

E031-Direttiva d'applicazione Microsoft 365

Direttiva sull'informatica della Confederazione

Classificazione: ¹	Nessuna
Carattere vincolante: ²	Direttiva
Tipo di direttiva: ³	Direttiva d'applicazione
Settore di pianificazione: ⁴	Prestazioni di base TIC a livello federale
Versione attuale:	2.1
Sostituisce la versione:	2.0
Stato (versione attuale):	Approvato
Decisione / Data di entrata in vigore (versione attuale):	Decisione in merito alla governance delle TIC: 15 maggio 2024 Entrata in vigore: 15 maggio 2024
Basi legali:	Il delegato alla trasformazione digitale e alla governance delle TIC in base all'articolo 17 capoverso 1 lettera e dell'ordinanza del 25 novembre 2020 sul coordinamento della trasformazione digitale e la governance delle TIC in seno all'Amministrazione federale (OTDI; RS 172.010.58)
Lingue:	Tedesco (originale), francese (traduzione), italiano (traduzione)

¹ Per i livelli di classificazione AD USO INTERNO e CONFIDENZIALE si veda l'art. 13 della legge del 18 dicembre 2020 sulla sicurezza delle informazioni (RS 128).

² Per la forma di atto e il carattere vincolante si veda la Guida di legislazione, Ufficio federale di giustizia, 1a edizione italiana 2019.

³ Cfr. [Piattaforma informativa TDI](#)

⁴ Settori di pianificazione secondo la Strategia TIC della Confederazione 2020-2023 del 3 aprile 2020 (SB000)

Indice

1	Disposizioni generali	3
1.1	Oggetto	3
1.2	Campo di applicazione	3
1.3	Definizioni.....	3
2	Direttiva di applicazione Microsoft 365	5
2.1	Competenze.....	5
2.2	Trattamento dei dati	5
2.3	Condizioni di utilizzo.....	6
3	Disposizioni finali	7
3.1	Applicazione.....	7
3.2	Verifica.....	7
3.3	Entrata in vigore.....	7
	Allegati	8
A.	Utilizzo dei servizi <i>M365</i>	8
B.	Panoramica della terminologia in uso	10
C.	Modifiche rispetto alla versione precedente	11
D.	Significato delle parole chiave relative al grado di obbligatorietà.....	11
E.	Riferimenti	11
F.	Abbreviazioni	12

1 Disposizioni generali

1.1 Oggetto

¹ La presente direttiva disciplina l'utilizzo della piattaforma Microsoft 365 quale parte del servizio standard di burotica.

² I fornitori di prestazioni e i beneficiari di prestazioni (ovvero gli utenti) devono attenersi alla presente direttiva per poter utilizzare i servizi Microsoft 365, i servizi basati su di essi o i servizi ampliati⁵. Il rispetto della direttiva garantisce l'uso conforme al diritto della piattaforma M365 e la protezione dei dati dell'Amministrazione federale.

³ La presente direttiva disciplina i principi per il trattamento dei dati sulla piattaforma Microsoft 365. Integra le direttive esistenti della Confederazione, dei dipartimenti e le altre linee guida delle unità amministrative sull'utilizzo degli strumenti informatici. L'attuazione della direttiva esige collaborazione e senso di responsabilità da parte di tutti i collaboratori dell'Amministrazione federale.

1.2 Campo d'applicazione

¹ Il campo d'applicazione della presente direttiva è identico a quello di cui all'articolo 2 dell'ordinanza sulla trasformazione digitale e l'informatica (OTDI).

² La presente direttiva si applica agli utenti dei servizi M365 del servizio standard di burotica.

³ Il grado di obbligatorietà⁶ delle singole disposizioni di cui al numero 2 della presente direttiva è stabilito secondo le parole chiave indicate nell'allegato D.

