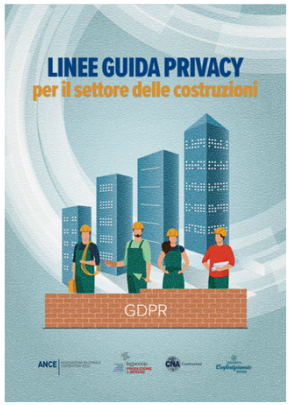
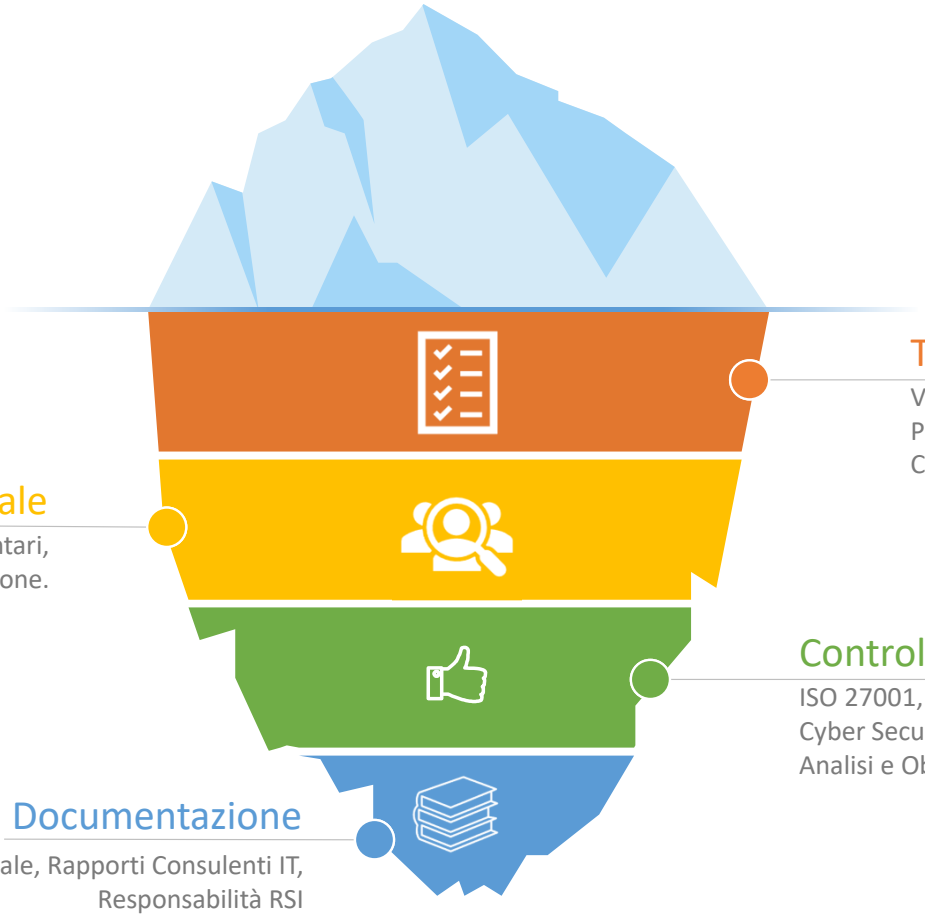

SQuadra-Privacy
Presentazione Aprile 2024

Linee Guida Privacy per le imprese Edili





Trattamenti

Valutazione impatto,
Progettazione e impostazioni,
Criticità e Rischi

Analisi aziendale

Conformità, Minacce, Inventari,
Responsabili esterni, Formazione.

Controlli

ISO 27001, Italia Digitale,
Cyber Security Report.
Analisi e Obiettivi.

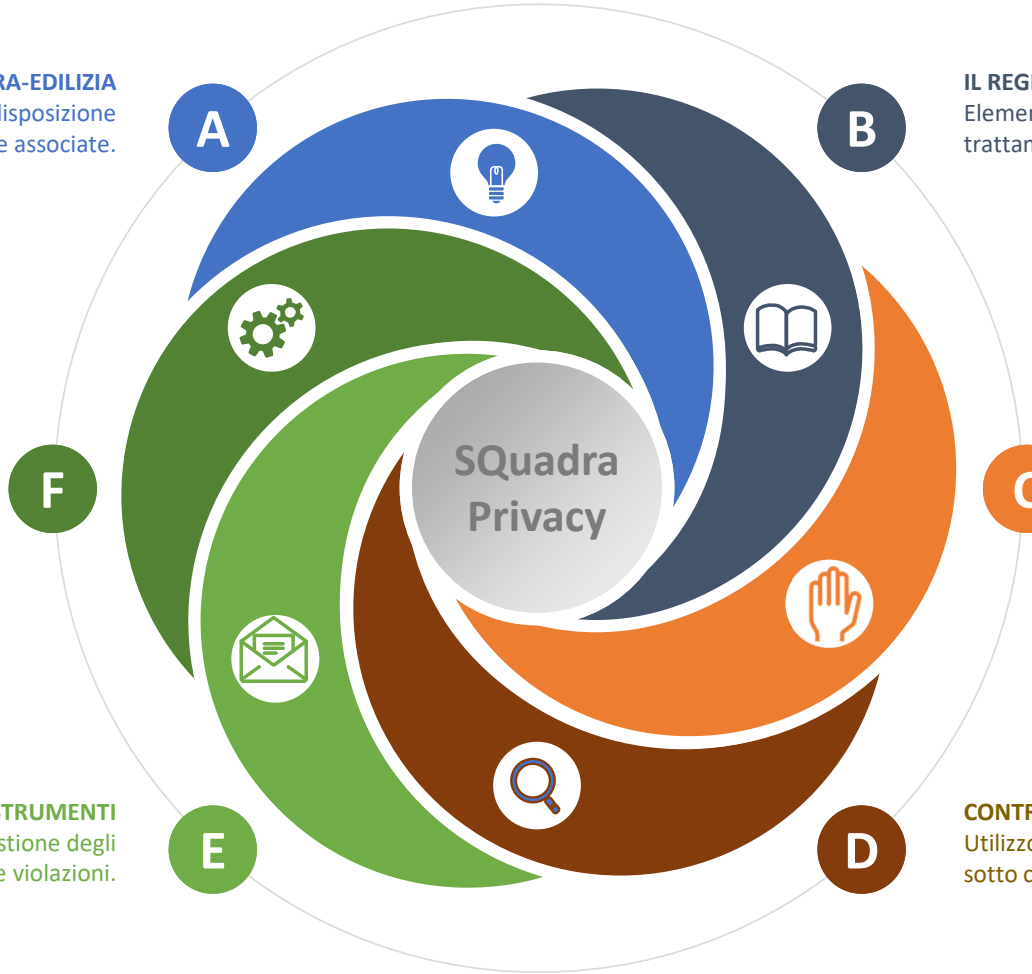
Documentazione

Manuale, Rapporti Consulenti IT,
Responsabilità RSI

SQuadra-Privacy

IL PROGETTO SQUADRA-EDILIZIA
Dal 2008 uno strumento a disposizione delle imprese associate.

IL REGISTRO DEI TRATTAMENTI
Elemento essenziale per l'analisi dei trattamenti effettuati.



SICUREZZA DELLE INFORMAZIONI
Problematiche tipiche e specifiche relative all'utilizzo delle nuove tecnologie.

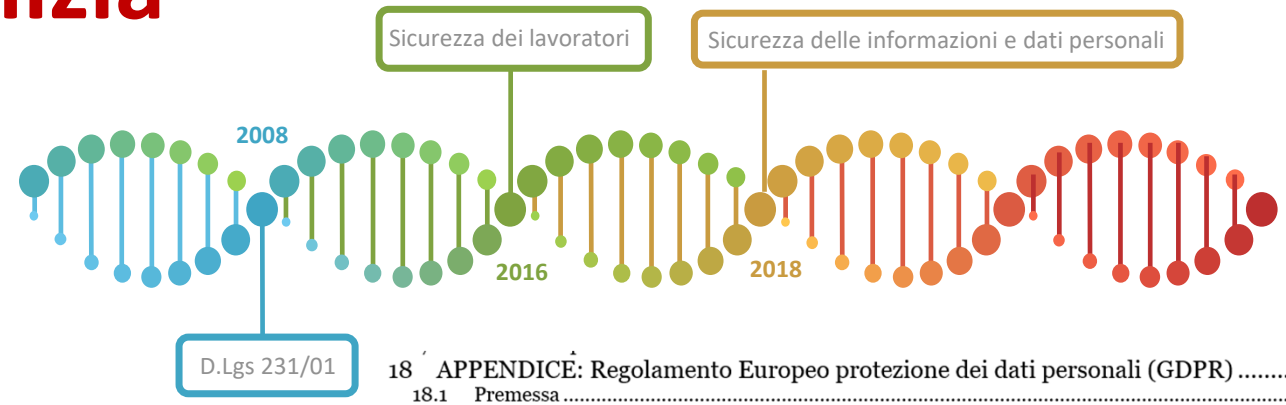
CONFORMITÀ E MINACCE
Autovalutazione della situazione di partenza e degli obiettivi.

ALTRI STRUMENTI
Documenti aggiuntivi e gestione degli incidenti e delle violazioni.

CONTROLLI
Utilizzo delle migliori pratiche per tenere sotto controllo i sistemi informatici.

