DOPAU 2.0

DOcumento descrittivo del **P**rocesso di **A**ccreditamento degli **U**tenti dell'Organizzazione

Logout

Documento aggiornato

Introduzione

La partecipazione alla Federazione IDEM abilita l'organizzazione partecipante a condividere le risorse on-line rese disponibili all'interno della comunità IDEM.
Al fine di assicurare che le asserzioni inviate dagli Identity Provider ai Service Provider siano sufficientemente robuste e fidate per garantire l'accesso alle risorse protette, si richiede all'organizzazione partecipante di compilare il DOPAU (DOcumento descrittivo del Processo di Accreditamento degli Utenti dell'Organizzazione).

Il DOPAU è un questionario che deve essere compilato da ogni organizzazione partecipante. Esso intende raccogliere informazioni riguardanti il sistema di Identity Management dell'ente. Le informazioni che verranno rilasciate saranno riservate alla Federazione IDEM e verranno trattate secondo quanto indicato nelle Nome di Partecipazione della Federazione IDEM.
La federazione si riserva la possibilità di utilizzare i dati in forma anonima e/o in maniera aggregata ai fini statistici.

Modalità di compilazione

Il questionario si suddivide in due parti:

- la prima parte riguarda domande relative ad ogni processo di accreditamento e gestione delle identità che genera credenziali utilizzate per l'accesso a risorse federate.
  Il questionario riguarda esclusivamente il ciclo di vita delle identità che hanno accesso alle risorse delle federazione. E' necessario, quindi, prima di compilare questa parte che l'organizzazione partecipante individui tutti i processi di accreditamento presenti all'interno del suo ente finalizzati al rilascio di credenziali utili per accedere alle risorse federate. Per ogni processo individuato verranno poste delle domande volte a comprendere il funzionamento dello stesso. Esse saranno suddivise in due sezioni: *Informazioni sul processo di accreditamento* e *La gestione delle Identità;*
- la seconda parte riguarda in generale il sistema di Identity Management dell'organizzazione e l'informazione all'utente e il consenso in relazione ai servizi accessibili con autenticazione federata.

Quasi tutte le domande sono a risposta chiusa. Qualora la risposta ad una domanda non rientrasse tra quelle indicate si richiede di esplicitarla nelle note compilabili in fondo a ciascuna sezione.

Si sottolinea che le domande non trattano gli aspetti già previsti per legge ai sensi del Codice in materia di protezione dei dati personali in relazione all'Allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" in quanto essi devono essere rispettati come obbligo di legge.

Compito dell'organizzazione sarà quello di una revisione periodica del DOPAU. Inoltre l'organizzazione ha il compito di modificare tempestivamente il contenuto del DOPAU qualora ci siano degli aggiornamenti sul sistema di Identity Management e sui processi di accreditamento indicati.

La Federazione IDEM si riserva di effettuare, in accordo con l'organizzazione partecipante, dei controlli sulla veridicità delle risposte.

L'organizzazione partecipante (nella figura del Referente Organizzativo) assume la piena responsabilità di quanto indicato nel DOPAU.

Si ricorda infine che la compilazione del questionario può essere interrotta e salvata.

La compilazione del questionario richiede circa 30 minuti.

Glossario

DOPAU	DOcumento descrittivo del Processo di Accreditamento degli Utenti dell'Organizzazione
Processo di Accreditamento	L'insieme delle fasi necessarie per la creazione dell'identità digitale
IdP	Identity Provider
OdA	Organizzazione di Appartenenza
pwd	password
RA	Registration Authority
SP	Service Provider

Questionario

1. **PARTE I - I PROCESSI DI ACCREDITAMENTO**
    1. Informazione sul processo di accreditamento
    2. La gestione delle Identità
2. **PARTE II - IL SISTEMA DI IDENTITY MANAGEMENT**
    1. L'informazione all'utente e il consenso
    2. Informazione sul sistema di Identity Management

