



VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI GDPR 2016/679

Istituto Comprensivo "Teresa Sarti" LEIC8AD00C

Scuola dell'Infanzia – Scuola Primaria – Scuola secondaria di 1°grado

SEDE LEGALE	Istituto Comprensivo "Teresa Sarti" p.zza Giovanni XXIII, 13 – 73020 – Campi S.na – LE C.F. 93115530755 Tel. 0832 791133 - Fax 0832 1831627 e-mail: leic8ad00c@istruzione.it - pec: leic8ad00c@pec.istruzione.it
Data di revisione	08/10/2018

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

- a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

ALGORITMO VALUTAZIONE

1° STEP: identificazione dei trattamenti

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),

- termine cancellazione dati, □ eventuale trasferimento paesi terzi, □ misure di sicurezza.

2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento (**C**). Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$LR = P \times C$$

LR = livello di rischio

P = probabilità di accadimento

C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

	PROBABILITA' DELL'EVENTO
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze (C)** è associato un indice numerico rappresentato nella seguente tabella:

	CONSEGUENZE
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

P r o b a b i l i t à	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
Conseguenze						

Entità Rischio	Valori di riferimento
Accettabile	$(1 \leq LR \leq 3)$
Medio - basso	$(4 \leq LR \leq 6)$
Rilevante	$(8 \leq LR \leq 12)$
Alto	$(15 \leq LR \leq 25)$

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

3 STEP: DPIA – valutazione del rischio normalizzato

Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevedono due o più criteri di obbligo DPIA.

Nel caso in cui, quindi, l'indice di rischio si colloca nel range $15 \div 25$, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.

La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

$$RN = f(P, C, Vu)$$

Dove:

P = probabilità

C = conseguenze generate dall'evento

$$RN = f (P, C, Vu)$$



V = vulnerabilità rispetto al grado di adeguatezza delle misure

In prima battuta viene ricavato il rischio intrinseco R_i come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

Alla **probabilità P** è associato un indice numerico rappresentato nella seguente tabella:

	Probabilità
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle **conseguenze (C)** è associato un indice numerico rappresentato nella seguente tabella:

	CONSEGUENZE
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

P R O B A B I L I T À	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO	
Ri = P x C	Valori di riferimento
Molto basso	$(1 \leq Ri \leq 2)$
Basso	$(3 \leq Ri \leq 4)$
Rilevante	$(6 \leq Ri \leq 9)$
Alto	$(12 \leq Ri \leq 16)$

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi. Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	<ul style="list-style-type: none"> Perdita Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> Perdita Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	<ul style="list-style-type: none"> Perdita Distruzione non autorizzata Modifica non autorizzata Divulgazione non autorizzata Accesso dati non autorizzato
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> Perdita Distruzione non autorizzata Modifica non autorizzata Divulgazione non autorizzata Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> Perdita Distruzione non autorizzata Modifica non autorizzata Divulgazione non autorizzata Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	<ul style="list-style-type: none"> Perdita Distruzione non autorizzata Modifica non autorizzata Divulgazione non autorizzata Accesso dati non autorizzato

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla **Vulnerabilità** (Vu) è associato un indice numerico rappresentato nella seguente tabella:

	VULNERABILITA'	Valore
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

Vu	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
Ri					

RISCHIO NORMALIZZATO	
RN = Ri x Vu	Valori di riferimento
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Alto	$12 \leq RN \leq 16$

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia **ALTA**, il Titolare attiva l'iter di consultazione del Garante.

RISULTATI DPIA

L'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati è rilevabile dal "REGISTRO DELLE ATTIVITA' PER IL TRATTAMENTO DEI DATI"

Elenco attività sottoposte a DPIA

- Alunni
- Personale ATA e Docenti
- Fornitori

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Dispositivi antincendio	<ul style="list-style-type: none"> • Agenti fisici (incendio, allagamento, attacchi esterni) 	Adeguate

E' applicata una gestione della password degli utenti	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
E' applicata una procedura per la gestione degli accessi	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate
E' eseguita la DPIA	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
E' presenta una politica per la sicurezza e la protezione dei dati	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) 	Adeguate
Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati	<ul style="list-style-type: none"> • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate
Esistono procedure per l'individuazione del custode delle password	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
I dati sono crittografati	<ul style="list-style-type: none"> • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
I documenti vengono firmati digitalmente	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate

I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	<ul style="list-style-type: none"> • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) 	Adeguate
Le password sono costituite da almeno otto caratteri alfanumerici	<ul style="list-style-type: none"> • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Le password sono modificate ogni 3 mesi	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Le procedure sono riesaminate con cadenza predefinita	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate
L'impianto elettrico è certificato ed a norma	<ul style="list-style-type: none"> • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) 	Adeguate
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Registrazione e deregistrazione degli utenti	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) 	Adeguate
Sistemi di allarme e di sorveglianza anti-intrusione	<ul style="list-style-type: none"> • Agenti fisici (incendio, allagamento, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) 	Adeguate

Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti	<ul style="list-style-type: none"> • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Sono applicate regole per la gestione delle password.		Adeguate
Sono definiti i ruoli e le responsabilità	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Sono gestiti i back up	<ul style="list-style-type: none"> • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate
Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili	<ul style="list-style-type: none"> • Agenti fisici (incendio, allagamento, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Sono utilizzati software antivirus e anti intrusione	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Vengono registrati e conservati i Log file	<ul style="list-style-type: none"> • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Viene eseguita opportuna manutenzione	<ul style="list-style-type: none"> • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Gravi	Basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Basso	0,25	Molto basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		

RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

A valle della DPIA l'attività risulta a rischio **Basso**