SQuadra Edilizia

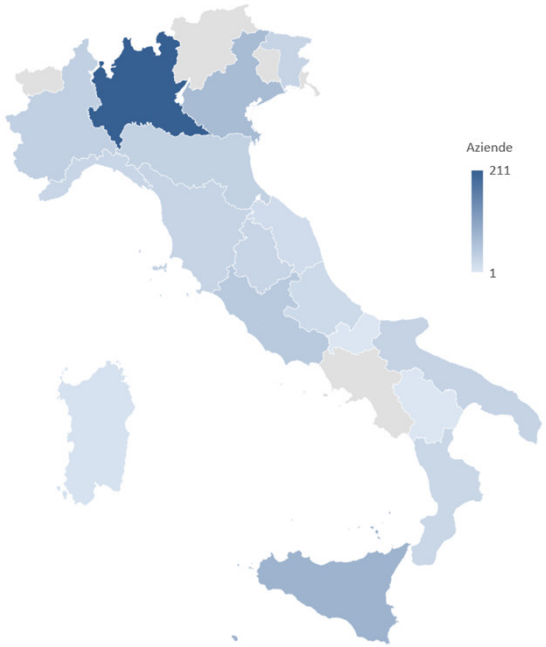
ANCE | ASSOCIAZIONE NAZIONALE COSTRUTTORI EDILI

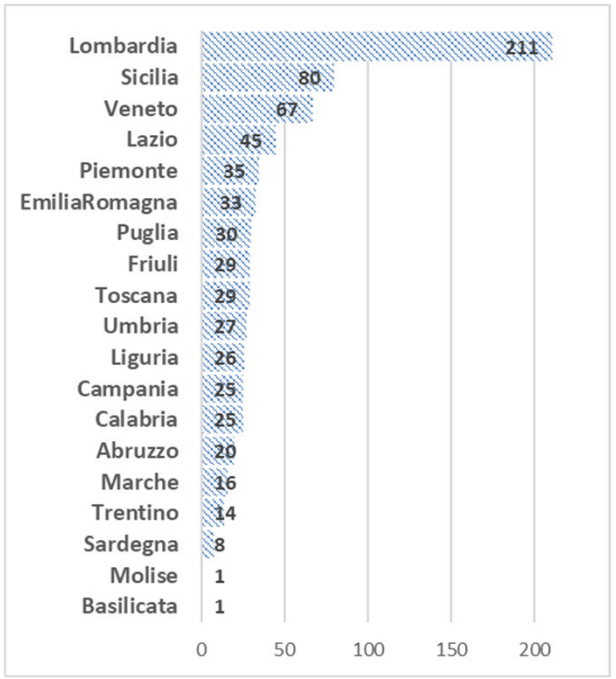


Raccolta di documentazione di supporto.

18 APPENDICE: Regolamento Europeo protezione dei dati personali (GDPR)
18.1 Premessa
18.2 Il Regolamento Europeo
18.2.1 Principi applicabili al trattamento dei dati [Art.5]
18.2.2 Informative e consenso.
18.2.3 Gestione delle violazioni.
18.2.4 Titolari e Responsabili della protezione dei dati.
18.2.5 I codici di condotta.
18.3 Criteri per determinare la necessità di effettuare una Valutazione Impatto Privacy (PIA)
18.4 Glossario predisposto da Confindustria per il Registro delle attività di Trattamento
19 APPENDICE: Sistema di Gestione per la Sicurezza delle Informazioni
19.1 Norma ISO 27001
19.2 Rischi
19.3 Eventi indesiderati.
20 APPENDICE: Controlli sui Sistemi Informativi
20.1 Norma ISO 27001
20.2 Norma ISO 27002:2022
20.3 Norma ISO 27701:2021
20.4 Agenzia per l'Italia Digitale
20.5 Framework Nazionale per la Cyber Security".
20.6 Controlli essenziali 2016
21 APPENDICE: Linee Guida ENISA sulla sicurezza dei dati personali
21.1 Introduzione
21.1.1 La Sicurezza delle informazioni
21.1.2 Gestione del Rischio
21.1.3 Obblighi di sicurezza nel GDPR
21.2 Valutazione dei Rischi per la sicurezza dei dati personali
22 APPENDICE: Protezione dei dati per progettazione e per impostazione predefinita
23 APPENDICE: Misure organizzative e tecniche per prevenire/mitigare violazioni
24 APPENDICE: Valutazione della gravità di una violazione

Credenziali





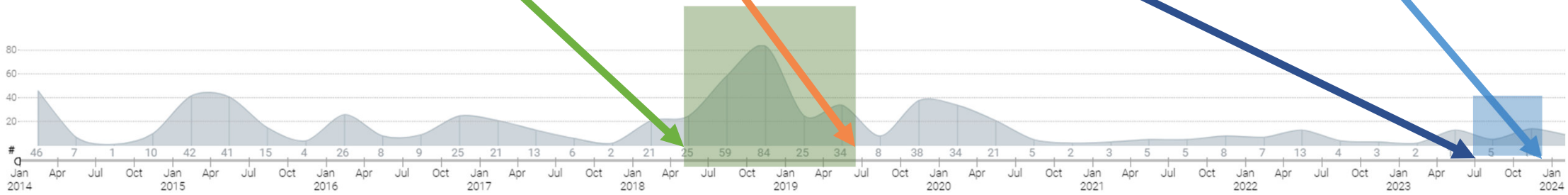
Sanzioni complete
19/5/2019

Regolamento applicabile
25/5/2018

Date di rilascio delle oltre 700 credenziali su tutto il territorio nazionale

Canali per Segnalazioni
Oltre 250 lavoratori
15/7/2023

Canali per Segnalazioni
Oltre 50 lavoratori o 231
17/12/2023



SQuadra

Fornitura del software applicativo «SQuadra» in modalità SaaS (Software as a Service) e la gestione delle relative informazioni.

Software come servizio, è un modello di distribuzione del software applicativo dove un produttore di software sviluppa, opera (direttamente o tramite terze parti) e gestisce un'applicazione web che mette a disposizione dei propri clienti via Internet (cloud computing).

DNV·GL

MANAGEMENT SYSTEM CERTIFICATE

Certificato no./Certificate No.: 281848-2019-AIS-ITA-ACCREDIA

Data prima emissione/Initial date: 27 febbraio 2019

Validità:/Valid: 27 febbraio 2019 - 27 febbraio 2022

Si certifica che il sistema di gestione di/This is to certify that the management system of

IL TIGLIO S.r.l.
Viale della Repubblica, 141 - 59100 Prato (PO) - Italy

È conforme ai requisiti della norma per il Sistema di Gestione/
Has been found to conform to the Management System standard:
ISO/IEC 27001:2013

Questa certificazione è valida per il seguente campo applicativo:

Fornitura del software applicativo "SQuadra" in modalità SaaS (Software as a Service) e gestione delle relative informazioni
(EA: 33)
In accordo con la Dichiarazione di Applicabilità, versione del 04 febbraio 2019

This certificate is valid for the following scope:

Supply of "SQuadra" application software in SaaS (Software as a Service) mode and management of related information
(EA: 33)
In accordance with the Statement of Applicability, version of 04 february 2019

Luogo e Data/Place and date:
Vimercate (MB), 27 febbraio 2019

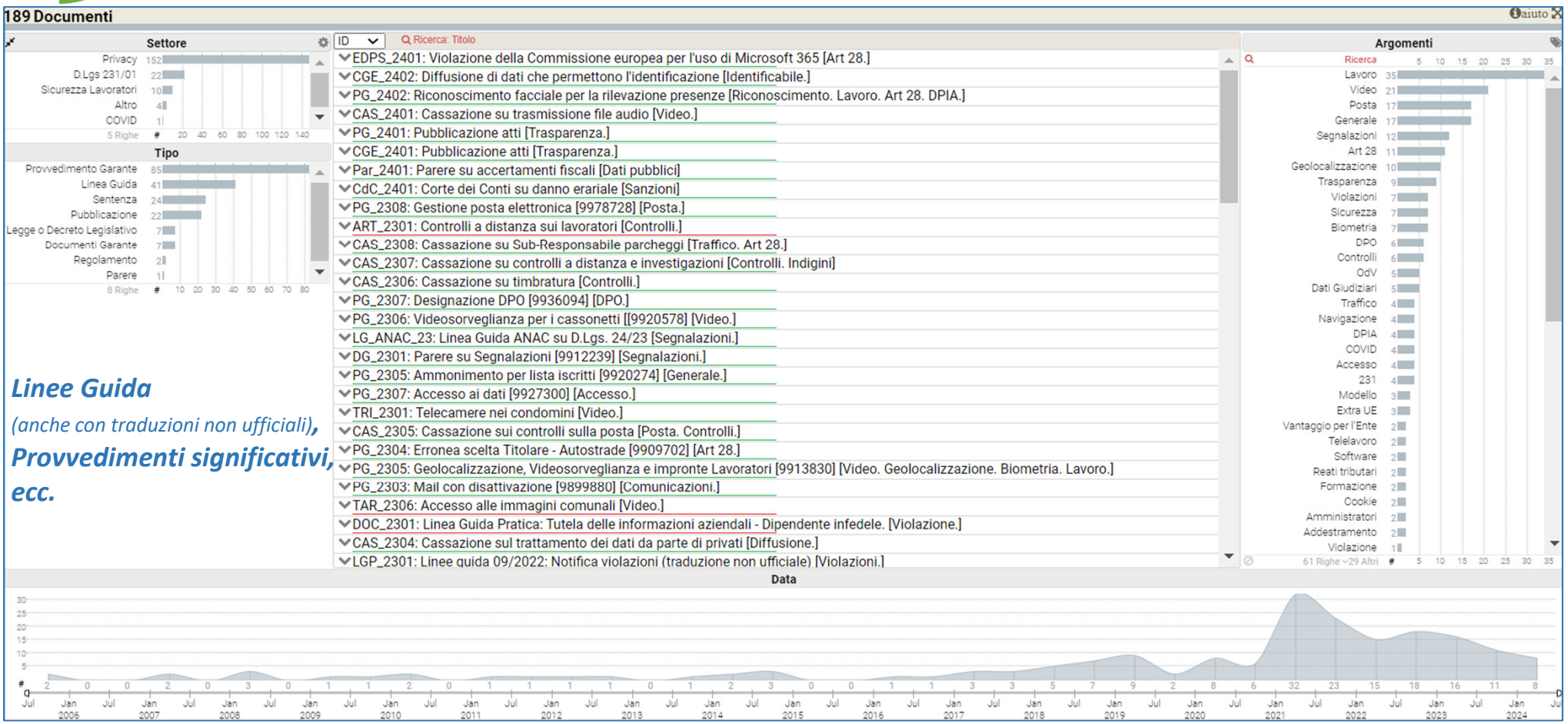
ACCREDIA

Per l'Organismo di Certificazione/
For the Certification Body
DNV GL – Business Assurance
Via Energy Park, 14 - 20871 Vimercate (MB) - Italy

