Identificativo: D04_SCO.1_FASE1(ALL2) Rev. 1.0

Data: 23/03/2021

PROCEDURA RISTRETTA PER L'AFFIDAMENTO DEI SERVIZI DI CLOUD COMPUTING, DI SICUREZZA, DI REALIZZAZIONE DI PORTALI E SERVIZI ON-LINE E DI COOPERAZIONE APPLICATIVA PER LE PUBBLICHE AMMINISTRAZIONI (ID SIGEF 1403)

LOTTO 2

CIG 8025774638

Regione Calabria

Misure tecniche e organizzative

Allegato 1 del deliverable D04_SCO.1_FASE1 "Metodologia della valutazione d'impatto per la protezione dei dati personali (DPIA)"

Raggruppamento Temporaneo di Imprese

composto da:

Leonardo Divisione Cyber Security SpA

IBM SpA

Sistemi Informativi SpA

Fastweb SpA

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
A) Politica generale di sicurezza per la protezione dei dati personali	A.1	La struttura organizzativa dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.	05 Politica di sicurezza	Basso	x	x	x			
A) Politica generale di sicurezza per la protezione dei dati personali	A.2	La politica generale di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.	05 Politica di sicurezza	Basso	x	x	x			
A) Politica generale di sicurezza per la protezione dei dati personali	A.3	La struttura organizzativa dovrebbe documentare separatamente, una politica di sicurezza dedicata al trattamento dei dati personali. La politica dovrebbe essere approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento e alle parti esterne interessate	05 Politica di sicurezza	Medio	x	x	x			
A) Politica generale di sicurezza per la protezione dei dati personali	A.4	La politica di sicurezza dovrebbe almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali.	05 Politica di sicurezza	Medio	x	x	x			
A) Politica generale di sicurezza per la protezione dei dati personali	A.5	Dovrebbe essere creato e mantenuto un inventario di politiche / procedure specifiche relative alla sicurezza dei dati personali, basato sulla politica generale di sicurezza.	05 Politica di sicurezza	Medio	x	x	x			
A) Politica generale di sicurezza per la protezione dei dati personali	A.6	Le politiche di sicurezza dovrebbero essere riviste e corrette, se necessario, su base semestrale.	05 Politica di sicurezza	Alto	x	x	x			
B) Ruoli e responsabilità	B.1	I ruoli e le responsabilità relativi al trattamento dei dati personali dovrebbero essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.	06.01.01 Ruoli e responsabilità per la sicurezza delle informazioni	Basso	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
B) Ruoli e responsabilità	B.2	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, la struttura organizzativa dovrebbe prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento (es . laptop, tablet, smartphone, hd esterni, pen drive, etc.).	06.01.01 Ruoli e responsabilità per la sicurezza delle informazioni	Basso	x	x	x			
B) Ruoli e responsabilità	B.3	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.	06.01.01 Ruoli e responsabilità per la sicurezza delle informazioni	Medio	x	x	x			
B) Ruoli e responsabilità	B.4	Il responsabile della sicurezza dovrebbe essere nominato formalmente (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati.	06.01.01 Ruoli e responsabilità per la sicurezza delle informazioni	Alto	x	x	x			
B) Ruoli e responsabilità	B.5	Compiti e responsabilità in conflitto, ad esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO, dovrebbero essere considerati separatamente per ridurre le ipotesi di modifiche non autorizzate o non intenzionali o un uso improprio di dati personali.	06.01.01 Ruoli e responsabilità per la sicurezza delle informazioni	Alto	x	x	x			
C) Politica per il controllo degli accessi	C.1	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.	09.01.01 Politica di controllo degli accessi	Basso		x	x			
C) Politica per il controllo degli accessi	C.2	Dovrebbe essere dettagliata e documentata una politica di controllo degli accessi. La struttura organizzativa dovrebbe determinare in questo documento le regole di controllo appropriate degli accessi, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nell'ambito dei processi e delle procedure relative ai dati personali.	09.01.01 Politica di controllo degli accessi	Medio		x	x			
C) Politica per il controllo degli accessi	C.3	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).	09.01.01 Politica di controllo degli accessi	Medio		x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
C) Politica per il controllo degli accessi	C.4	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff	09.01.01 Politica di controllo degli accessi	Alto		x	x			
D) Gestione delle risorse / asset	D.1	La struttura organizzativa dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).	08 Gestione delle risorse	Basso	x	x	x			
D) Gestione delle risorse / asset	D.2	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.	08 Gestione delle risorse	Basso	x	x	x			
D) Gestione delle risorse / asset	D.3	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	08 Gestione delle risorse	Medio	x	x	x			
D) Gestione delle risorse / asset	D.4	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.	08 Gestione delle risorse	Alto	x	x	x			
E) Gestione delle modifiche apportare alle risorse, agli apparati e ai sistemi IT	E.1	La struttura organizzativa dovrebbe assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.	12.01 Procedure operative e responsabilità	Basso	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
E) Gestione delle modifiche apportare alle risorse, agli apparati e ai sistemi IT	E.2	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, dovrebbero essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.	12.01 Procedure operative e responsabilità	Basso	x	x	x			
E) Gestione delle modifiche apportare alle risorse, agli apparati e ai sistemi IT	E.3	Dovrebbe essere prevista e applicata una politica interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La politica di gestione delle modifiche dovrebbe essere regolarmente aggiornata.	12.01 Procedure operative e responsabilità	Medio	x	x	x			
F) Responsabili del trattamento	F.1	Le linee guida e le procedure formali relative al trattamento dei dati personali, da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing), dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza della struttura organizzativa.	15 Rapporti con i fornitori	Basso	x	x	x			
F) Responsabili del trattamento	F.2	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.	15 Rapporti con i fornitori	Basso	x	x	x			
F) Responsabili del trattamento	F.3	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.	15 Rapporti con i fornitori	Basso	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
F) Responsabili del trattamento	F.4	La struttura organizzativa dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.	15 Rapporti con i fornitori	Medio	x	x	x			
F) Responsabili del trattamento	F.5	I dipendenti del responsabile del trattamento che stanno trattando dati personali dovrebbero essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.	15 Rapporti con i fornitori	Alto	x	x	x			
G) Gestione degli incidenti / violazioni di dati personali (personal data breaches)	G.1	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.	16 Gestione degli incidenti di sicurezza delle informazioni	Basso	x	x	x			
G) Gestione degli incidenti / violazioni di dati personali (personal data breaches)	G.2	Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) dovrebbero essere segnalate immediatamente al Management competente secondo l'organizzazione interna. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.	16 Gestione degli incidenti di sicurezza delle informazioni	Basso	x	x	x			
G) Gestione degli incidenti / violazioni di dati personali (personal data breaches)	G.3	Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	16 Gestione degli incidenti di sicurezza delle informazioni	Medio	x	x	x			
G) Gestione degli incidenti / violazioni di dati personali (personal data breaches)	G.4	Gli incidenti e le violazioni dei dati personali dovrebbero essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione intraprese.	16 Gestione degli incidenti di sicurezza delle informazioni	Alto	x	x	x			
H) Continuità operativa	H.1	La struttura organizzativa dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).	17 Aspetti di sicurezza nella gestione della continuità operativa	Basso	x					

