'autenticazione è il primo meccanismo che attiviamo quando vogliamo accedere a un ambiente fornendo informazioni che identificano univocamente noi stessi (le nostre credenziali).

❖ Autorizzazione

L'autorizzazione è il secondo meccanismo che viene attivato, una volta che la procedura di autenticazione ha avuto successo. Si tratta di un controllo effettuato dal servizio a cui vogliamo accedere, in base alle informazioni precedentemente fornite.

Single Sign-On (SSO)

Il Single Sign-On (SSO) è il meccanismo tramite il quale, all'interno di un'organizzazione, un utente può utilizzare le stesse credenziali per accedere a più servizi poiché esiste un'unica infrastruttura che gestisce le identità digitali.

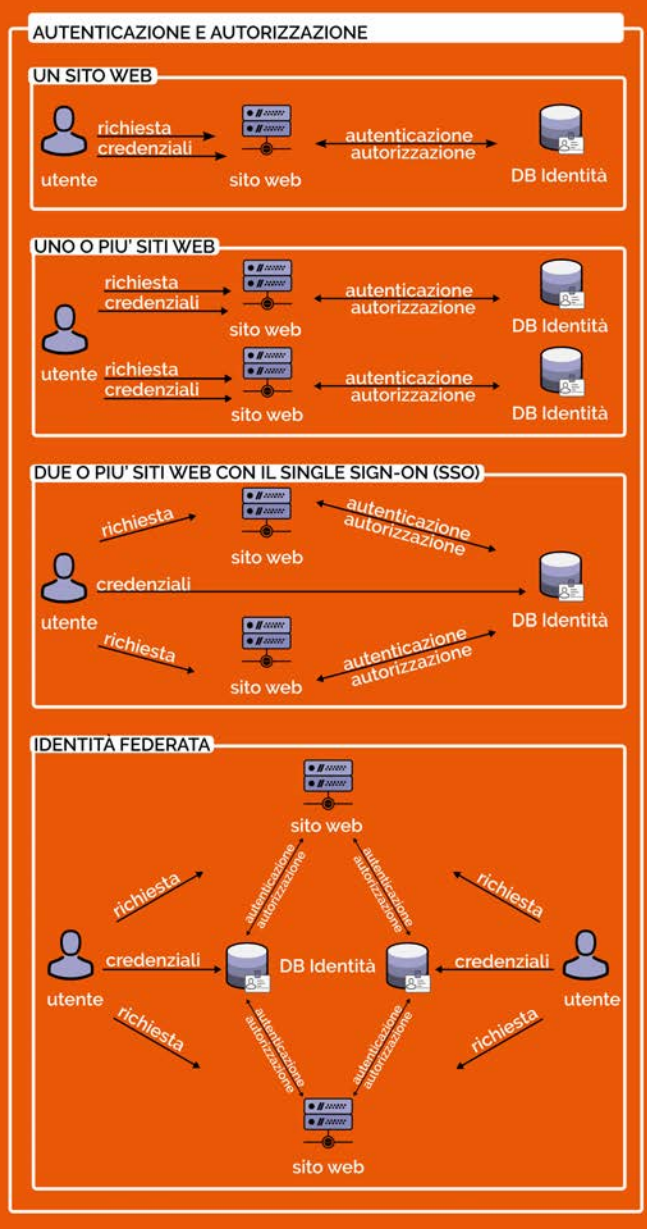
Quando parliamo di identità digitale federata?

L'identità digitale si dice federata quando lo stesso meccanismo di accesso viene esteso dall'organizzazione di appartenenza e permette di accedere ad una moltitudine di servizi forniti da diverse organizzazioni. Pertanto, un utente può usufruire dei servizi e delle risorse di tutte le organizzazioni federate senza modificare le proprie credenziali.

Soluzioni Up2U IAM

Up2U offre soluzioni che consentano agli utenti di gestire le proprie identità sulla piattaforma resa disponibile all'interno del progetto.
Per accedere ai servizi Up2U è necessario andare al link della piattaforma (learn.up2university.eu) e accedere attraverso i seguenti metodi.

Nella pagina di accesso (https://bit.ly/2OrVuw8) troverai tutti i seguenti metodi di autenticazione.