Zeno Beltrami
Management Representative

La validità del presente Certificato è subordinata al rispetto delle condizioni contenute nel Contratto di Certificazione/
Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.
DNV GL Business Assurance Italia S.r.l., Via Energy Park, 14 - 20871 Vimercate (MB) - Italy. TEL:039 68 99 905. www.dnvgl.it

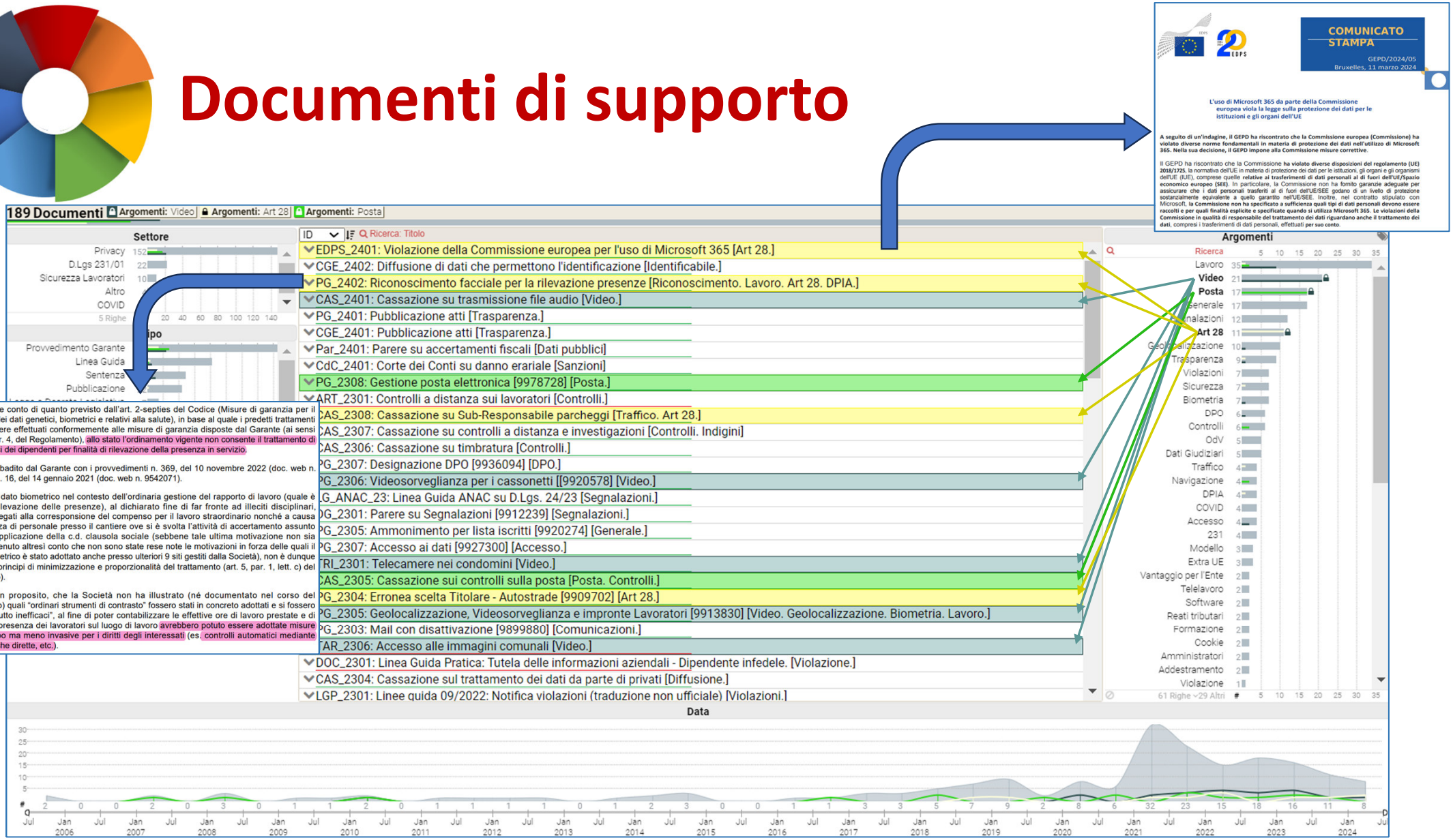
Documenti di supporto



Linee Guida

(anche con traduzioni non ufficiali), ***Provvedimenti significativi, ecc.***

Documenti di supporto



Tenuto anche conto di quanto previsto dall'art. 2-septies del Codice (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute), in base al quale i predetti trattamenti possono essere effettuati conformemente alle misure di garanzia disposte dal Garante (ai sensi dell'art. 9, par. 4, del Regolamento), allo stato l'ordinamento vigente non consente il trattamento di dati biometrici dei dipendenti per finalità di rilevazione della presenza in servizio.

Ciò è stato ribadito dal Garante con i provvedimenti n. 369, del 10 novembre 2022 (doc. web n. 9832838) e n. 16, del 14 gennaio 2021 (doc. web n. 9542071).

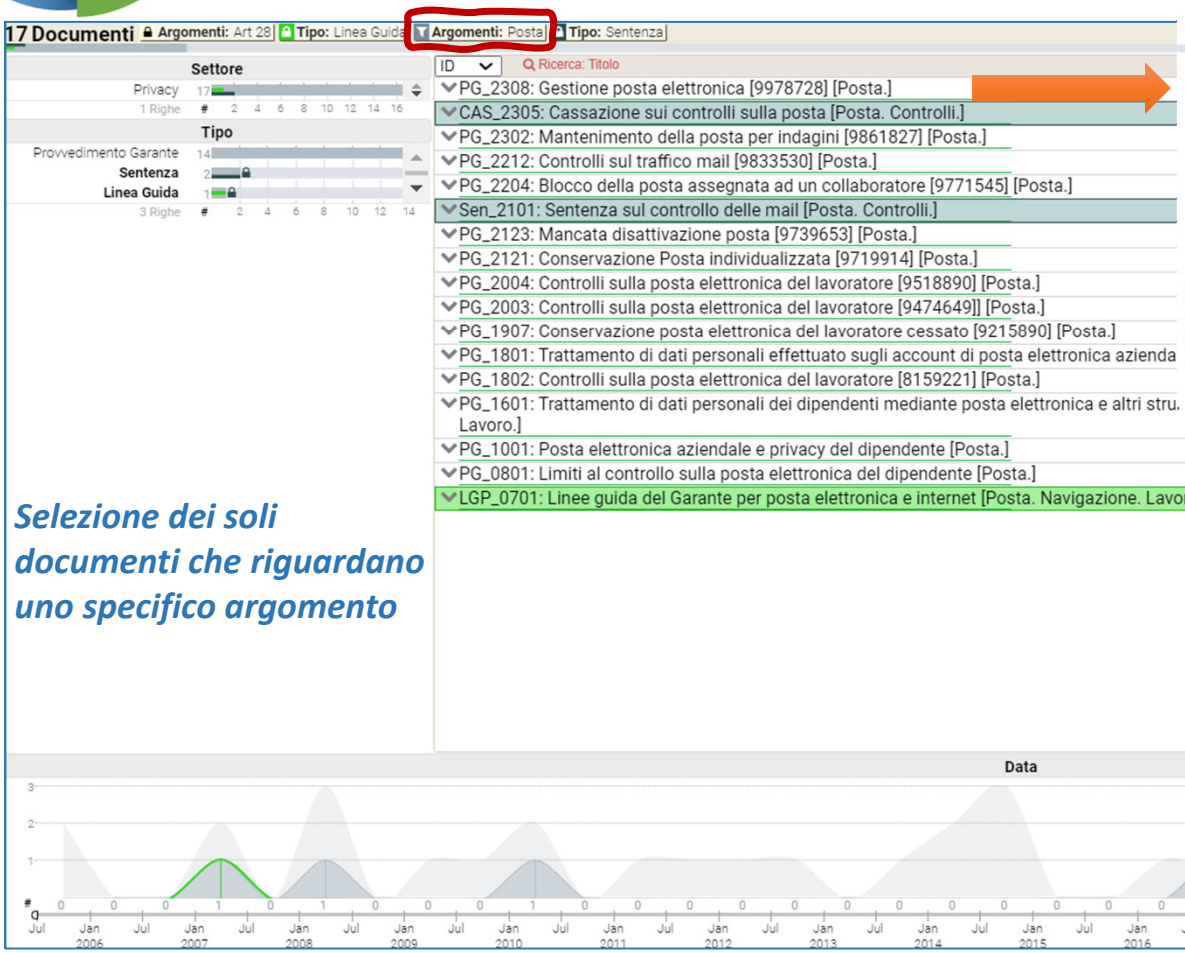
L'utilizzo del dato biometrico nel contesto dell'ordinaria gestione del rapporto di lavoro (quale è l'attività di rilevazione delle presenze), al dichiarato fine di far fronte ad illeciti disciplinari, contenziosi legati alla corresponsione del compenso per il lavoro straordinario nonché a causa della presenza di personale presso il cantiere ove si è svolta l'attività di accertamento assunto mediante l'applicazione della c.d. clausola sociale (sebbene tale ultima motivazione non sia conferente, tenuto altresì conto che non sono state rese note le motivazioni in forza delle quali il sistema biometrico è stato adottato anche presso ulteriori 9 siti gestiti dalla Società), non è dunque conforme ai principi di minimizzazione e proporzionalità del trattamento (art. 5, par. 1, lett. c) del Regolamento).