1.3 Definizioni

¹ Nella presente direttiva si intende per:

- a. *piattaforma Microsoft 365*: servizi basati sul cloud pubblico Microsoft 365 e messi a disposizione dal servizio standard di burotica. La piattaforma è integrata nell'ambiente di burotica dell'Amministrazione federale e ne è dunque parte integrante;
- b. *Microsoft 365 (M365)*: raccolta di applicazioni e funzioni basate sul cloud pubblico per la burotica (p. es. Teams, SharePoint Online, OneDrive for Business e tool amministrativi e di sicurezza) nonché di applicazioni *Microsoft 365 Apps for Enterprise* installate localmente nella postazione di lavoro;
- c. *portafoglio M365 della Confederazione*: servizi basati sul cloud pubblico di Microsoft 365 rilasciati dal servizio standard di burotica;
- d. *servizi M365*: servizi utilizzati secondo il portafoglio M365 della Confederazione. Si tratta in particolare di:
 - 1) *Microsoft 365 Apps for Enterprise (M365 Apps)*: applicazioni Office di burotica installate localmente nella postazione di lavoro (Teams, Outlook, Word, Excel, PowerPoint, OneNote, Access, ecc.),

⁵ P. es. Contact Center, Attendant Console, Shared Line Appearance, Teams Apps e altri ancora.

⁶ Grado di obbligatorietà conforme alle specifiche della *Request of Comments: RFC 2119 (PCB 14)*, *The Internet Engineering Task Force (IETF)*. Tali indicazioni secondo RFC 2119 fanno parte di una prassi consolidata nella definizione di standard internazionali.

- 2) *Microsoft 365*: applicazioni di burocratica basate sul cloud e utilizzabili tramite browser (p. es. Teams, Outlook Web Access, Word Online, Excel Online, PowerPoint Online),
 - 3) *Exchange Online*: sistema utilizzato per i servizi di posta elettronica che permette di accedere ai messaggi, al calendario, ai contatti e alle attività,
 - 4) *Teams*: piattaforma di collaborazione basata sul cloud che combina chat di lavoro singole e di gruppo, audioconferenza e videoconferenza, condivisione di documenti e di appuntamenti nel calendario nonché integrazione dello stato relativo alla raggiungibilità dei collaboratori in una postazione di lavoro centrale,
 - 5) *SharePoint Online*: piattaforma di collaborazione basata sul cloud. SharePoint Online permette all'Amministrazione federale di archiviare, utilizzare e gestire contenuti e applicazioni in modo congiunto,
 - 6) *OneDrive for Business*: sistema di archiviazione personale su cloud per i dati personali e privati come definito nella direttiva E026. Ove possibile, i dati aziendali devono essere archiviati negli archivi condivisi o nei sistemi previsti a tale scopo,
 - 7) *Viva Engage* (in precedenza *Yammer*): rete sociale utilizzata in ambito lavorativo. Pone l'accento in particolare sulla condivisione e la modifica di documenti, sullo scambio di conoscenze e sulla collaborazione e la comunicazione interna e tra imprese. All'interno dell'Amministrazione federale è utilizzata principalmente per le cosiddette «Communities of Practice».
- e. *Account Modern*: un account utente conforme al catalogo dei servizi standard gestito nell'Active Directory on-premises e replicato nell'Azure Active Directory. I servizi M365 sono disponibili solo ora con l'*Account Modern*;
- f. *postazione di lavoro*: il sistema di postazione di lavoro è costituito dal servizio relativo alla postazione di lavoro [SD105] e dal servizio Virtual Desktop [SD119], offerto dai servizi standard di burocratica secondo il catalogo di servizi standard [SD100]. Il sistema è integrato negli ambienti di burocratica della Confederazione e consente l'accesso alle applicazioni specializzate della Confederazione.

² Una panoramica dei termini in uso e dell'ambito di applicazione è riportata graficamente nell'allegato B.

2 Direttiva di applicazione Microsoft 365

2.1 Competenze

¹ Il servizio standard di burotica garantisce, insieme ai fornitori di prestazioni, le prestazioni TIC di base della postazione di lavoro secondo il catalogo di servizi standard [SD100].

² Il servizio standard di burotica garantisce la messa a disposizione dei servizi M365 nonché la protezione IT di base [Si001].

³ I dipartimenti e le unità amministrative (beneficiari di prestazioni) conoscono i dati e i processi aziendali che intendono trattare con M365 nonché i requisiti applicabili ai rispettivi settori. DEVONO pertanto determinare i requisiti di protezione dei dati di cui sono responsabili. Verificano se le misure di protezione IT di base sono sufficienti per i dati di cui sono responsabili. In particolare, devono garantire che su M365 non siano trattati dati non autorizzati ai sensi del numero 2.2 capoverso 1.