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
H) Continuità operativa	H.2	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	17 Aspetti di sicurezza nella gestione della continuità operativa	Medio	x					
H) Continuità operativa	H.3	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi fondamentali che attengono alla sicurezza dei dati personali.	17 Aspetti di sicurezza nella gestione della continuità operativa	Medio	x					
H) Continuità operativa	H.4	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.	17 Aspetti di sicurezza nella gestione della continuità operativa	Alto	x					
H) Continuità operativa	H.5	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.	17 Aspetti di sicurezza nella gestione della continuità operativa	Alto	x					
I) Obblighi di confidenzialità	I.1	La struttura organizzativa dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento, comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità dovrebbero essere assegnati e chiaramente comunicati durante il processo di pre-assunzione e / o assunzione.	07 Sicurezza delle risorse umane	Basso	x	x	x			
I) Obblighi di confidenzialità	I.2	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento, dovrebbero essere invitati ad esaminare e condividere le politiche di sicurezza della struttura organizzativa e firmare i rispettivi accordi di riservatezza e di non divulgazione.	07 Sicurezza delle risorse umane	Medio	x	x	x			
I) Obblighi di confidenzialità	I.3	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).	07 Sicurezza delle risorse umane	Alto	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
J) Formazione	J.1	La struttura organizzativa dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.	07.02.02 Consapevolezza, educazione e formazione sulla sicurezza delle informazioni	Basso	x	x	x			
J) Formazione	J.2	La struttura organizzativa dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici per l'introduzione (alle questioni di protezione dei dati) dei nuovi arrivati.	07.02.02 Consapevolezza, educazione e formazione sulla sicurezza delle informazioni	Medio	x	x	x			
J) Formazione	J.3	Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti.	07.02.02 Consapevolezza, educazione e formazione sulla sicurezza delle informazioni	Alto	x	x	x			
K) Controllo degli accessi e autenticazione	K.1	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	09 Controllo degli accessi	Basso		x	x			
K) Controllo degli accessi e autenticazione	K.2	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	09 Controllo degli accessi	Basso		x	x			
K) Controllo degli accessi e autenticazione	K.3	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo dovrebbe essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.	09 Controllo degli accessi	Basso		x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
K) Controllo degli accessi e autenticazione	K.4	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).	09 Controllo degli accessi	Basso		x	x			
K) Controllo degli accessi e autenticazione	K.5	Dovrebbe essere definita e documentata una politica specifica per le password. La politica dovrebbe includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.	09 Controllo degli accessi	Medio		x	x			
K) Controllo degli accessi e autenticazione	K.6	Le password degli utenti dovrebbero essere memorizzate in una forma "hash".	09 Controllo degli accessi	Medio		x	x			
K) Controllo degli accessi e autenticazione	K.7	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.	09 Controllo degli accessi	Alto		x	x			
K) Controllo degli accessi e autenticazione	K.8	Dovrebbe essere soggetto ad autenticazione ogni dispositivo (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale	09 Controllo degli accessi	Alto		x	x			
L) Generazione di file di log e monitoraggio	L.1	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	12.04 Registrazione e monitoraggio	Basso	x	x	x			
L) Generazione di file di log e monitoraggio	L.2	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento	12.04 Registrazione e monitoraggio	Basso	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
L) Generazione di file di log e monitoraggio	L.3	Le azioni degli amministratori di sistema e degli operatori di sistema, incluse l'aggiunta / cancellazione / modifica dei diritti dell'utente, dovrebbero essere registrate.	12.04 Registrazione e monitoraggio	Medio	x	x	x			
L) Generazione di file di log e monitoraggio	L.4	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.	12.04 Registrazione e monitoraggio	Medio	x	x	x			
L) Generazione di file di log e monitoraggio	L.5	Un sistema di monitoraggio dovrebbe elaborare i file log, produrre report sullo stato del sistema e notificare potenziali allarmi.	12.04 Registrazione e monitoraggio	Medio	x	x	x			