Premesso, in proposito, che la Società non ha illustrato (né documentato nel corso del procedimento) quali "ordinari strumenti di contrasto" fossero stati in concreto adottati e si fossero rivelati "del tutto inefficaci", al fine di poter contabilizzare le effettive ore di lavoro prestate e di accertare la presenza dei lavoratori sul luogo di lavoro avrebbero potuto essere adottate misure utili allo scopo ma meno invasive per i diritti degli interessati (es. controlli automatici mediante badge, verifiche dirette, etc.).

Filtro per Argomento

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Provvedimento del 21 dicembre 2023 - Documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" [9978728]

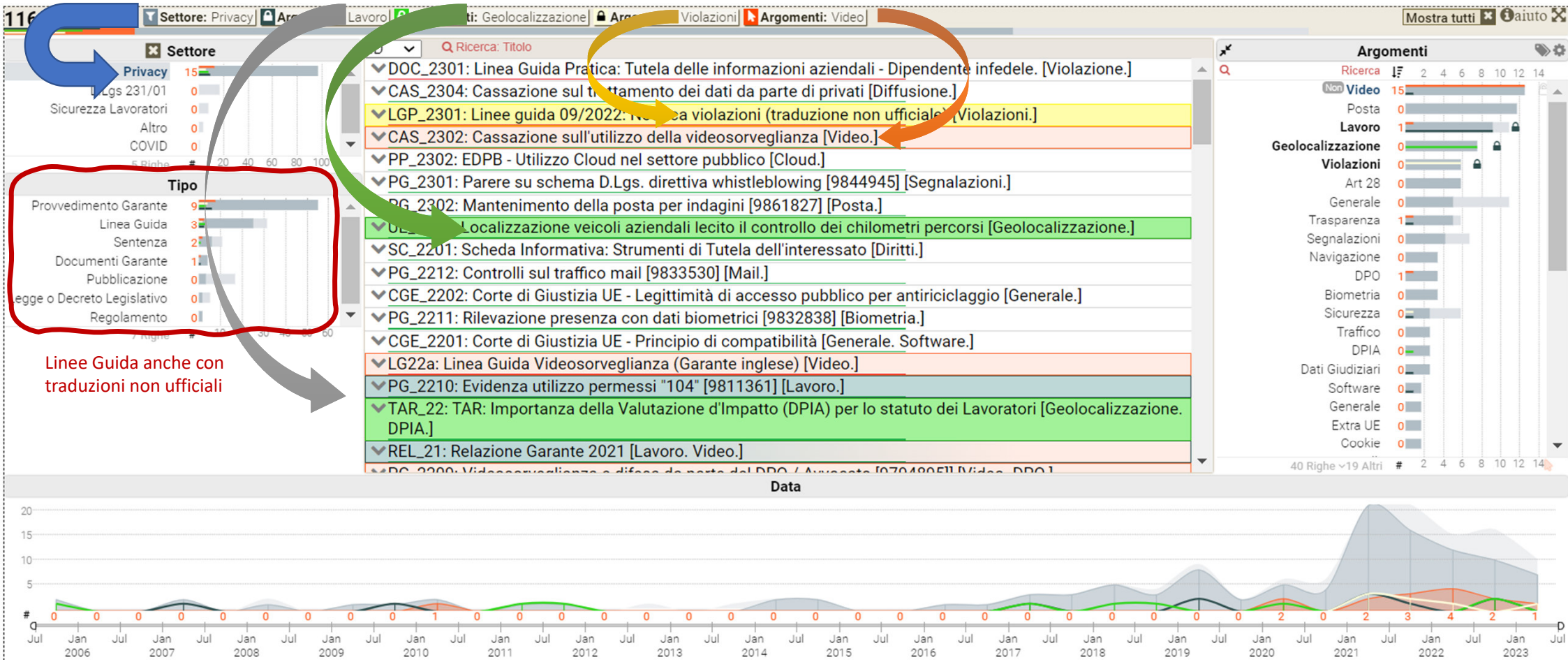


Selezione dei soli documenti che riguardano uno specifico argomento

2. La normativa in materia di protezione dei dati personali

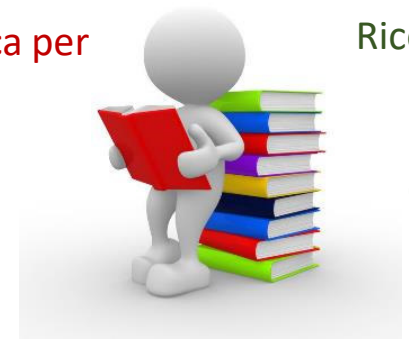
Come costantemente affermato dal Garante, il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati - riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente (artt. 2 e 15 Cost.), che proteggono il nucleo essenziale della dignità della persona e il pieno sviluppo della sua personalità nelle formazioni sociali. Ciò comporta che, anche nel contesto lavorativo pubblico e privato, sussista una legittima aspettativa di riservatezza in relazione ai messaggi oggetto di corrispondenza (v. punto 5.2 lett. b), delle "Linee guida del Garante per posta elettronica e Internet" del 1° marzo 2007, n. 13, doc. web n. 1387522; cfr., tra i tanti, provv. 4 dicembre 2019, n. 216, doc. web n. 9215890 e i precedenti in esso citati).

Documenti di supporto



Caratteristiche di SQuadra

Problematica per l'impresa di Costruzione



Ricerca delle migliori pratiche

Predisposizione di esempi direttamente applicabili ad una impresa «standard» di piccole dimensioni