Autenticazione con Single Sign-On (SSO)

L'autenticazione è il processo mediante il quale un utente fornisce informazioni che si identificano in modo univoco (le loro credenziali). L'autorizzazione è il meccanismo mediante il quale un sistema determina quale livello di accesso deve avere un particolare utente autenticato alle risorse protette controllate dal sistema.

eduGAIN

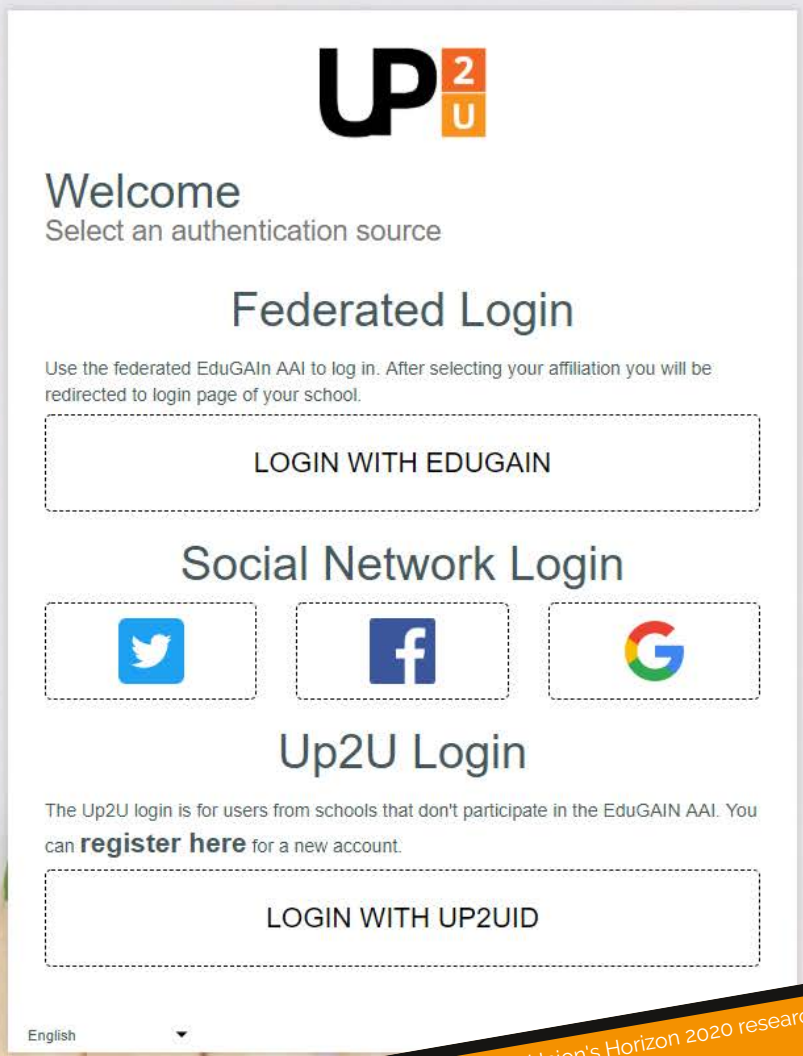
eduGAIN è usato per dare accesso all'ecosistema Up2U a tutti gli utenti del settore accademico e alle NREN (reti nazionali dell'istruzione e della ricerca) aderenti al progetto.Il servizio eduGAIN collega le federazioni di identità accademiche di tutto il mondo e aiuta studenti, ricercatori ed educatori ad accedere ai servizi online riducendo al minimo il numero di credenziali che utenti e fornitori di servizi devono gestire, riducendo così costi, complessità e rischi per la sicurezza.

Registrazione locale

Il portale di Up2U fornisce anche l'opzione di registrazione locale, permettendo così agli utenti senza un provider di identità (IdP) la possibilità di diventare membri del Next Generation Digital Learning Environment (NGDLE).

Autenticazione tramite social network

È possibile accedere ad Up2U via social network. Utilizzando le informazioni di accesso esistenti da un provider di social network come Facebook, Twitter o Google, l'utente può accedere alla piattaforma invece di creare un nuovo account specifico. Tutti i canali sono gestiti da un livello LDAP (Lightweight Directory Access Protocol). L'autenticazione utente LDAP è il processo di convalida di una combinazione di nome utente e password con un server di directory. Le directory LDAP sono una tecnologia standard per la memorizzazione di informazioni su utenti, gruppi e autorizzazioni.