Organizzatore/Ente	Centro di Riferimento Oncologico di Aviano
Nome e cognome di chi compila il questionario	Ricci Roberto

PARTE I - I PROCESSI DI ACCREDITAMENTO

Quanti processi di accreditamento sono presenti nella tua Organizzazione di Appartenenza ("Oda")? (indicare un numero)
1

Elenca i processi di accreditamento individuati nella domanda precedente:

1. IDEM – IdP in the Cloud
2.
3.
4.
5.
6.
7.
8.
9.
10.

Relativamente ai processi di accreditamento indicati rispondete alle domande presenti nella sezione **1.1**.

Attenzione E' necessario rispondere al blocco di domande relativamente a ciascun processo di accreditamento (es: 5 processi indicati, 5 blocchi di risposte). Blocchi successivi al numero di processi di accreditamento indicati **verranno ignorati durante il salvataggio dei dati** (es: 5 processi e 7 blocchi compilati).

1.1 - INFORMAZIONI SUL PROCESSO DI ACCREDITAMENTO

[-] Comprimi il blocco 1

Domande relative al processo di accreditamento #1

1.1.1 Descrivere brevemente a quale categoria di utenza è rivolto (max 1000 parole)

Il servizio è rivolto a tutte le categorie di utenza del CRO di Aviano, in particolare medici, fisici, biologi, farmacisti, chimici, bioinformatici, ricercatori contrattisti e borsisti, tirocinanti e specializzandi.

1.1.2 Esiste un ufficio/un referente (RA: Registration Authority) all'interno della tua OdA incaricato di effettuare gli accreditamenti per questa tipologia di utenti?

- (●) **a.** Si, esiste/esistono una/più persone designata/e che sono le uniche incaricate ad effettuare gli accreditamenti
- ( ) **b.** No, ognuno si auto-accredita
- ( ) **c.** L'accreditamento avviene in maniera automatica tramite il sistema di Identity Management a seguito di un'identificazione dell'utente da parte degli uffici amministrativi (Ufficio Risorse Umane, Segreteria Studenti, etc.) all'atto dell'inizio di un rapporto formale con l'OdA (es. assunzione, immatricolazione, etc.) anche se non finalizzata al rilascio delle credenziali
- ( ) **d.** Ogni utente accreditato può effettuare l'accreditamento di altre persone (es. in caso di visitatore)
- ( ) **e.** Altro

1.1.3 La procedura di registrazione/accreditamento dell'utente avviene dopo che (più risposte possibili):

- [ ] **a.** La persona è stata identificata de visu attraverso un documento di identità personale
- [ ] **b.** La persona è stata identificata sulla base dell'acquisizione dei dati di una carta di credito o di una SIM card
- [ ] **c.** Senza alcun tipo di identificazione
- [x] **d.** Altro

1.1.4 Esiste una policy e/o un documento descrittivo dei passi che devono essere eseguiti per effettuare l'identificazione?

- (●) **a.** Si
- ( ) **b.** No

1.1.5 Quali tra gli attributi richiesti dalla Federazione IDEM (obbligatori, raccomandati o opzionali) vengono registrati e tenuti aggiornati nel tempo dall'OdA (più risposte possibili)?

	Nome LDAP	Origine	Descrizione	Stato
[x]	Sn	LDAPv3 rfc4519	*Descrizione:* Cognome *Semantica:* Cognome della persona come usato nelle comunicazioni ufficiali *Esempio:* Rossi	raccomandato