Non come scrivere una procedura ma esempi concreti personalizzabili

Strumenti per la personalizzazione

Risparmio costi consulenza

- *Costi diretti*
- *Tempo per spiegare le specificità*

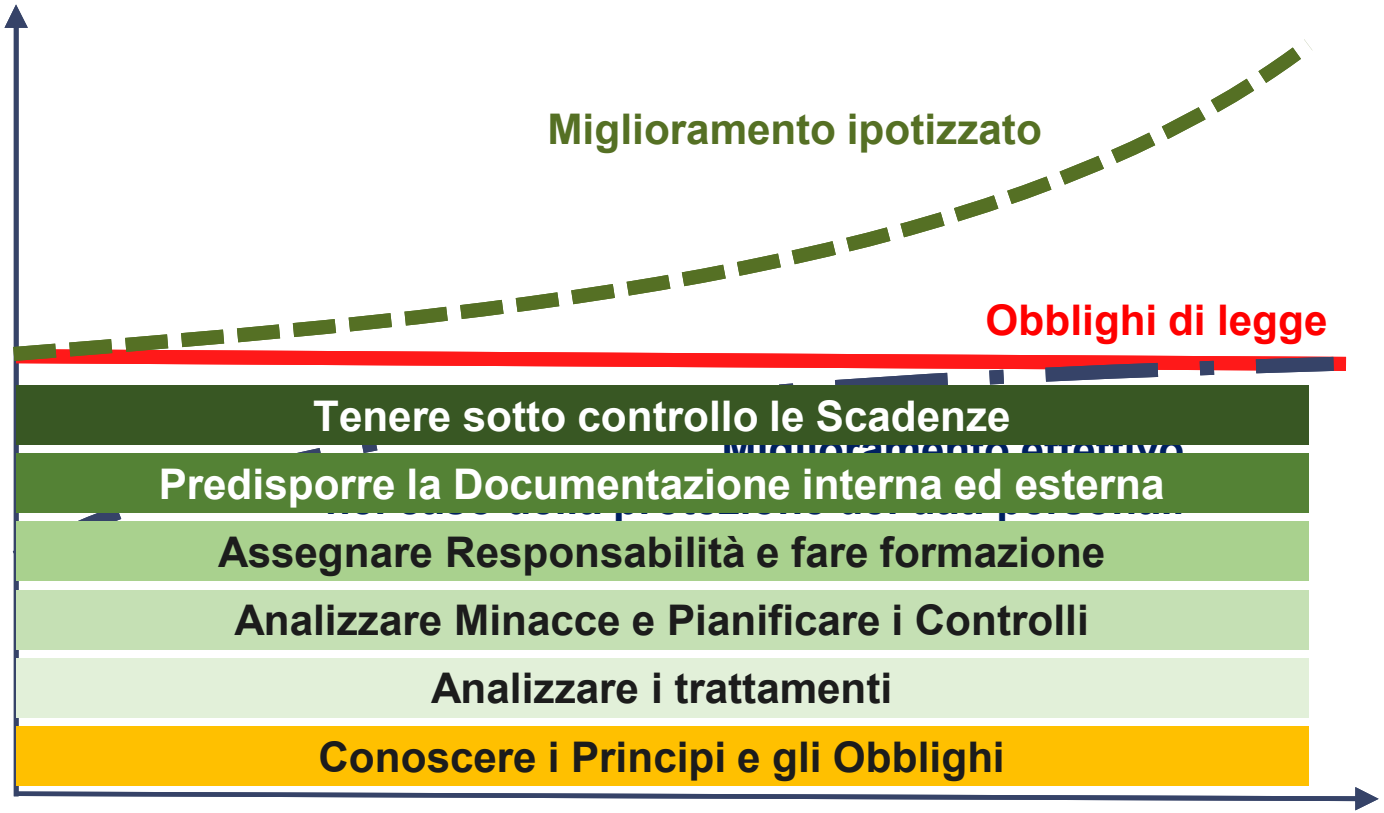
Soluzione specifica per l'azienda

Non adattamento di soluzioni generiche

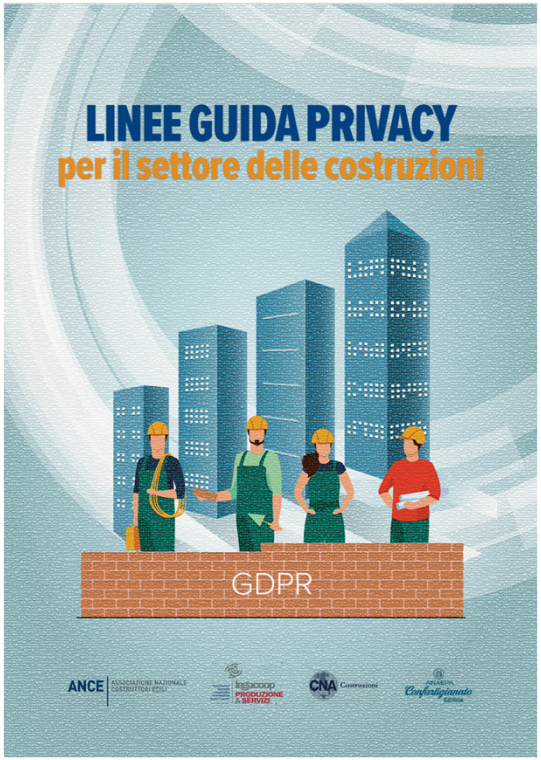
Coinvolgimento e consapevolezza

Tempi rapidi prima applicazione

Adozione di un Sistema di Gestione



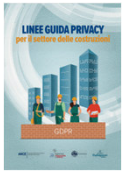
Condivisione con la filiera

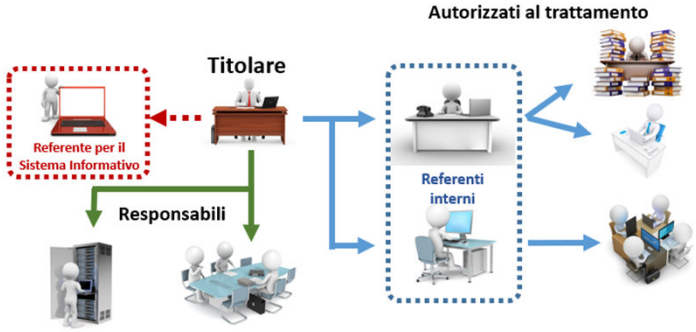


Documenti condivisi e migliorati dal confronto:

- Informative.
- Designazioni Referenti ed Autorizzati.
- Nomine Responsabili.
- Procedure e Valutazioni (Videosorveglianza e Geolocalizzazione).
- Procedure (Violazioni, Esercizio dei diritti, Gestione del Personali).
- Policy e prescrizioni per gli autorizzati ai trattamenti.

Definizione caratteristiche





a: Nessuna Videosorveglianza o Geolocalizzazione per i Lavoratori
b: Con Videosorveglianza sui Lavoratori (con accordo sindacale)
c: Con Geolocalizzazione sui Lavoratori (con accordo sindacale)
d: Con Videosorveglianza e Geolocalizzazione per i Lavoratori

i Aziendali

				Mail Titolare	Titolare_Privacy@EdiliziaM.it
Cod.Fiscale	01122334455	P.IVA	PIVA_Tiglio	Indirizzo Spedizione	giulianomarullo@gmail.com
DPO	Ing. Rossi Mario			Mail DPO	
Amministratori Sistema	disponibile nell'				
Resp. Sistema Informatico	Antonio Rossi				
Bacheca	area riservata del sito aziendale				

a: Impresa individuale, professionista. Un solo PC (spesso portatile).
b: Micro. Pochi PC, piccolo server, Nessun Amministratore di Sistema esterno.
c: Piccola. Vari PC con uno o più Server (anche virtuali). Amministratore di Sistema (in genere esterno).
d: Media. Molto PC e dispositivi mobili con vari Server (anche virtuali). Amministratore di Sistema (in genere esterno).
e: Grande Impresa / Impresa che vuole certificarsi 27001.

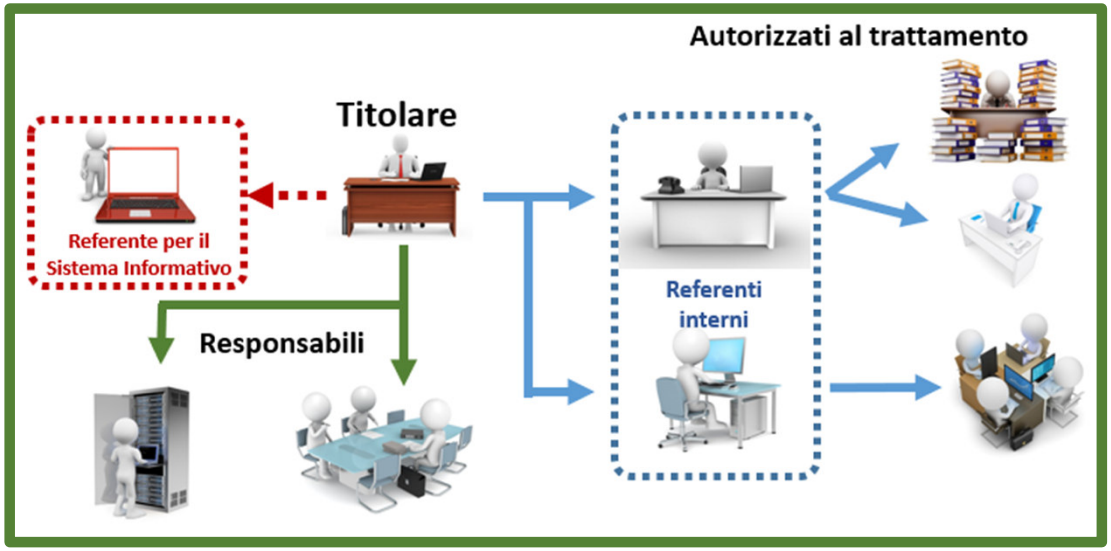
Caratteristiche del sistema informatico	c: Piccola. Vari PC con uno o più Server (anche virtuali). Amministrat		a: Utilizzo solo di Software standard b: Segue direttamente lo sviluppo di programmi personalizzati. c: Sviluppo software all'interno
Caratteristiche controllo sui Lavoratori	d: Con Videosorveglianza e Geolocalizzazione per i Lavoratori		
Consulenti IT	c: Rapporti occasionali con più fornitori per l'HW ed il SW (tutti di chiara f...	Sviluppo SW	b: Segue direttamente lo sviluppo di programmi personalizzati.
Seg		Utilizzo WiFi	a: Nessun utilizzo
Uso		ati strumenti per l'a	
Vie		ita per PC	
Car		sta chiusa	

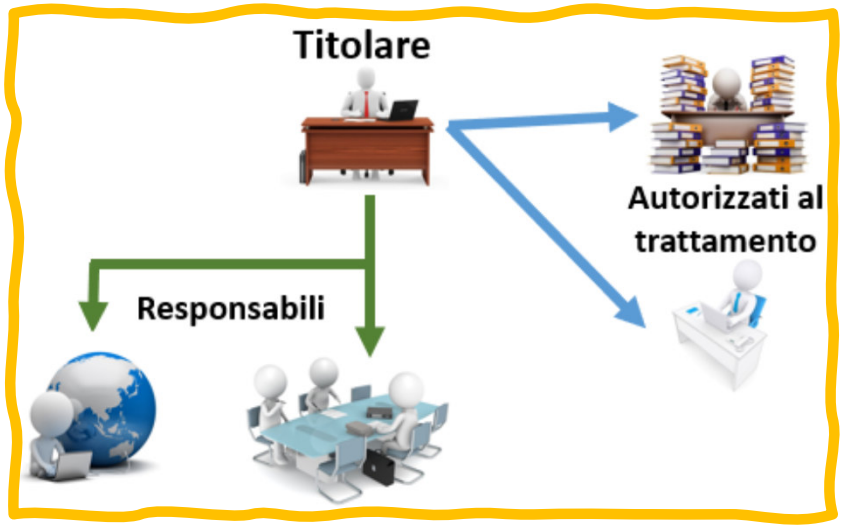
a: Rapporto consolidato con un solo fornitore che coordina tutte le problematiche HW e SW di chiara fama (Locale o Nazionale).
b: Rapporto consolidato con un solo fornitore per l'HW e pochi fornitori SW tutti di chiara fama (Locale o Nazionale).
c: Rapporti occasionali con più fornitori per l'HW ed il SW (tutti di chiara fama).
d: Rapporti con più fornitori di cui, almeno uno, offre garanzie limitate.

a: Nessun utilizzo
b: Utilizzo solo per ospiti per il solo accesso ad internet
c: Utilizzo solo per ospiti per accesso ad internet ed alle stampanti
d: Utilizzo solo in sedi esterne (es. Cantieri) per tutte le attività
e: Utilizzo per le normali attività sia in ufficio che in sedi esterne

Utilizzo del Telelavoro	☐
Linee Guida Edilizia ISTECO	☑

Supporto «su misura»