The innovation action leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 732049 - Up2U

CC BY SA

10 suggerimenti per gli studenti sulla sicurezza informatica

- Utilizza software anti-virus.
- Non aprire e-mail, messaggi e allegati da fonti sconosciute. Sospetta di eventuali e-mail, messaggi e allegati inaspettati, anche se provengono da una fonte conosciuta.
- Proteggi i tuoi dispositivi (smartphone, tablet, laptop,...) da possibili tentativi di intrusione.
- Scarica regolarmente aggiornamenti di sicurezza e patch per sistemi operativi e altri software.
- Usa password difficili da indovinare. Usa combinazioni di lettere maiuscole, minuscole, numeri e altri caratteri non facilmente reperibili nel dizionario. Assicurati che le tue password siano composte da almeno 12 caratteri.
- Effettua regolarmente il backup dei dati su hard-disk o cloud.
- Non condividere l'accesso ai tuoi dispositivi con estranei. Informati sui rischi di condivisione dei file.
- Disconnettiti da Internet quando non lo stai usando.
- Controlla la sicurezza dei tuoi dispositivi con cadenza regolare.
- Assicurati di sapere cosa fare se ritieni che un dispositivo o un sistema sia infetto o compromesso.





10 suggerimenti sul BYOD

- Usa la crittografia per proteggere i tuoi dati (Impostazioni -> Sicurezza -> Cifra dispositivo), anche se stai per ripristinare lo smartphone.
- Non installare software da fonti inaffidabili (le fonti affidabili sono, ad esempio, Google Play, App Store di Apple, Appstore di Amazon per Android). Verifica che le autorizzazioni delle applicazioni siano chiare.
- Cancella i dati da remoto in caso di smarrimento o furto del dispositivo (Gestione dispositivi Android di Google, Anti-Theft, Cerberus, ecc.) e presta attenzione ai dati sui dispositivi dismessi.
- Utilizza un PIN o una password sufficientemente complicati per proteggere il dispositivo. È un po' macchinoso, ma è sicuramente più sicuro. Una buona password è la scelta migliore, ma utilizza almeno una sequenza non banale di caratteri.
- Attiva il Bluetooth solo quando necessario.
- Evita il collegamento a reti wireless sconosciute.
- Mantieni tutti i dispositivi aggiornati con la versione più recente del firmware.
- Effettua il backup dei tuoi dati.
- Evita di memorizzare nomi utente e password sul dispositivo o nel browser.
- Non eseguire il jailbreak o il root del dispositivo (jailbreaking o rooting di un dispositivo sono processi che rimuovono le restrizioni della piattaforma, consentendo agli utenti di installare qualsiasi applicazione da qualsiasi sorgente, installare un sistema operativo modificato e avere permessi di amministratore).



The innovation action leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 732049 - Up2U

CC BY SA

Come si applica il GDPR alle scuole coinvolte nel progetto UP2U



Che cos'è il GDPR?

Il regolamento generale sulla protezione dei dati (GDPR) è un quadro normativo che disciplina la raccolta e il trattamento delle informazioni personali all'interno dell'Unione europea (UE). Il GDPR è entrato in vigore in tutta l'Unione europea il 25 maggio 2018, sostituendo la direttiva 95/46/CE sulla protezione dei dati, per:

- Armonizzare le leggi sulla privacy dei dati in tutta Europa
- Proteggere e rafforzare la riservatezza dei dati di tutti i cittadini dell'UE
- Ridisegnare il modo in cui le organizzazioni di tutta Europa affrontano la privacy dei dati.

A chi si applica il GDPR?

Si applica a coloro che trattano i dati personali. Più esattamente si applica a coloro che "determinano le finalità e i mezzi del trattamento di dati personali" (Articolo 4 paragrafo 7). Il trattamento dei dati personali deve avvenire nel rispetto dei principi e delle regole stabiliti dal GDPR.
Nel progetto Up2U, le finalità e i mezzi con cui i dati personali vengono elaborati sono determinati dai partner del progetto in conformità con i contenuti del Grant Agreement e dell'Up2U Consortium Agreement.
Pertanto, nell'ambito del progetto Up2U, il Titolare del trattamento dei dati è il gruppo di partecipanti al progetto, che ha emanato un regolamento sui rispettivi obblighi e responsabilità, firmando un accordo specifico (Joint Controller Agreement).



Conformità al GDPR del progetto UP2U

Se la tua scuola aderisce al progetto Up2U, i dati personali provenienti da insegnanti, personale scolastico e studenti (soggetti interessati) che utilizzano i nostri strumenti e servizi ICT saranno controllati ed elaborati da Up2U.

Nell'ambito del progetto Up2U alle scuole pilota non è richiesta alcuna azione per essere conformi al GDPR, in quanto le scuole non elaborano né raccolgono dati personali e non determinano le finalità e i mezzi del trattamento di tali dati.