⁴ I documenti trattati DEVONO essere classificati e debitamente contrassegnati dagli utenti o da processi automatizzati in base al livello di classificazione secondo la legge sulla sicurezza delle informazioni (LSIn) e la legge sulla protezione dei dati (LPD).

⁵ I dipartimenti e le unità amministrative (beneficiari di prestazioni) stabiliscono, se necessario, ulteriori requisiti e misure applicabili al proprio ambito di competenza.

⁶ Il servizio standard di burotica fornisce sostegno ai dipartimenti e alle unità amministrative (in particolare con strumenti TIC, mezzi ausiliari, offerte formative ecc.) nell'adempimento dei propri compiti di cui al capoverso 3.

2.2 Trattamento dei dati

1 In M365 POSSONO essere trattate le «informazioni non classificate» secondo l'ordinanza sulla sicurezza delle informazioni (OSIn) nonché i «dati personali» secondo la LPD.

Per le informazioni con un livello di classificazione superiore secondo l'OSIn e i «dati personali degni di particolare protezione» nonché le profilazioni secondo la LPD, i servizi M365 sono espressamente vietati. I dati in questione devono essere aperti e trattati con la versione di Office installata localmente e gli strumenti autorizzati a tale scopo⁷. Devono essere salvati sui servizi autorizzati per l'unità amministrativa, quali GEVER o applicazioni specializzate.

L'impiego attualmente autorizzato dei singoli servizi M365 è specificato nell'allegato A.

² Salvo se è vietato da un regolamento sul trattamento dei dati o da una direttiva di un'unità amministrativa, le informazioni coperte dal segreto d'ufficio POSSONO essere trattate con i servizi M365⁸.

⁷ Attualmente sono inclusi gli strumenti di crittografia SecureCenter e il prodotto successivo CHCrypt.

⁸ Secondo le spiegazioni fornite nell'ambito dell'analisi delle basi giuridiche concernente Microsoft 365, il trattamento di dati coperti dal segreto d'ufficio è autorizzato in base ai contratti stipulati con Microsoft e alla modifica di legge adottata nell'art. 320 CP (v. [Progetto CEBA](#) → Basi legali).

Nelle direttive per evitare i rischi di violazione del segreto d'ufficio nell'Amministrazione federale (Si001-Hi03) sono elencate le raccomandazioni per evitare le violazioni del segreto d'ufficio che possono diventare rilevanti nell'ambito della comunicazione di dati a terzi nei casi di assistenza tecnica. In caso di dubbio, si raccomanda di consultare il servizio giuridico della propria unità amministrativa.

³ I dipartimenti e/o le unità amministrative DOVREBBERO fornire supporto ai propri collaboratori nella classificazione delle informazioni secondo la LPD. Poiché soltanto le unità amministrative conoscono i propri affari e i propri contenuti, SONO AUTORIZZATI a stabilire regolamenti specifici alla propria organizzazione per l'utilizzo di M365.

⁴ I servizi M365 DOVREBBERO essere utilizzati per scopi professionali secondo la direttiva d'applicazione sul sistema di postazione di lavoro E026.

⁵ Gli utenti SONO AUTORIZZATI a trattare temporaneamente le informazioni pertinenti agli affari con i servizi M365. Al termine dei lavori, tali informazioni devono essere reinserite nel rispettivo sistema di gestione degli affari GEVER o nell'applicazione specializzata⁹.

⁶ Prima di registrare qualsiasi comunicazione audio e/o video DEVE essere ottenuto il consenso da tutti i partecipanti.

⁷ Per ciascuna interazione con *Viva Engage* DEVE essere definito almeno un moderatore che intervenga se necessario nelle discussioni (p.es. in caso di insulti, esternazioni razziste o discriminatorie).

2.3 Condizioni di utilizzo

¹ Se offerti da Microsoft, i servizi M365 sono gestiti in Svizzera e i dati sono archiviati in territorio svizzero. Laddove ciò non sia possibile, i servizi sono gestiti all'interno dell'Unione Europea (limite dei dati dell'UE)¹⁰.