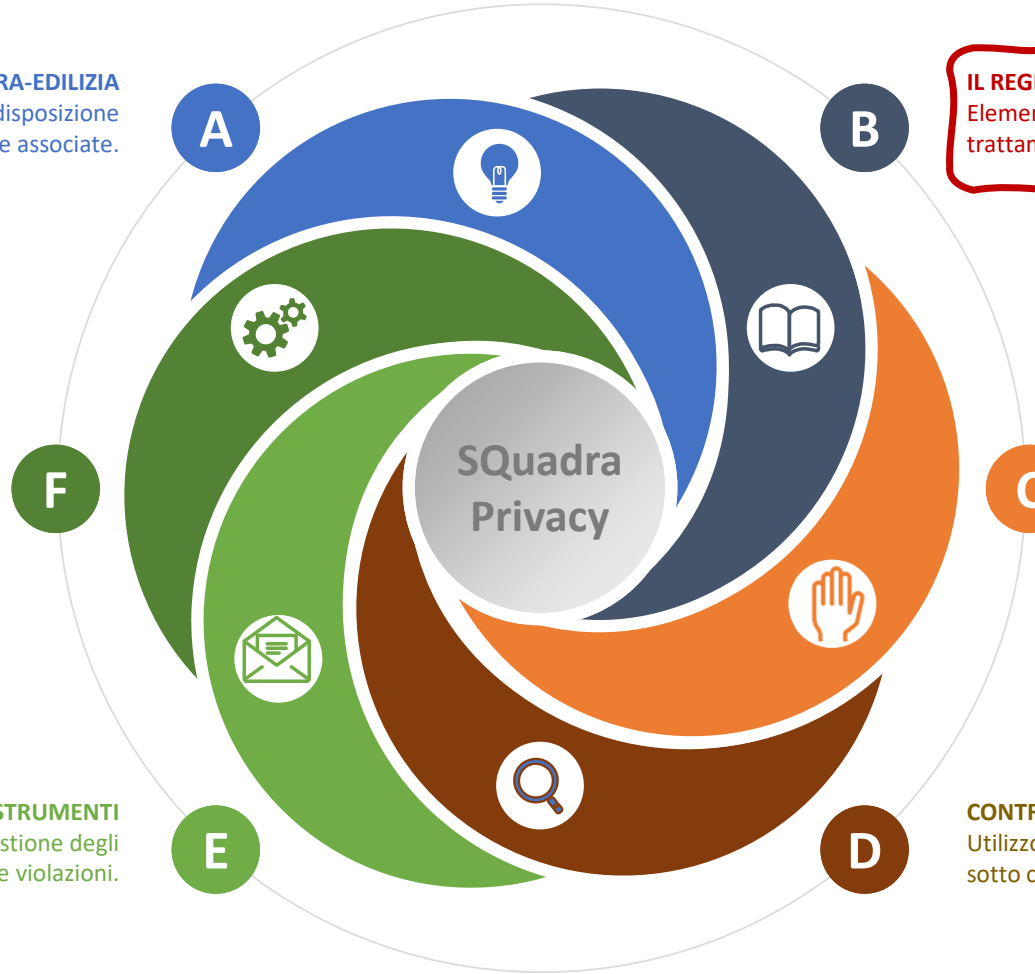




SQuadra-Privacy

IL PROGETTO SQUADRA-EDILIZIA
Dal 2008 uno strumento a disposizione delle imprese associate.

IL REGISTRO DEI TRATTAMENTI
Elemento essenziale per l'analisi dei trattamenti effettuati.



SICUREZZA DELLE INFORMAZIONI
Problematiche tipiche e specifiche relative all'utilizzo delle nuove tecnologie.

CONFORMITÀ E MINACCE
Autovalutazione della situazione di partenza e degli obiettivi.

ALTRI STRUMENTI
Documenti aggiuntivi e gestione degli incidenti e delle violazioni.

CONTROLLI
Utilizzo delle migliori pratiche per tenere sotto controllo i sistemi informatici.

Registro dei Trattamenti

- Esercizi commerciali, esercizi pubblici o **artigiani con almeno un dipendente** (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o **che trattino dati sanitari dei clienti** (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.).
- **Liberi professionisti con almeno un dipendente** e/o che **trattino dati sanitari** e/o **dati relativi a condanne penali o reati** (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- Il **condominio** ove tratti "categorie particolari di dati" (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

8 ottobre 2018

Il Registro aziendale può contenere informazioni anche relativamente a trattamenti che non riguardano i dati personali

Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del RGPD, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.

Tipi di Registri

Registro (Intermedio)
Contiene gli elementi suggeriti dalle autorità europee

Registro (Esteso)
Permette una analisi completa del trattamento

Registro (Semplificato)
Contiene gli elementi essenziali

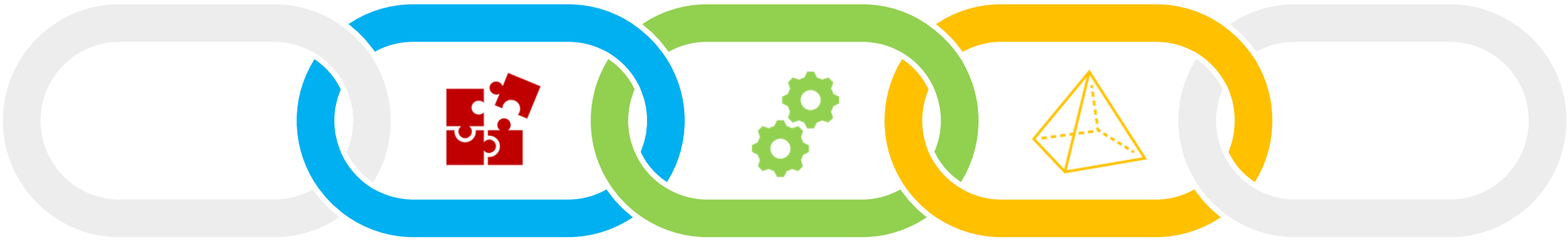
Registro dei Trattamenti

Esteso

Permette una analisi completa del trattamento.

Semplificato

Elementi essenziali



Intermedio

Elementi suggeriti dalle autorità europee

Registro dei Trattamenti (esteso)

Elementi «trasversali»

«Per trattamento»

Registro dei trattamenti esteso

- Obblighi e Diritti
- Responsabilità e Ruoli
- Valutazione Impatto
- Art. 30 (Registro)
- Criticità
- Rischi
- Art. 25

Un «contenitore» dove poter analizzare tutti gli aspetti di ogni trattamento

19 APPENDICE: Regolamento Europeo protezione dei dati personali (GDPR) 260
19.1 Premessa 260
19.2 Il Regolamento Europeo 260
19.2.1 Principi applicabili al trattamento dei dati [Art.5] 260
19.2.2 Informative e consenso. 260
19.2.3 Gestione delle violazioni. 261
19.2.4 Titolari e Responsabili della protezione dei dati. 261
19.2.5 I codici di condotta. 261
19.3 Criteri per determinare la necessità di effettuare una Valutazione Impatto Privacy (PIA) 261
19.4 Glossario predisposto da Confindustria per il Registro delle attività di Trattamento 264
20 APPENDICE: Sistema di Gestione per la Sicurezza delle Informazioni .....
20.1 Norma ISO 27001 .....
20.2 Rischi 268
20.3 Eventi indesiderati .....
21 APPENDICE: Controlli sui Sistemi Informativi .....
21.1 Norma ISO 27001 .....
21.2 Agenzia per l'Italia Digitale 273
21.3 Framework Nazionale per la Cyber Security" .....
21.4 Controlli essenziali 2016 .....
22 APPENDICE: Linee Guida ENISA sulla sicurezza dei dati personali .....
22.1 Introduzione 280
22.1.1 La Sicurezza delle informazioni 280
22.1.2 Gestione del Rischio 280
22.1.3 Obblighi di sicurezza nel GDPR 281
22.2 Valutazione dei Rischi per la sicurezza dei dati personali 282
23 APPENDICE: Protezione dei dati per progettazione e per impostazione predefinita 285
24 APPENDICE: Misure organizzative e tecniche per prevenire/mitigare violazioni 288
25 APPENDICE: Valutazione della gravità di una violazione 293

MINACCE

CONTROLLI

VIOLAZIONI

Registro dei Trattamenti (esteso)

Rischio del Trattamento di non assicurare:

- Riservatezza
- Integrità
- Disponibilità

Importanza del Trattamento

Codice	Area	Dettaglio	Importanza	Tipo Dati	Riservatezz	Integrità	Disponibilit	Responsabile
T00.a	a. Sistema Informativo	Manutenzione del sistema informatico.	Molto Alta	Particolari / Riservati	Critico	Alto	Alto	Ing.Ciro Napoli
T00.b	a. Sistema Informativo	Addetti alle pulizie.	Bassa	Particolari / Riservati	Critico	Trascurabile	Medio	Anna Neri
T01.a	b. Personale	Gestione Paghe e note spese, rileva...	Media	Particolari / Riservati	Basso	Medio	Alto	Ing. Enrico Milano
T01.b	b. Personale	Assunzioni, collaborazioni, dimission...	Media	Particolari / Riservati	Medio	Medio	Medio	Ing. Enrico Milano
T01.c	b. Personale	Curricula	Molto Bassa	Particolari / Riservati	Basso	Trascurabile	Trascurabile	Ark. Bruno Roma
T01.c	b. Personale	Formazione ed addestramento	Media	Anagrafici-Identific...	Basso	Medio	Basso	Ing. Enrico Milano
T01.d	b. Personale	Sorveglianza sanitaria	Alta	Particolari / Riservati	Basso	Medio	Basso	Ing. Enrico Milano
T02.a	c. Clienti/Fornitori	Inserimento in registri e gestione del ...	Media	Anagrafici-Identific...	Basso	Medio	Medio	Ing. Enrico Milano
T02.b	c. Clienti/Fornitori	Dati per fatturazione attiva e passiva.	Alta	Anagrafici-Identific...	Basso	Alto	Alto	Ing. Enrico Milano
T03.a	d. Qualità	Risultati Audit e trattamento NC.	Bassa	Altri dati / Riservati	Medio	Basso	Basso	Anna Neri

Registro dei Trattamenti (esteso)

Codice	T00.a	Area	a. Sistema Inform	Inizio	gg/mm/aaaa	Fine	gg/mm/aaaa
Finalità	Manutenzione del sistema informatico.						
Importanza	f: Molto Alta			Tipo Dati (Per i dati personali / Per la società) - Livello più alto	c: Particolari / Riservati		
Dati normali	Tutti i tipi di dato			Dati particolari	Tutti i tipi di dati PARTICOLARI		
FORMATO DEI DATI TRATTATI:	Digitale	✓	Cartaceo				

Descrizione e Finalità

Articolo 32

Sicurezza del trattamento (C83)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Criticità

Riservatezza	5: Critica	La diffusione delle informazioni può mettere a repentaglio la sostenibilità dell'organizzazione o ha impatti elevati relativi al rispetto della normativa vigente.
Integrità	3: Media	I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente.
Disponibilità	4: Alta	L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti. Sono dati senza i quali l'azienda è in grado di operare per brevi periodi di tempo. In questa categoria rientrano i dati utilizzati nei processi aziendali standard o che rappresentano un investimento significativo e sono difficili da ricostruire.
Tempo di Interruzione accettabile (ore)	48,0	Tempo di Perdita accettabile (ore) 12,0
Vulnerabilità da attacchi intenzionali	C: Alta	I dati sono appetibili o l'immagine aziendale è compromessa, e quindi può essere condotto da malintenzionati molto motivati, tecnicamente preparati e con ingenti risorse a disposizione; o in alternativa, gli studi confermano che tentativi di attacco sono comunque portati molto di frequente.
Vulnerabilità accidentali	b: Media	L'ambito è mediamente complesso e quindi possono essere commessi errori.