Le scuole pilota vengono informate attraverso il Memorandum of Understanding (MoU) circa le attività previste dal progetto Up2U, al fine di assicurare che le azioni del progetto corrispondano alla missione della scuola.

Il Titolare del trattamento dei dati è il gruppo di partner Up2U che ha firmato un Joint Controller Agreement, un accordo che serve a regolare i rispettivi compiti, le relazioni interne tra i Data Controller congiunti e la gestione delle attività nei confronti degli interessati e delle autorità. Il referente per i diritti degli interessati è, in conformità con l'art. 26, il "Punto di contatto", rappresentato dall'Associazione GÉANT.

Il trattamento dei dati personali inizierà con l'accesso alla piattaforma Next-Generation Digital Learning Environment (NGDLE) e terminerà alla fine del progetto.



The innovation action leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 732049 - Up2U

CC BY SA

Linee guida alle OER

Suggerimenti per l'uso delle OER

1: Scegliere una licenza Creative Commons per la tua OER

Per poter scegliere una licenza Creative Commons (CC) per un oggetto di apprendimento come un OER o per qualsiasi altro lavoro o creazione, dovresti essere in grado di rispondere a quattro domande:

- Sei d'accordo con il fatto che altre persone potrebbero copiare e distribuire i tuoi contenuti senza alcun tipo di permesso?
- Sei d'accordo con il fatto che altre persone possano modificare e adattare i contenuti quando li usano?
- Ti importa se altre persone useranno il tuo contenuto a scopo di lucro?
- Se autorizzi modifiche al tuo lavoro, desideri che il nuovo contenuto abbia la stessa licenza che hai scelto?

Creative Commons ha un servizio online che potrebbe aiutarti a identificare la licenza appropriata, basata sulla risposta a queste domande.

2: Ricercare oggetti di base con una licenza compatibile

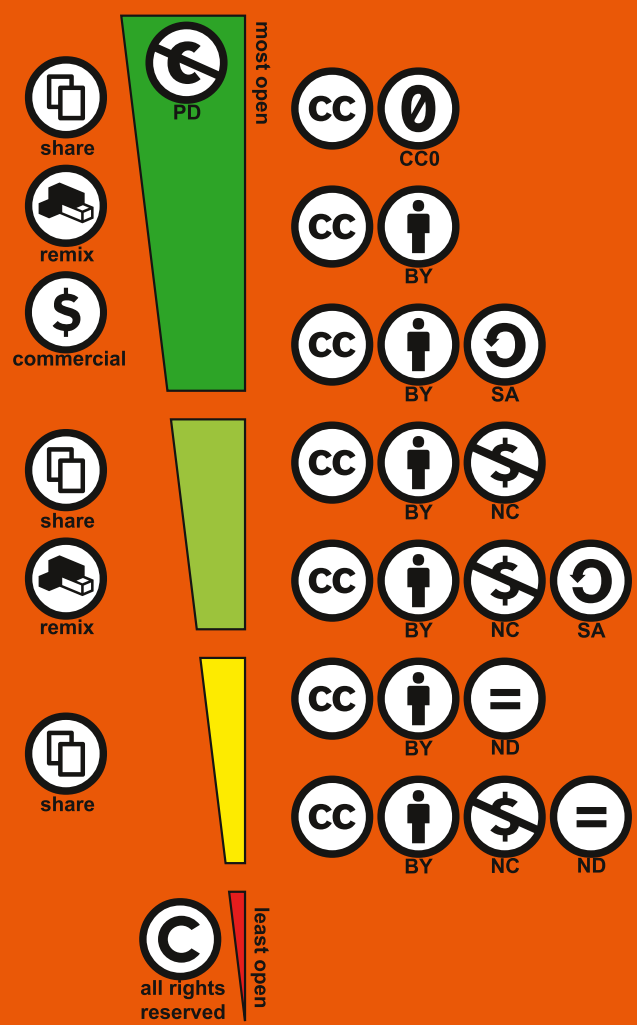
Esistono sei diverse licenze d'uso e ognuna presenta condizioni speciali. Durante la fase di selezione delle risorse, è necessario prendere in considerazione quelle con una licenza d'uso compatibile con quella che si intende utilizzare, in modo che possano essere integrate come un Business Object (BO) nel proprio Learning Object (LO). Un grafico di compatibilità è fornito qui a destra.