² Per motivi legati al diritto in materia di acquisti o alla sicurezza, alcuni servizi M365 non sono disponibili. La gamma di servizi a disposizione è definita nel *portafoglio M365 della Confederazione*.

³ Per poter utilizzare i servizi M365, l'unità amministrativa ordina, in base al catalogo dei servizi standard, la prestazione di mercato «*Account Modern*».

⁴ Con gli smart device gestiti tramite il sistema di gestione dei dispositivi mobili, i servizi M365 POSSONO essere utilizzati senza alcuna limitazione. Con tutti gli altri dispositivi privati o esterni POSSONO essere utilizzati i servizi M365 soltanto nella modalità di elaborazione online (Office Online) tramite browser¹¹.

⁵ L'accesso completo ai servizi di M365 (login) DEVE avvenire utilizzando i mezzi di autenticazione approvati (p. es. smartcard o altro sistema di autenticazione a più fattori)¹².

⁶ Al primo accesso alla piattaforma M365, gli utenti DEVONO confermare di aver preso atto della presente direttiva d'applicazione e rispettarne i principi ivi contenuti.

⁹ Art. 4 dell'ordinanza sulla gestione elettronica degli affari nell'Amministrazione federale (Ordinanza GEVER, RS 172.010.441).

¹⁰ Informazioni concernenti il luogo di archiviazione dei dati dei clienti da parte di Microsoft 365 > <https://learn.microsoft.com/it-ch/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide>.

¹¹ V. anche allegato A tabella 2. Tale aspetto è implementato sul piano tecnico dai fornitori di prestazioni.

¹² Tale aspetto è implementato sul piano tecnico dai fornitori di prestazioni.

3 Disposizioni finali

3.1 Applicazione

I dipartimenti e la Cancelleria federale garantiscono l'applicazione della presente direttiva nei loro rispettivi ambiti di competenza in virtù dell'articolo 3 OTDI.

3.2 Verifica

Il settore Trasformazione digitale e governance delle TIC della Cancelleria federale (settore TDT della CaF) verifica l'attualità e l'adeguatezza della presente direttiva al più tardi quattro anni dopo la sua entrata in vigore.

3.3 Entrata in vigore

¹ La presente direttiva entra in vigore il 15 maggio 2024.

² Per la piattaforma CEBA Agil si applica la versione 1.1 fino alla messa fuori servizio di CEBA Agil.

Allegati

A. Utilizzo dei servizi M365

Le tabelle seguenti illustrano le possibilità di utilizzo dei principali **servizi M365** in relazione agli aspetti concernenti la protezione dei dati e delle informazioni.

I requisiti e le limitazioni per il livello di classificazione AD USO INTERNO ai sensi dell'OSIn saranno verificati nuovamente non appena saranno disponibili le prescrizioni in materia di trattamento della SEPOS.

Verde: autorizzato senza limitazioni **Giallo:** autorizzato con limitazioni **Rosso:** non autorizzato

Classifica- zione LPD	Classifica- zione OSIn	Applicazioni Office locali (installate sulla postazione di lavoro)	M365 Online (versione Office Web)	Teams	SharePoint Online	OneDrive for Business	Viva Engage	Tutte le altre (p. es. Planner, To Do List, ...)
Dati perso- nali	Non classi- ficato	Senza limitazioni	Senza limitazioni sui dispo- sitivi dell'Amm. fed. (posta- zioni di lavoro). Soltanto trattamento online sui dispositivi non gestiti dall'Amm. fed. (p. es. PC privato).	Senza limitazioni	Senza limitazioni	Senza limitazioni	Senza limitazioni	Senza limitazioni
	AD USO IN- TERNO	Il trattamento sulla postazione di lavoro è autorizzato senza limitazioni. Tuttavia, le informazioni devono essere archivate sui sistemi on-premises come GEVER o in archivi o applica- zioni autorizzati dall'unità amministra- tiva. Non è consentita l'archiviazione in M365.	Trattamento non autoriz- zato	Trattamento, archi- viazione e comunica- zione chat, video e audio non autorizzati	Trattamento e archi- viazione non autoriz- zati	Archiviazione non autorizzata	Trattamento e archi- viazione non autoriz- zati	Trattamento e archi- viazione non autoriz- zati
Dati perso- nali degni di partico- lare prote- zione e profilazione	CONFI- DENZIALE	I documenti devono essere protetti tramite la crittografia autorizzata ¹³ . Trattamento possibile unicamente nella Safe Area locale del sistema di critto- grafia. Archiviazione in GEVER o in archivi o applicazioni autorizzate dall'unità am- ministrativa.	Trattamento non autoriz- zato	Trattamento, archi- viazione e comunica- zione chat, video e audio non autorizzati	Trattamento e archi- viazione non autoriz- zati	Archiviazione non autorizzata	Trattamento e archi- viazione non autoriz- zati	Trattamento e archi- viazione non autoriz- zati
	SEGRETO	Non autorizzato	Non autorizzato	Non autorizzato	Non autorizzato	Non autorizzato	Non autorizzato	Non autorizzato