Registro dei Trattamenti (esteso)

Riservatezza

1 - Bassa	I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici.
2 - Media	I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business aziendale o sul rispetto della normativa vigente.
3 - Alta	I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine). Un'eventuale loro diffusione ha elevati impatti sul business aziendale ma non sul rispetto della normativa vigente.
4 - Critica	La diffusione delle informazioni può mettere a repentaglio la sostenibilità dell'organizzazione o ha impatti elevati relativi al rispetto della normativa vigente.

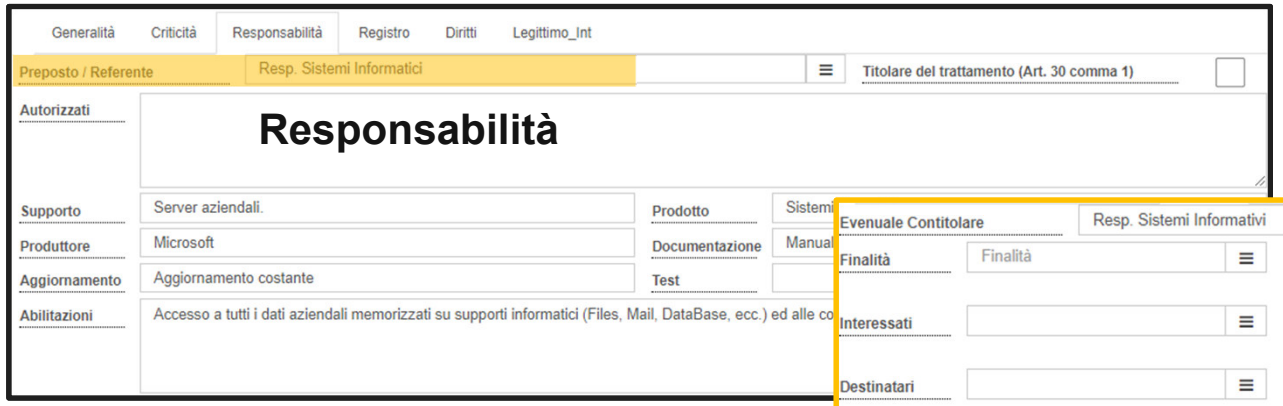
Integrità

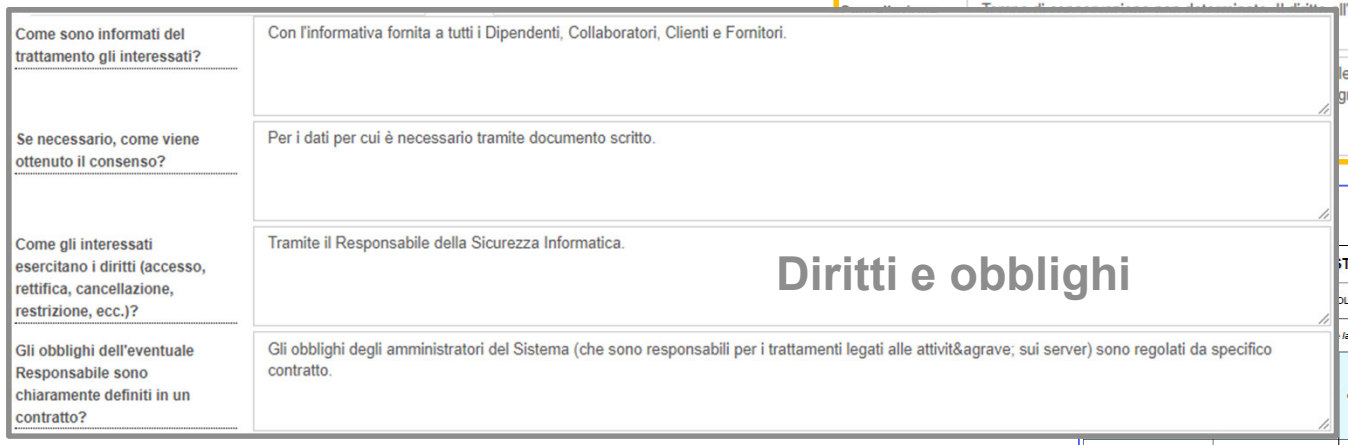
1 - Bassa	I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie.
2 - Media	I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente.
3 - Alta	I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati ha elevati impatti sulle attività operative, ma non sul rispetto della normativa vigente.
4 - Critica	La mancanza di integrità delle informazioni ha elevati impatti sul sulle attività o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione. I dati sono utilizzati per transazioni economiche, finanziarie o sanitarie.

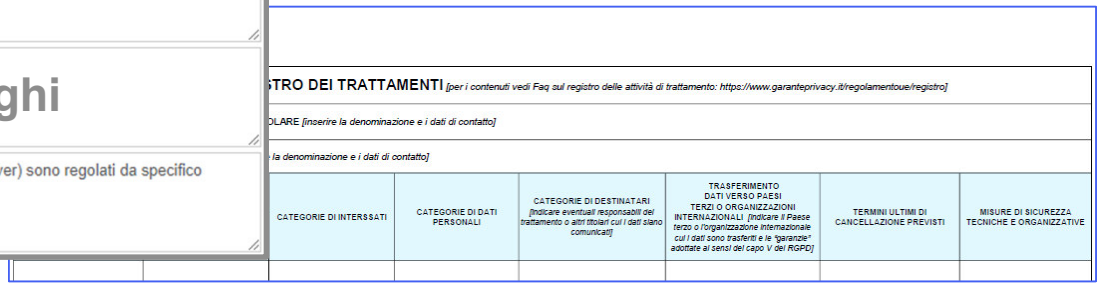
Disponibilità

1 - Bassa	L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti.
2 - Media	L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti.
3 - Alta	L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti.
4 - Critica	L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine.

Registro dei Trattamenti (esteso)







Registro dei Trattamenti (esteso)

Dettagli per ogni Trattamento - Ruoli

Responsabile Esterno	Società Servizi Informatici
Trattamento	Manutenzione di sistemi, aggiornamento e controllo di tutta la rete, configurazione e verifica dei backup, installazione software, supporto per la definizione delle policy aziendali.
Quota trattamento esterno	d: Una parte molto significativa.
Contratto del	01/05/2017
Responsabile verifica	Resp. Sistemi Informatici
Ultima_Verifica	10/05/2018
Mesi Prossima verifica	12
Note	

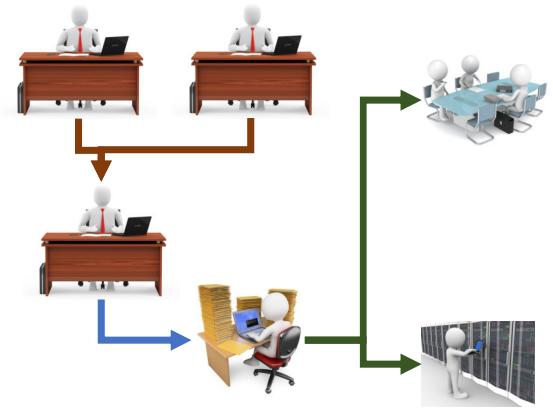
Responsabili

A cui sono affidate parti del trattamento
Es. Consulente per paghe e contributi.