☑	givenName	LDAPv3 rfc4519	*Descrizione:* Nome *Semantica:* Nome proprio della persona come usato nelle comunicazioni ufficiali *Esempio:* Andrea	raccomandato
☑	Cn	LDAPv3 rfc4519	*Descrizione:* Nome e Cognome *Semantica:* Indica il nome completo della persona *Esempio:* Andrea Rossi	raccomandato
☐	preferredlanguage	inetOrgPerson rfc2798	*Descrizione:* Lingua preferita dall'utente *Semantica:* Lingua scritta o parlata preferita dall'utente *Esempi:* it it-ch	opzionale
☐	schacMotherTongue	schac	*Descrizione:* Lingua madre dell'utente *Semantica:* E' la prima lingua che una persona impara *Esempi:* it it-ch	opzionale
☐	Title	LDAPv3 rfc4519	*Descrizione:* Titolo della persona nel contesto dell'organizzazione *Semantica:* Indica il titolo di una persona nel contesto della propria organizzazione *Esempio:* Direttore	opzionale
☐	schacPersonalTitle	schac	*Descrizione:* Titolo usato per salutare il soggetto *Semantica:* Specifica il titolo personale dell'utente *Esempio:* Sig.	opzionale
☐	schacPersonalPosition	LDAPv3 rfc4519	*Descrizione:* Il codice rappresentativo dell'inquadramento della persona all'interno dell'organizzazione secondo le convenzioni descritte nell'appendice B del documento "Specifiche tecniche per la compilazione e l'uso degli attributi" presente nel sito della Federazione Idem *Semantica:* Specifica la posizione (ruolo) all'interno dell'organizzazione *Esempio:* PO, PA, RU, ...	opzionale
☑	mail	Cosine rfc4524	*Descrizione:* Indirizzo eMail *Semantica:* Indica la casella di posta elettronica dell'utente *Esempio:* andrea.rossi@unimi.it	raccomandato
☐	telephoneNumber	LDAPv3 rfc4519	*Descrizione:* Recapito telefonico *Semantica:* Numero di telefono dell'utente, indicato in accordo al formato internazionale dei numeri di telefono *Esempio:* +39 02 779 160 81	opzionale
☐	mobile	Cosine rfc4524	*Descrizione:* Recapito cellulare *Semantica:* Indica il numero di cellulare associato all'utente, indicato in accordo al formato internazionale dei numeri di telefono *Esempio:* +39 347 379 15 71	opzionale
☐	facsimileTelephoneNumber	LDAPv3 rfc4519	*Descrizione:* Recapito fax *Semantica:* Numero di fax dell'utente, indicato in accordo al formato internazionale dei numeri di telefono *Esempio:* +39 02 779 160 81	opzionale

☐	schacUserPresenceID	schac	*Descrizione:* Insieme di recapiti relativi alla presenza della persona in rete *Semantica:* Recapiti relativi a diversi protocolli di rete *Esempi:* xmpp:a.rossi@univpm.it sip:rossi@myweb.com sip:+39-95-505-600@unimi.it;transport?TCP;user=phone sips:alice@atlanta.com?subject=project%20x&priority=urgent h323:andy@myweb.it:808;params skype:andrea.rossi	opzionale
☑	eduPersonOrgDN	eduPerson	*Descrizione:* L'organizzazione dell'utente *Semantica:* Il Distinguished Name (DN) della entry che rappresenta l'organizzazione di appartenenza alla quale la persona è associata *Esempi:* o=unimore,dc=unimore,dc=it o=Istituto di Fisiologia Clinica,dc=ifc,dc=cnr,dc=it	opzionale
☐	eduPersonOrgUnitDN	eduPerson	*Descrizione:* L'unità organizzativa di appartenenza alla quale la peraona è associata *Semantica:* Il Distinguished Name (DN) della entry che rappresenta l'unità organizzativa di appartenenza alla quale la persona è associata (ad esempio Dipartimento) *Esempio:* ou=Dipartimento di Fisica,o=unimore,dc=unimore,dc=it	opzionale
☑	eduPersonScopedAffiliation	eduPerson	*Descrizione:* Indica l'affiliazione dell'utente presso l'organizzazione di appartenenza, nella forma [affiliazione]@[organizzazione] *Semantica:* Affiliazione secondo le convenzioni descritte nell'Appendice B del documento "Specifiche tecniche per la compilazione e l'uso degli attributi" in congiunzione con l'Organizzazione di Appartenenza indicata nella forma [oganizzazione] *Esempi:* staff@biblio.bo.cnr.it faculty@unica.it	obbligatorio
☑	eduPersonTargetedID	eduPerson	*Descrizione:* Identificativo anonimo, persistente, non riassegnabile di un utente che viene trasferito dall'Organizzazione di Appartenenza ad un Fornitore di Servizio (oppure ad un gruppo di Fornitori). L'Organizzazione di Appartenenza comunica ad ogni Fornitore di Servizio (oppure ad un gruppo di Fornitori) solo il valore appropriato e non rivela tale valore ad altri Fornitori di Servizi. *Semantica:* Ogni valore è un identificativo anonimo persistente associato all'utente per la fruizione di uno specifico servizio composto da tre parti, nella forma [organizzazione]![servizio]![stringa opaca]. Per organizzazione si intende l'identificativo dell'IdP dell'utente. La stringa opaca deve essere univoca all'interno dell'organizzazione e generata con un meccanismo di hashing di dati univoci all'interno dell'utente. Gli identificativi persistenti definiti in SAML 2.0 sono conformi a queste specifiche. *Esempi:*	obbligatorio