¹³ P. es. Secure Center o CHCrypt.

Tabella 1: possibilità di utilizzo dei servizi M365

Possibilità di utilizzo dei servizi M365 in base alla categoria di dispositivo

La tabella seguente illustra le possibilità di utilizzo in base alle diverse categorie di dispositivo. I servizi M365 possono essere utilizzati senza alcuna limitazione sui dispositivi gestiti dall'Amministrazione federale per il trattamento di dati personali e informazioni non classificate. Dai dispositivi esterni l'accesso a M365 è possibile sia tramite mobile VDI service o tramite browser (solo tool online). L'accesso è effettuato tramite un account della Confederazione e un sistema di autenticazione a più fattori. I dati cui è stato attribuito un livello di classificazione più elevato possono essere generalmente trattati con limitazioni oppure non possono essere trattati.

Classificazione LPD	Classificazione OSIn	Dispositivo		
		Postazione di lavoro completamente gestita dall'Amministrazione federale (client di burotica) con applicazioni Office installate localmente e OneDrive for Business (incluso VDI mobile)	Postazione di lavoro in parte gestita dall'Amministrazione federale Dispositivo dotato di MDM della Confederazione quali smart device con applicazioni Office installate localmente e One Drive for Business.	Dispositivo esterno non gestito dall'Amministrazione federale (p. es. PC privato, BYOD, smartphone privato senza MDM)
Dati personali	Non classificato	Utilizzabili senza limitazioni	Utilizzabili senza limitazioni	Trattamento possibile soltanto online su M365 tramite browser (M365 Office Online) (con account della Confederazione e autenticazione a più fattori) Eccezione per il VDI mobile: utilizzabile senza limitazioni
	AD USO INTERNO	Il trattamento è autorizzato senza limitazioni sulla postazione di lavoro. Tuttavia, le informazioni devono essere archiviate sui sistemi on-premises come GEVER o in archivi o applicazioni autorizzati dall'unità amministrativa. Il salvataggio in M365 o in One Drive for Business non è autorizzato.	Il trattamento è autorizzato senza limitazioni sullo smartphone integrato sull'MDM Tuttavia, le informazioni devono essere archiviate sui sistemi on-premises come GEVER o in archivi o applicazioni autorizzati dall'unità amministrativa. Il salvataggio in M365 o in One Drive for Business non è autorizzato.	Trattamento, archiviazione e comunicazione chat, video e audio non autorizzati tramite Teams. Eccezione per il VDI mobile: utilizzabile senza limitazioni Tuttavia, le informazioni devono essere archiviate sui sistemi on-premises come GEVER o in archivi o applicazioni autorizzati dall'unità amministrativa. Il salvataggio in M365 o in One Drive for Business non è autorizzato.
Dati personali degni di particolare protezione e profilazione	CONFIDENZIALE	I documenti devono essere protetti tramite la crittografia autorizzata. Trattamento possibile unicamente nella Safe Area locale del sistema di crittografia. Archiviazione in GEVER o in archivi o applicazioni autorizzate dall'unità amministrativa. Comunicazione chat, video e audio non autorizzati tramite Teams.	Trattamento, archiviazione e comunicazione chat, video e audio non autorizzati tramite Teams. (non vi è alcuna integrazione con il sistema di crittografia)	Trattamento, archiviazione e comunicazione chat, video e audio non autorizzati tramite Teams. (non vi è alcuna integrazione con il sistema di crittografia)

Tabella 2: Panoramica dell'utilizzo dei servizi M365 in base ai dispositivi

B. Panoramica della terminologia in uso

La direttiva di applicazione E031 riguarda l'utilizzo della piattaforma Microsoft 365 indicata nel grafico qui sotto. Si tratta di una suddivisione schematica tra la piattaforma Microsoft 365 e i servizi di burotica della Confederazione. Il grafico mostra le correlazioni esistenti tra i termini utilizzati nella direttiva.