M) Sicurezza dei server e dei database	M.1	I server ove risiedono database e applicazioni dovrebbero essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	12 Sicurezza delle operazioni	Basso	x	x	x			
M) Sicurezza dei server e dei database	M.2	I server ove risiedono database e applicazioni dovrebbero trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).	12 Sicurezza delle operazioni	Basso	x	x	x			
M) Sicurezza dei server e dei database	M.3	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.	12 Sicurezza delle operazioni	Medio	x	x	x			
M) Sicurezza dei server e dei database	M.4	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.	12 Sicurezza delle operazioni	Medio	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
M) Sicurezza dei server e dei database	M.5	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni	12 Sicurezza delle operazioni	Medio	x	x	x			
M) Sicurezza dei server e dei database	M.6	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.	12 Sicurezza delle operazioni	Alto	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.1	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	14.01 Requisiti di sicurezza dei sistemi informativi	Basso	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.2	Le applicazioni anti-virus e le firme di rilevamento dovrebbero essere configurate su base settimanale.	14.01 Requisiti di sicurezza dei sistemi informativi	Basso	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.3	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	14.01 Requisiti di sicurezza dei sistemi informativi	Basso	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.4	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	14.01 Requisiti di sicurezza dei sistemi informativi	Basso	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.5	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo dovrebbero essere installati regolarmente.	14.01 Requisiti di sicurezza dei sistemi informativi	Basso	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
N) Sicurezza delle postazioni di lavoro	N.6	Le applicazioni antivirus e le firme di rilevamento dovrebbero essere configurate su base giornaliera.	14.01 Requisiti di sicurezza dei sistemi informativi	Medio	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.7	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).	14.01 Requisiti di sicurezza dei sistemi informativi	Alto	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.8	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.	14.01 Requisiti di sicurezza dei sistemi informativi	Alto	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.9	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.	14.01 Requisiti di sicurezza dei sistemi informativi	Alto	x	x	x			
O) Sicurezza della rete e delle comunicazioni elettroniche	O.1	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione dovrebbe essere crittografata tramite protocolli crittografici (TLS / SSL).	13 Sicurezza delle comunicazioni	Basso	x	x	x			
O) Sicurezza della rete e delle comunicazioni elettroniche	O.2	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.	13 Sicurezza delle comunicazioni	Medio	x	x	x			
O) Sicurezza della rete e delle comunicazioni elettroniche	O.3	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica della struttura organizzativa (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.	13 Sicurezza delle comunicazioni	Medio	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
O) Sicurezza della rete e delle comunicazioni elettroniche	O.4	Il traffico da e verso il sistema IT dovrebbe essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.	13 Sicurezza delle comunicazioni	Medio	x	x	x			
O) Sicurezza della rete e delle comunicazioni elettroniche	O.5	La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate per il trattamento dei dati personali.	13 Sicurezza delle comunicazioni	Alto	x	x	x			
O) Sicurezza della rete e delle comunicazioni elettroniche	O.6	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.	13 Sicurezza delle comunicazioni	Alto	x	x	x			
O) Sicurezza della rete e delle comunicazioni elettroniche	O.7	L'accesso al sistema IT dovrebbe essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC)	13 Sicurezza delle comunicazioni	Alto	x	x	x			
P) Back-up	P.1	Le procedure di back-up e ripristino dei dati dovrebbero essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	12.03 Back-up	Basso	x	x				
P) Back-up	P.2	Ai back-up dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	12.03 Back-up	Basso	x	x				
P) Back-up	P.3	L'esecuzione dei back-up dovrebbe essere monitorata per garantire che venga completata.	12.03 Back-up	Basso	x	x				