			biblio.bo.cnr.it!servizio_1!1304asf2rsfs unica.it!servizio_n!alskdj92920alsk	
☑	eduPersonPrincipalName	eduPerson	*Descrizione:* Identificativo unico persistente dell'utente *Semantica:* Un identificativo che permette di riconoscere univocamente un utente in maniera coerente tra servizi diversi, nella forma: [identiificativo]@[organizzazione] *Esempi:* 132lk1j21@biblio.bo.cnr.it m.rossi@esempio.it	raccomandato
☑	eduPersonEntitlement	eduPerson	*Descrizione:* URI (URN o URL) che indica il diritto di accesso ad una risorsa. *Semantica:* I valori contenuti sono tipicamente delle URI che individuano una risorsa o una particolare proprietà dell'utente stesso. L'utente è autorizzato ad accedere ad una risorsa solo se eduPersonEntitlement contiene una particolare e predefinita URL. *Esempi:* http://nilde.bo.cnr.it urn:mace:internet2:terena.nl:garr:service	concordati con il fornitore di servizi

1.1.6 Quali meccanismi di autenticazione sono implementati dall'OdA e utilizzati dall'Identity Provider (più risposte possibili)?

- ☑ **a.** Username/password
- ☐ **b.** SmartCard
- ☐ **c.** SmartCardPKI (si viene autenticati attraverso una smartcard con inclusa una chiave privata e un PIN)
- ☐ **d.** Kerberos
- ☐ **e.** InternetProtocol (si viene autenticati attraverso l'utilizzo di un indirizzo IP)
- ☐ **f.** InternetProtocolPassword (si viene autenticati attraverso l'utilizzo di un indirizzo IP + una username/pwd)
- ☐ **g.** PGP (si viene autenticati tramite un firma digitale dove la chiave è validata come parte di un PGP Public Key Infrastructure)
- ☐ **h.** TimeSyncToken (si viene autenticati attraverso un token a tempo)
- ☐ **i.** TLSClient (si è autenticati mediante un certificato lato client utilizzando un trasporto sicuro SSL/TLS)
- ☐ **l.** X.509 (si viene autenticati mediante una firma digitale con una chiave validata come parte in un X.509 Public Key Infrastructured)
- ☐ **m.** Altro

1.1.7 Un utente può avere più identità digitali (e di conseguenza diverse credenziali) rilasciate dalla sua OdA (es. dipendente che è anche studente, ecc...)?