3: Riconoscere le risorse utilizzate

È importante riconoscere le risorse utilizzate per il Learning Object che stai creando.
Un acronimo utile da ricordare, per aiutarti a fare una corretta attribuzione di ogni risorsa, è "TYAOL", che indica i cinque aspetti da citare:

Title (Titolo) - Il nome o il titolo dell'opera.
Year (Anno) - La data in cui il lavoro è stato pubblicato.
Author (Autore) - Il nome del creatore del lavoro.
Origin (Origine) - Dove si trova il lavoro.
Licence (Licenza) - Come il lavoro può essere utilizzato.

È importante verificare la compatibilità tra le autorizzazioni e le condizioni delle sei licenze CC per non ignorare i desideri degli autori delle opere che usi.



https://en.wikipedia.org/wiki/Creative_Commons_license

Definire i metadati

Quando pubblichi la tua risorsa, il servizio in cui sarà pubblicata dovrebbe includere e correlarla alle stesse informazioni di base, note anche come metadati o firma descrittiva, che usi per attribuire o citare il lavoro di un'altra persona. In breve, ricorda l'acronimo TYAOL e assicurati che le informazioni siano chiaramente visibili in modo che altre persone possano dare la corretta attribuzione al tuo lavoro.
Inoltre, è consigliabile includere:

- Entità: valutare in ciascun caso la necessità di associare anche dati come l'entità, istituzione o organizzazione che supporta il processo di produzione, e i rispettivi collaboratori.
- Contatto: fornire i dettagli di contatto, ad es. un indirizzo email controllato frequentemente, in modo che se qualcuno è interessato alla tua risorsa possa comunicare con te.

Quando si crea un Learning Object, si consiglia di includere una pagina o uno spazio per i crediti in cui sono incorporati i metadati. In questo modo, anche quando il materiale viene spostato dal sito di pubblicazione originale, manterrà i dati necessari per il riconoscimento appropriato.

5: Pubblicare o distribuire

L'ultimo passaggio nella creazione della tua OER è di pubblicarla o distribuirla, per renderla disponibile ai tuoi studenti e ad altri potenziali utenti.
Esistono diversi sistemi per la condivisione delle informazioni digitali, ad esempio l'invio del file tramite e-mail o il caricamento su un social network affinché gli studenti possano scaricarlo e visualizzarlo sui propri dispositivi. L'efficacia di questi metodi è dimostrata. Tuttavia, la piattaforma Up2U offre alcuni vantaggi nella condivisione di queste risorse che consentono di:

- Risparmiare tempo. Se pubblichi l'OER su un singolo sito, devi solo indicare il link o l'indirizzo per chiunque possa accedervi da qualsiasi dispositivo, sia per visualizzarlo sia per scaricarlo.
- Espandere potenzialmente il pubblico. Hai la possibilità di aumentare il numero di utenti e il loro accesso alla risorsa, soprattutto considerando che questo è l'obiettivo quando si sceglie una licenza CC.
- Rendere facile l'accesso e la visualizzazione. Consente una visualizzazione diretta e immediata di OER senza download.
- Seguire le migliori pratiche per la pubblicazione e la distribuzione delle informazioni, attraverso l'uso di moduli.

Up2U offre una gamma di servizi Web che funzionano come repository di contenuti da condividere e che includono moduli che richiedono la compilazione di campi come:

- Titolo
- Descrizione
- Categoria
- Tag o parole chiave
- Lingua

I servizi per la pubblicazione di OER includono quelli utilizzati per cercare informazioni, ad esempio:

- Immagini, audio, video: DSpace.
- Testo: blog, siti web.
- Condivisione di risorse: il servizio di storage su cloud CERNBox.

I tool Up2U per creare e riutilizzare OER

Di seguito viene riportata una selezione di strumenti dell'ecosistema Up2U che consentono la creazione e la gestione di OER.

Moodle

Web: moodle.org
Up2U platform: learn.up2university.eu
Tutorial: docs.moodle.org/22/en/Moodle_video_tutorials

H5P

Web: h5p.org
Tutorial: h5p.org/documentation
Examples: h5p.org/content-types-and-applications

Knockplop

Web: github.com/so010/knockplop
Tutorial: up2university.eu/2018/01/18/knockplop

SeLCont

Web: github.com/netmode/selcont
Tutorial: www.netmode.ntua.gr/main/index.php?option=com_content&view=article&id=142&Itemid=9

The innovation action leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 732049 - Up2U

CC BY SA