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
P) Back-up	P.4	Dovrebbero essere eseguiti regolarmente back-up completi.	12.03 Back-up	Basso	x	x				
P) Back-up	P.5	I supporti di back-up dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.	12.03 Back-up	Medio	x	x				
P) Back-up	P.6	I back-up incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.	12.03 Back-up	Medio	x	x				
P) Back-up	P.7	Le copie di back-up dovrebbero essere conservate in modo sicuro in luoghi diversi.	12.03 Back-up	Medio	x	x				
P) Back-up	P.8	Se viene utilizzato un servizio di terze parti per l'archiviazione di back-up, la copia dovrebbe essere crittografata prima di essere trasmessa dal titolare del trattamento.	12.03 Back-up	Medio	x	x				
P) Back-up	P.9	Le copie dei back-up dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.	12.03 Back-up	Alto	x	x				
Q) Dispositivi mobili / portatili	Q.1	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	06.02 Dispositivi mobili e telelavoro	Basso	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
Q) Dispositivi mobili / portatili	Q.2	I dispositivi mobili, ai quali è consentito accedere al sistema informativo, dovrebbero essere pre-registrati e pre-autorizzati.	06.02 Dispositivi mobili e telelavoro	Basso	x	x	x			
Q) Dispositivi mobili / portatili	Q.3	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.	06.02 Dispositivi mobili e telelavoro	Basso	x	x	x			
Q) Dispositivi mobili / portatili	Q.4	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.	06.02 Dispositivi mobili e telelavoro	Medio	x	x	x			
Q) Dispositivi mobili / portatili	Q.5	La struttura organizzativa dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.	06.02 Dispositivi mobili e telelavoro	Medio	x	x	x			
Q) Dispositivi mobili / portatili	Q.6	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso compartimentazioni software sicure.	06.02 Dispositivi mobili e telelavoro	Medio	x	x	x			
Q) Dispositivi mobili / portatili	Q.7	I dispositivi mobili dovrebbero essere fisicamente protetti contro il furto quando non sono in uso.	06.02 Dispositivi mobili e telelavoro	Medio	x	x	x			
Q) Dispositivi mobili / portatili	Q.8	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte)	06.02 Dispositivi mobili e telelavoro	Alto	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
Q) Dispositivi mobili / portatili	Q.9	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.	06.02 Dispositivi mobili e telelavoro	Alto	x	x	x			
R) Sicurezza nel ciclo di vita delle applicazioni	R.1	Durante il ciclo di vita dello sviluppo, dovrebbero essere seguite le best practice, lo stato dell'arte e ben noti pratiche di sviluppo sicuro, framework o standard.	12.06 Gestione delle vulnerabilità tecniche e 14.02 Sicurezza nei processi di sviluppo e supporto	Basso	x	x	x			
R) Sicurezza nel ciclo di vita delle applicazioni	R.2	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	12.06 Gestione delle vulnerabilità tecniche e 14.02 Sicurezza nei processi di sviluppo e supporto	Basso	x	x	x			
R) Sicurezza nel ciclo di vita delle applicazioni	R.3	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET)) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	12.06 Gestione delle vulnerabilità tecniche e 14.02 Sicurezza nei processi di sviluppo e supporto	Basso	x	x	x			
R) Sicurezza nel ciclo di vita delle applicazioni	R.4	Dovrebbero essere seguiti standard e pratiche di codifica sicure.	12.06 Gestione delle vulnerabilità tecniche e 14.02 Sicurezza nei processi di sviluppo e supporto	Basso	x	x	x			
R) Sicurezza nel ciclo di vita delle applicazioni	R.5	Durante le attività di sviluppo, dovrebbero essere eseguite attività di test e convalida dei requisiti di sicurezza inizialmente implementati.	12.06 Gestione delle vulnerabilità tecniche e 14.02 Sicurezza nei processi di sviluppo e supporto	Basso	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
R) Sicurezza nel ciclo di vita delle applicazioni	R.6	Vulnerability assessment e penetration test su applicazioni e infrastrutture dovrebbero essere eseguiti da una terza parte fidata prima di procedere con la loro adozione operativa. L'applicazione non dovrebbe essere adottata fino a quando non si raggiunga il livello di sicurezza richiesto.	12.06 Gestione delle vulnerabilità tecniche e 14.02 Sicurezza nei processi di sviluppo e supporto	Medio	x	x	x			
R) Sicurezza nel ciclo di vita delle applicazioni	R.7	I penetration test dovrebbero essere eseguiti periodicamente.	12.06 Gestione delle vulnerabilità tecniche e 14.02 Sicurezza nei processi di sviluppo e supporto	Medio	x	x	x			
R) Sicurezza nel ciclo di vita delle applicazioni	R.8	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.	12.06 Gestione delle vulnerabilità tecniche e 14.02 Sicurezza nei processi di sviluppo e supporto	Medio	x	x	x			
R) Sicurezza nel ciclo di vita delle applicazioni	R.9	Le patch software dovrebbero essere testate e valutate prima di essere installate in un ambiente operativo.	12.06 Gestione delle vulnerabilità tecniche e 14.02 Sicurezza nei processi di sviluppo e supporto	Medio	x	x	x			
S) Cancellazione / eliminazione dei dati	S.1	La sovrascrittura software dei dati dovrebbe essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), è necessario eseguire la distruzione fisica.	08.03.02 Smaltimento dei supporti e 11.02.07 Smaltimento o riutilizzo sicuro dell'attrezzatura	Basso	x	x	x			

Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
S) Cancellazione / eliminazione dei dati	S.2	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.	08.03.02 Smaltimento dei supporti e 11.02.07 Smaltimento o riutilizzo sicuro dell'attrezzatura	Basso	x	x	x			
S) Cancellazione / eliminazione dei dati	S.3	Dovrebbero essere eseguiti più passaggi di sovrascrittura basata su software, su tutti i supporti, prima di essere smaltiti.	08.03.02 Smaltimento dei supporti e 11.02.07 Smaltimento o riutilizzo sicuro dell'attrezzatura	Medio	x	x	x			
S) Cancellazione / eliminazione dei dati	S.4	Se sono utilizzati servizi di terze parti per smaltire in modo sicuro supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre, ove opportuno, un verbale di distruzione dei record.	08.03.02 Smaltimento dei supporti e 11.02.07 Smaltimento o riutilizzo sicuro dell'attrezzatura	Medio	x	x	x			
S) Cancellazione / eliminazione dei dati	S.5	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.	08.03.02 Smaltimento dei supporti e 11.02.07 Smaltimento o riutilizzo sicuro dell'attrezzatura	Alto	x	x	x			
S) Cancellazione / eliminazione dei dati	S.6	Se è una terza parte, (quindi un responsabile del trattamento) ad occuparsi della distruzione di supporti o file cartacei, il processo si dovrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento all'esterno dei dati personali.	08.03.02 Smaltimento dei supporti e 11.02.07 Smaltimento o riutilizzo sicuro dell'attrezzatura	Alto	x	x	x			
T) Sicurezza fisica	T.1	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.	11 Sicurezza fisica e ambientale	Basso	x	x	x			