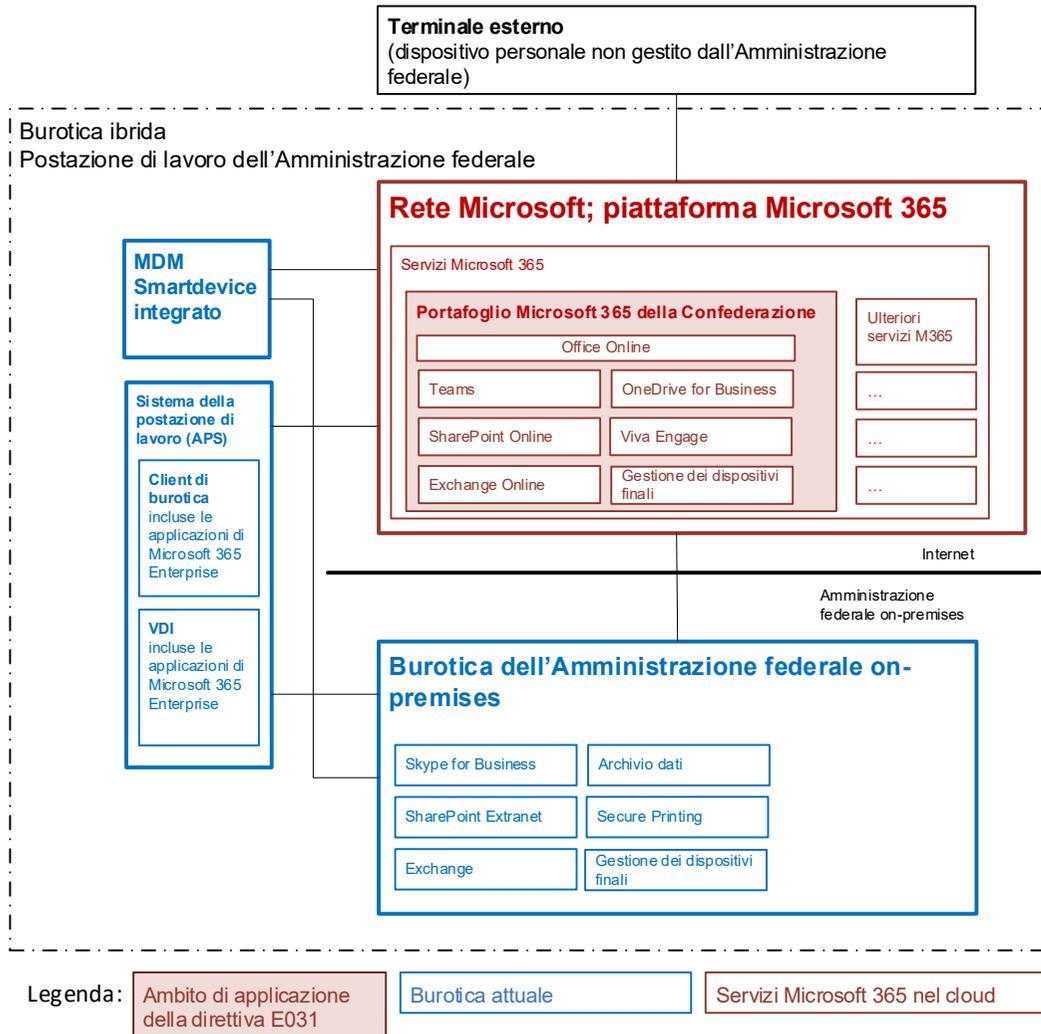


Grafico 1: Panoramica della terminologia

C. Modifiche rispetto alla versione precedente

Adeguamento delle norme sul trattamento in base all'ultima versione dell'OSIn.