- ○ **a.** Si
- ◉ **b.** No

1.1.8 Come avviene la consegna delle credenziali?

- ○ **a.** Vengono consegnate all'utente a mano/a voce dall'ufficio/persona preposta all'accreditamento
- ◉ **b.** Vengono consegnate all'utente attraverso l'invio di una email dalla persona/ufficio preposto all'accreditamento
- ○ **c.** Vengono inviate all'utente per posta in busta chiusa
- ○ **d.** Altro

[+] Espandi il blocco 2
[+] Espandi il blocco 3
[+] Espandi il blocco 4
[+] Espandi il blocco 5
[+] Espandi il blocco 6
[+] Espandi il blocco 7
[+] Espandi il blocco 8
[+] Espandi il blocco 9
[+] Espandi il blocco 10

Attenzione I "blocchi" relativi ai processi di accreditamento devono corrispondere con il numero indicato a inizio documento.

1.1.9 E' possibile allegare un file che descriva il flusso dei vari processi di accreditamento dichiarati. L'allegato deve essere in formato **pdf** e della dimensione massima di **40MB**.

Sfoglia... Nessun file selezionato.

Attenzione E' possibile caricare un solo file con le caratteristiche indicate. Per aggiornare il documento allegato basta caricare nuovamente il file. Il precedente file caricato sarà cancellato automaticamente.

1.1.10 Indicare eventuali note aggiuntive che possano servire a completare le risposte sopra compilate (usare questo box per completare le informazioni per tutti i processi di accreditamento indicati)

La persona è stata identificata de visu attraverso un documento di identità personale dall'ufficio personale.
La persona è stata identificata de visu con o senza documento di identità personale dal personale addetto al rilascio delle credenziali

1.2 - LA GESTIONE DELL'IDENTITA'

1.2.1 Nel caso in cui l'OdA fornisca all'utente credenziali del tipo username/password, dichiarare quali delle seguenti politiche di sicurezza sono implementate dal sistema di gestione delle identità (più risposte possibili):

- [x] **a.** Al primo accesso l'utente è obbligato a cambiare la password
- [x] **b.** Un algoritmo, all'atto della sua impostazione, controlla il livello di robustezza della password, segnalandolo all'utente
- [x] **c.** All'atto del cambiamento della password, la nuova non può essere uguale alla vecchia
- [ ] **d.** Blocco delle credenziali in caso di ripetuto inserimento di password non corretta
- [ ] **e.** Altro

1.2.2 All'utente sono fornite istruzioni relativamente alla sua responsabilità nella custodia e nel mantenimento della segretezza delle sue credenziali:

- (•) **a.** Si
- ( ) **b.** No

1.2.3 Se si, quali misure sono adottate per rendere consapevole l'utente della riservatezza e dell'importanza delle credenziali? (più risposte possibili)

- [ ] **a.** Formazione per il personale neoassunto o dei nuovi iscritti
- [ ] **b.** L'utente firma un'assunzione di responsabilità
- [x] **c.** Ci sono espliciti riferimenti in regolamento/i dell'OdA
- [ ] **d.** Ci sono diverse comunicazioni in occasione di specifici eventi
- [x] **e.** Ci sono comunicazioni periodiche
- [ ] **f.** Esiste documentazione online che tratta questi argomenti
- [ ] **g.** Vengono svolti seminari/corsi attinenti la problematica aperti a personale e studenti
- [ ] **h.** Altro

1.2.4 Esiste una policy relativa alle gestione delle credenziali?

- ( ) **a.** Si, è pubblicata su web
- (•) **b.** Si, è fornita all'utente contestualmente all'accreditamento
- ( ) **c.** Si, ma non è pubblicata
- ( ) **d.** No
- ( ) **e.** Altro

1.2.5 Con periodicità almeno annuale viene effettuata una verifica (audit) dell'aderenza dell'identità digitale rispetto allo stato dell'utente?