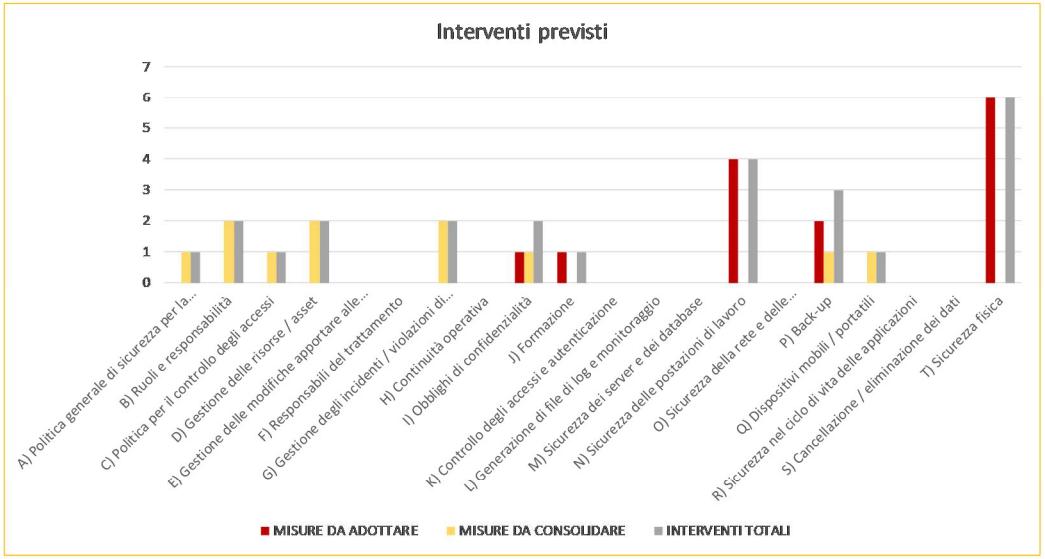
Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
T) Sicurezza fisica	T.2	Identificazione chiara, tramite mezzi appropriati, ad es. i badge identificativi, per tutto il personale e i visitatori che accedono ai locali della struttura organizzativa, dovrebbero essere stabiliti, a seconda dei casi.	11 Sicurezza fisica e ambientale	Medio	x	x	x			
T) Sicurezza fisica	T.3	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi dovrebbero essere mantenuti e monitorati in modo sicuro.	11 Sicurezza fisica e ambientale	Medio	x	x	x			
T) Sicurezza fisica	T.4	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.	11 Sicurezza fisica e ambientale	Medio	x	x	x			
T) Sicurezza fisica	T.5	Se del caso, dovrebbero essere costruite barriere fisiche per impedire l'accesso fisico non autorizzato.	11 Sicurezza fisica e ambientale	Medio	x	x	x			
T) Sicurezza fisica	T.7	Un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS) dovrebbero essere attivati nella sala server.	11 Sicurezza fisica e ambientale	Medio	x	x	x			
T) Sicurezza fisica	T.8	Il personale di servizio di supporto esterno dovrebbe avere accesso limitato alle aree protette.	11 Sicurezza fisica e ambientale	Medio	x	x	x			