D. Significato delle parole chiave relative al grado di obbligatorietà

Il grado di obbligatorietà¹⁴ delle singole disposizioni di cui al numero 2 della presente direttiva è indicato secondo le parole chiave in stampatello elencate qui di seguito.

Parola chiave	Grado di obbligatorietà
DEVE	Disposizione da rispettare obbligatoriamente (salvo le eccezioni autorizzate)
NON DEVE	L'opzione non è ammessa.
PUÒ/È AUTO-RIZZATO	L'opzione è autorizzata espressamente. L'unità amministrativa può decidere se usufruire di tale possibilità. Qualora il requisito riguardi una soluzione TIC, il rispettivo fornitore di tale soluzione deve offrire l'opzione in questione.
DOVREBBE	Opzione da scegliere nei casi normali. Tuttavia, l'unità amministrativa può discostarsi da questa disposizione senza che il settore TDT della CaF o l'UFCS abbiano concesso un'eccezione, a condizione che ciò non metta a rischio l'efficienza economica e/o la sicurezza. L'eccezione deve essere debitamente motivata per iscritto al settore TDT della CaF o l'UFCS.
PUÒ	Opzione ammessa. Qualora il requisito riguardi una soluzione TIC, il rispettivo fornitore di tale soluzione decide se supportare tale opzione.

E. Riferimenti

ID	Riferimento ¹⁵
LPD	Legge federale del 19 giugno 1992 sulla protezione dei dati (LPD; RS 235.1)
E026	E026 – Direttiva d'applicazione sul sistema di postazione di lavoro (disponibile in ted. e franc.)
Ordinanza GEVER	Ordinanza del 3 aprile 2019 sulla gestione elettronica degli affari nell'Amministrazione federale (Ordinanza GEVER; RS 172.010.441)
LSIn	Legge federale del 18 dicembre 2020 sulla sicurezza delle informazioni in seno alla Confederazione (LSIn; RS 128)
OSIn	Ordinanza dell'8 novembre 2023 sulla sicurezza delle informazioni in seno all'Amministrazione federale e all'esercito (OSIn; RS 128.1)
RFC 2119	Request for Comments: 2119 (PCB14), The Internet Engineering Task Force (IETF)
SB000	SB000 – Strategia TIC della Confederazione 2020–2023

¹⁴ Grado di obbligatorietà conforme alle specifiche della *Request of Comments: RFC 2119 (PCB 14), The Internet Engineering Task Force (IETF)*. Tali indicazioni secondo RFC 2119 fanno parte di una prassi consolidata nella definizione di standard internazionali.

¹⁵ Gli atti emanati dall'Assemblea federale sono ordinati nella raccolta sistematica del diritto federale. In caso di riferimento a una direttiva della Confederazione è indicata la versione valida alla data in cui è stata approvata.

ID	Riferimento ¹⁵
SD100 - Catalogo dei servizi standard	Il catalogo dei servizi standard TIC elenca i servizi forniti nonché le relative varianti e opzioni. È destinato in primo luogo ai manager dell'integrazione dei dipartimenti e ai fornitori di prestazioni dei servizi standard. SD100 - Catalogo dei servizi standard
Si001	Si001 - Protezione di base delle TIC nell'Amministrazione federale
Si001-Hi3	Si001 - Hi03: Direttive per evitare i rischi di violazione del segreto d'ufficio nell'Amministrazione federale - Versione 1.4 (disponibile in ted.)
Art. 320 cpv. 1 CP (Segreto d'ufficio)	Il segreto d'ufficio sussiste allorché vi è l'obbligo legale di serbare il segreto e si tratta di fatti che non sono né di dominio pubblico né generalmente accessibili e che non possono essere divulgati a tutela di interessi pubblici e privati.
OTDI	Ordinanza sul coordinamento della trasformazione digitale e la governance delle TIC in seno all'Amministrazione federale (OTDI; RS 172.010.58)

F. Abbreviazioni

Sigla	Significato
CaF	Cancelleria federale
CEBA	Programma di burotica Cloud Enabling
TDT	Settore Trasformazione digitale e governance delle TIC della Cancelleria federale
GEVER	Gestione elettronica degli affari
TIC	Tecnologie dell'informazione e della comunicazione
MDM	Mobile Device Management
UFCS	Ufficio federale della cibersicurezza
RFC	Request for Comments