- ( ) **a.** Si, automaticamente il sistema di gestione dell'identità verifica le identità digitale rispetto alle fonte autoritative
- ( ) **b.** Si, manualmente da uno o più incaricati
- (•) **c.** Si, in modalità mista automatica e manuale in base alle categorie di utenti
- ( ) **d.** No
- ( ) **e.** Altro

1.2.6 Il sistema di gestione delle identità consente di discriminare gruppi di utenti in base al livello della qualità del riconoscimento effettuato all'atto del rilascio delle credenziali?

- ( ) **a.** Si, in caso di riconoscimento de visu da una RA
- ( ) **b.** Si, in caso di riconoscimento tramite numero cellulare
- (•) **c.** No

1.2.7 Quanto dura l'accreditamento, cioè quando avviene la disabilitazione delle credenziali?

- ( ) **a.** Avviene al termine del rapporto di lavoro con l'OdA oppure al termine del corso di studi (perché si è laureato)
- ( ) **b.** Non vengono mai disabilitate
- (•) **c.** Vengono disabilitate dopo n mesi della data di cessazione del rapporto di lavoro con l'OdA o dopo n mesi dal termine del corso di studi (perché si è laureato)
- ( ) **d.** Vengono disabilitate a seguito di una rinuncia esplicita (per uno studente)
- ( ) **e.** Vengono disabilitate a seguito di una rinuncia implicita, ovvero dopo n mesi che non ha più sostenuto esami e/o non ha più pagato le tasse
- ( ) **f.** Altro

1.2.8 L'utente viene avvisato dell'imminente scadenza/disabilitazione dell'account?

- ○ **a.** Si
- ◉ **b.** No

1.2.9 Esiste la cancellazione definitiva dell'utente dal sistema di accreditamento?

- ○ **a.** Si, in automatico a seguito della sua disattivazione/disabilitazione
- ◉ **b.** Si, avviene manualmente ogni tanto da un ufficio incaricato a seguito dalla sua disattivazione/disabilitazione
- ○ **c.** L'utente non viene mai cancellato dal sistema di accreditamento
- ○ **d.** Altro

1.2.10 Indicare eventuali note aggiuntive che possano servire a completare le risposte sopra compilate

PARTE II - IL SISTEMA DI IDENTITY MANAGEMENT

2.1 - L'INFORMAZIONE ALL'UTENTE E IL CONSENSO

2.1.1 L'OdA informa gli utenti della disponibilità di servizi accessibili con autenticazione federata? (più risposte possibili)

- ☑ **a.** Si, mediante pagina web dedicata ai servizi di autenticazione federata
- ☐ **b.** Si, mediante la distribuzione di materiale cartaceo
- ☐ **c.** Si, mediante eventi informativi/divulgativi
- ☐ **d.** No

2.1.2 L'OdA informa gli utenti di quali siano le federazioni di identità a cui partecipa? (più risposte possibili)

- ☐ **a.** Si, mediante una pagina web dedicata ai servizi di autenticazione federata
- ☐ **b.** Si, mediante la distribuzione di materiale cartaceo
- ☐ **c.** Si, mediante eventi informativi/divulgativi
- ☑ **d.** No
- ☐ **e.** Altro

2.1.3 L'OdA informa gli utenti, anche in maniera semplificata, dei meccanismi di funzionamento dei sistemi federati (ad es. rilascio degli attributi da IdP a SP, eventuali rischi connessi, ecc.)? (più risposte possibili)

- ☐ **a.** Si, mediante una pagina web dedicata ai servizi di autenticazione federata
- ☐ **b.** Si, mediante la distribuzione di materiale cartaceo informativo/divulgativo
- ☐ **c.** Si, mediante eventi informativi/divulgativi
- ☑ **d.** No
- ☐ **e.** Altro

2.1.4 L'OdA informa l'utente sui dati personali che l'Identity Provider trasferirà ad uno specifico Service Provider di interesse per l'utente stesso? (più risposte possibili)

- ☐ **a.** Si, mediante un'informativa disponibile su di una pagina web dedicata ai servizi di autenticazione federata