Figura 1 Set di misure[1] tecniche e organizzative

[1] Misure tratte dal "Manuale ENISA (Agenzia dell'Unione europea per la cibersicurezza) sulla Sicurezza nel trattamento dei dati personali", opportunamente adattate al contesto e integrate con informazioni aggiuntive.

DASHBOARD PER IL TRATTAMENTO DEL RISCHIO

AREE DI INTERVENTO	MISURE DA ADOTTARE	MISURE DA CONSOLIDARE	INTERVENTI TOTALI
A) Politica generale di sicurezza per la protezione dei dati personali	0	1	1
B) Ruoli e responsabilità	0	2	2
C) Politica per il controllo degli accessi	0	1	1
D) Gestione delle risorse / asset	0	2	2
E) Gestione delle modifiche apportare alle risorse, agli apparati e ai sistemi IT	0	0	0
F) Responsabili del trattamento	0	0	0
G) Gestione degli incidenti / violazioni di dati personali (personal data breaches)	0	2	2
H) Continuità operativa	0	0	0
I) Obblighi di confidenzialità	1	1	2
J) Formazione	1	0	1
K) Controllo degli accessi e autenticazione	0	0	0
L) Generazione di file di log e monitoraggio	0	0	0
M) Sicurezza dei server e dei database	0	0	0
N) Sicurezza delle postazioni di lavoro	4	0	4
O) Sicurezza della rete e delle comunicazioni elettroniche	0	0	0
P) Back-up	2	1	3
Q) Dispositivi mobili / portatili	0	1	1
R) Sicurezza nel ciclo di vita delle applicazioni	0	0	0
S) Cancellazione / eliminazione dei dati	0	0	0
T) Sicurezza fisica	6	0	6
	14	11	25



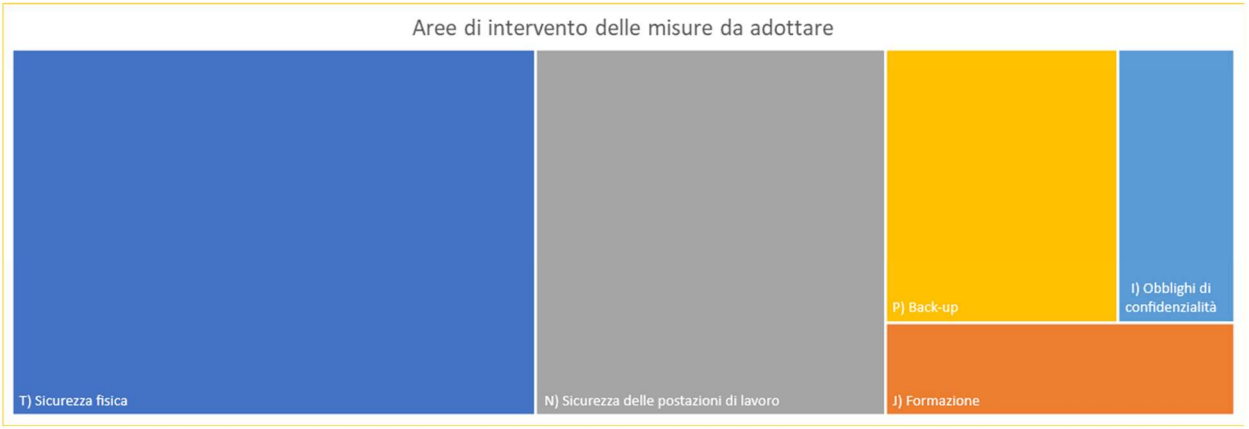


Figura 2 Visualizzazione di esempio della dashboard per il trattamento del rischio inclusa nel tool ARIEC