- [ ] **b.** Si, mediante un'informativa su di una pagina web dedicata raggiungibile dalla pagina di login dell'Identity Provider o direttamente disponibile su quest'ultima
- [x] **c.** Si, in maniera dinamica all'atto del primo accesso al Service Provider, mediante l'uso di un meccanismo di visualizzazione degli attributi tipo uApprove o Consent
- [ ] **d.** Si, distribuendo agli utenti un'informativa cartacea
- [ ] **e.** No
- [ ] **f.** Altro

2.1.5 L'OdA, ove questo sia previsto dal D.Lgs. 196/2003, chiede all'utente il consenso al trasferimento dei suoi dati personali dall'Identity Provider ai Service Provider federati di interesse per l'utente stesso? (più risposte possibili)

- [ ] **a.** Si, mediante un'accettazione esplicita rilasciata on line tramite applicazione web con accesso autenticato
- [x] **b.** Si, in maniera dinamica all'atto del primo accesso al Service Provider, mediante l'uso di un meccanismo di visualizzazione degli attributi tipo uApprove o Consent
- [ ] **c.** Si, facendo firmare agli utenti un modulo di consenso cartaceo
- [ ] **d.** No
- [ ] **e.** Altro

2.1.6 Indicare eventuali note aggiuntive che possano servire a completare le risposte sopra compilate

2.2 - INFORMAZIONI SUL SISTEMA DI IDENTITY MANAGEMENT

2.2.1 La policy dell'OdA permette di rilasciare gli attributi che i Service Provider federati dichiarano necessari al funzionamento del servizio?

- ( ) **a.** Si, se il servizio viene erogato dall'Italia
- ( ) **b.** Si, se il servizio viene erogato dall'Europa
- (•) **c.** Si, se il Service Provider dichiara di accettare la direttiva europea sul trattamento dei dati personali
- ( ) **d.** No

2.2.2 La policy dell'OdA permette di rilasciare gli attributi che i Service Provider federati dichiarano non necessari (opzionali) al funzionamento del servizio?

- ( ) **a.** Si, se il servizio viene erogato dall'Italia
- ( ) **b.** Si, se il servizio viene erogato dall'Europa
- (•) **c.** Si, se il Service Provider dichiara di accettare la direttiva europea sul trattamento dei dati personali
- ( ) **d.** No

2.2.3 Quali misure sono adottate per garantire la continuità del servizio del sistema di autenticazione e autorizzazione (scelte multiple)?

- [x] **a.** Infrastruttura fault tolerant
- [x] **b.** Piano per disaster recovery
- [ ] **c.** Istanze multiple dell'IdP
- [ ] **d.** Altro

2.2.4 Gli interventi di manutenzione che comportano interruzioni o variazioni del servizio sono pianificati e gli utenti preavvisati?

- (●) **a.** Si
- ( ) **b.** No

2.2.5 I messaggi che restituisce l'IdP all'utente in caso di errore o malfunzionamento sono:

- (●) **a.** Legati al tipo di errore (es. si inserisce la pwd errata l'IdP restituisce un messaggio tipo "utenze e/o pwd errata")
- ( ) **b.** Riportano l'indicazione di come procedere, in particolare i contatti di riferimento (es. indirizzo email, pagina web)
- ( ) **c.** Altro

2.2.6 Le credenziali che vengono mantenute dal sistemi di Identity Management sono sempre trasmesse in modalità sicura e crittografata?

- (●) **a.** Si
- ( ) **b.** No, non sempre

2.2.7 Esistono applicazioni esterne all'OdA che utilizzano direttamente la directory istituzionale (ad esempio Ldap) e non l'Identity Provider?

- ( ) **a.** Si
- (●) **b.** No

2.2.8 Indicare eventuali note aggiuntive che possano servire a completare le risposte sopra compilate

Vuoi registrare il documento in bozza o in versione definitiva?

(●) In bozza (modificabile successivamente) ( ) Documento definitivo (non modificabile successivamente)

Registra il documento