Titolari

Che hanno affidato il trattamento
Es. Società collegate

Titolare	Società A del Gruppo
Contitolare	Nessuno
Trattamento	Gestione del personale di società del Gruppo.
Contratto del	01/05/2018
Ultima relazione (se richiesta)	01/05/2018
Mesi Prossima relazione (se prevista una periodicità)	12
Note	



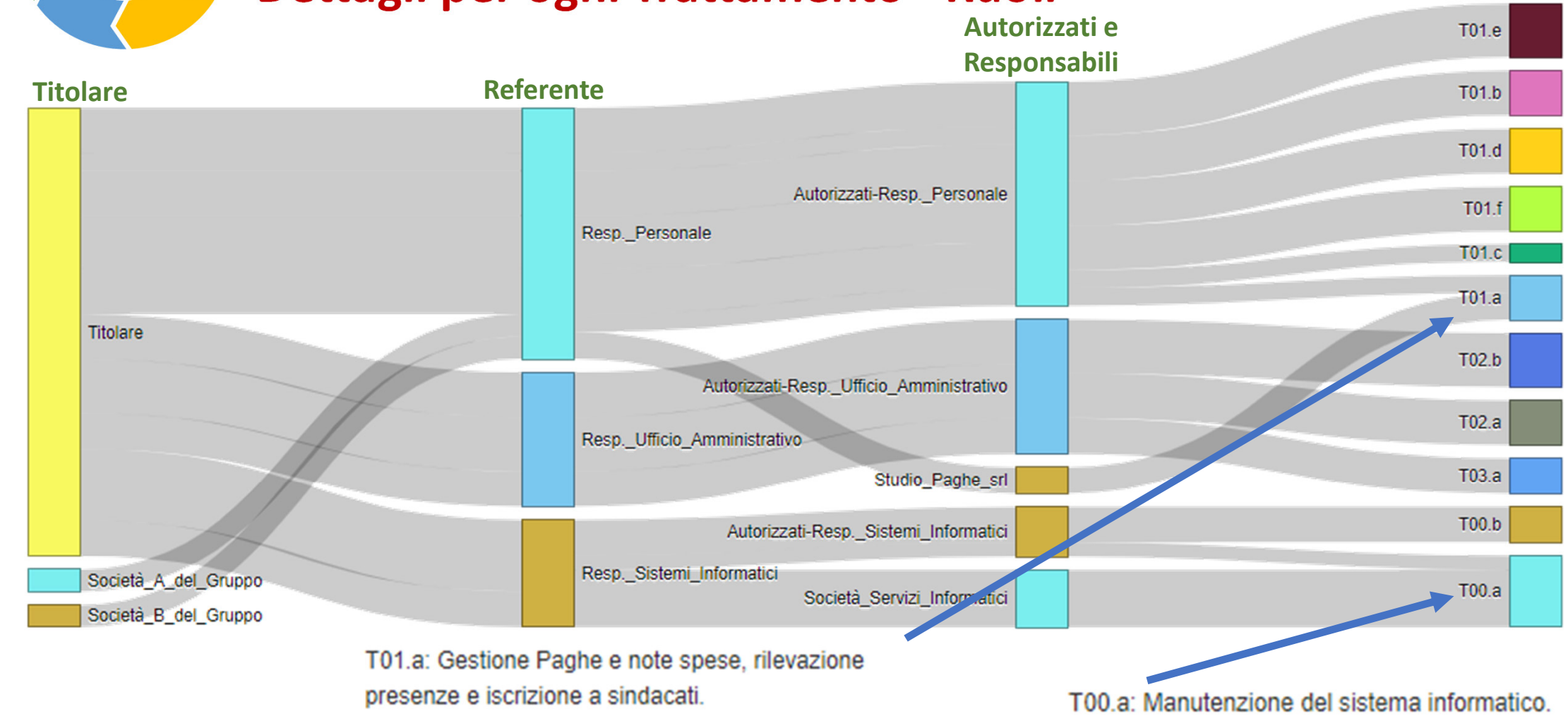
Organigramma

Tutte le figure coinvolte nel trattamento

Ruolo	Denominazione	Indirizzo
Contitolare del trattamento	Azzurri Carloi	Via Roma 11
Responsabile della protezione dei dati (DPO)	Bianchi Anna	Via Pisa 25
Delegato dal Titolare del trattamento – Referente privacy	Gialli Marco	Via Napoli 25
Rappresentante del Titolare del trattamento	Neri Antonio	Via Firenze 1
Titolare del trattamento	Rossi Giovanni	Via Milano 12
Sub-responsabile del trattamento	Rossini Carlo	Via Palermo 25
Responsabile del trattamento	Verdini Carlo	Via Catania 25

Registro dei Trattamenti (esteso)

Dettagli per ogni Trattamento - Ruoli



T01.a: Gestione Paghe e note spese, rilevazione presenze e iscrizione a sindacati.

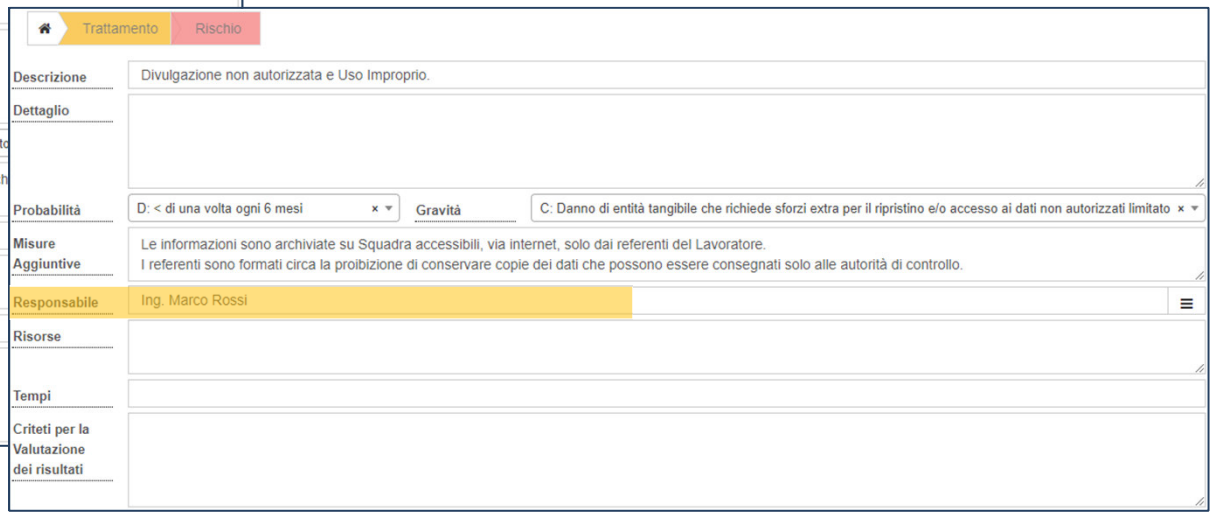
T00.a: Manutenzione del sistema informatico.

Registro dei Trattamenti (esteso)

Dettagli per ogni Trattamento - Rischi

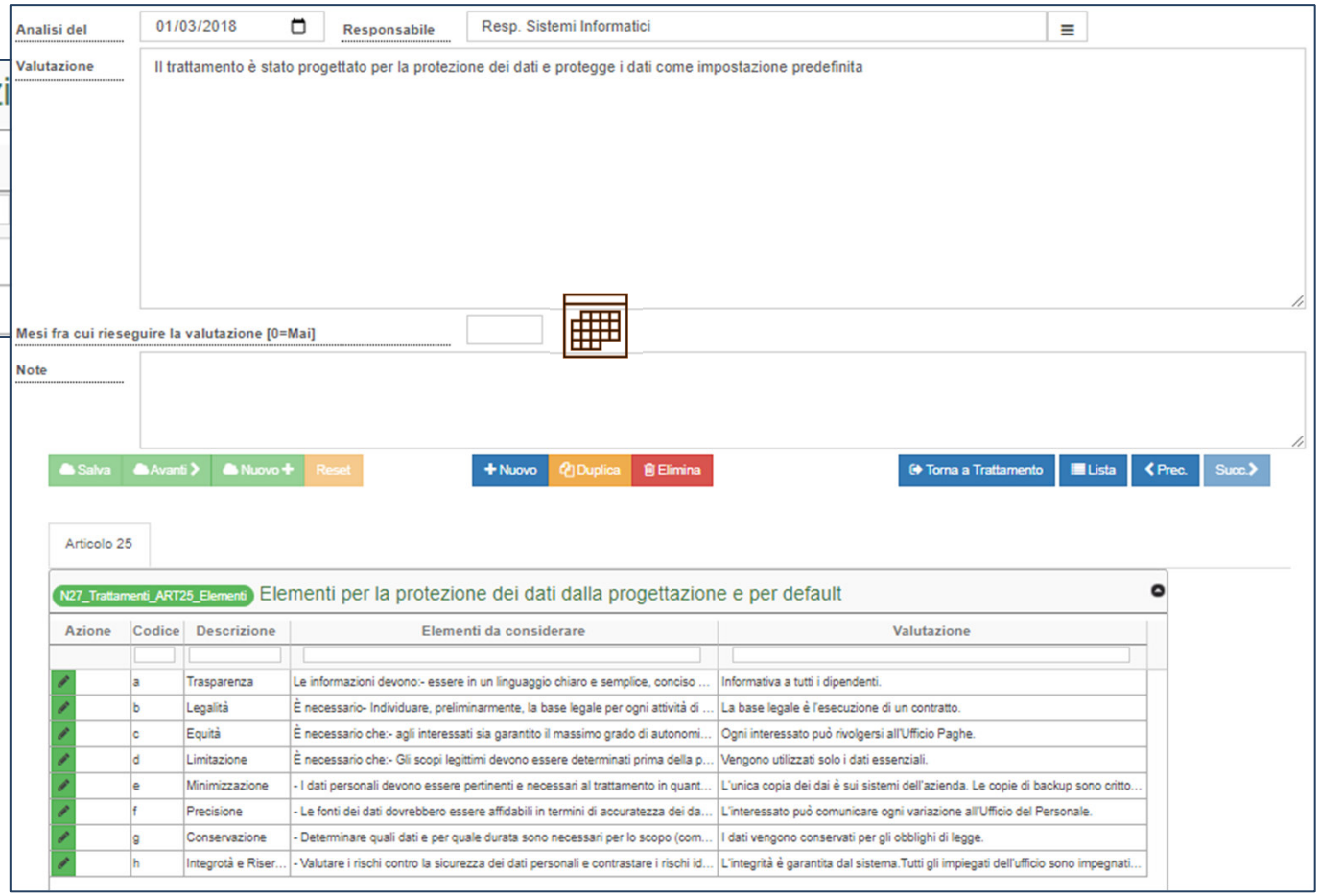
Descrizione	Probabilità	Gravità	Rischio	Misure	Responsabile
Perdita, Distruzione.	C.< di una volta l...	B.Non richiede s...	B.Basso	Accessi autorizzati al solo personale...	Dott. Marco Gialli
Divulgazione non autorizzata e Uso I...	D.< di una volta ...	C.Danno di entit...	D.Alto	Le informazioni sono archiviate su S...	Ing. Marco Rossi

Rischi legati al trattamento



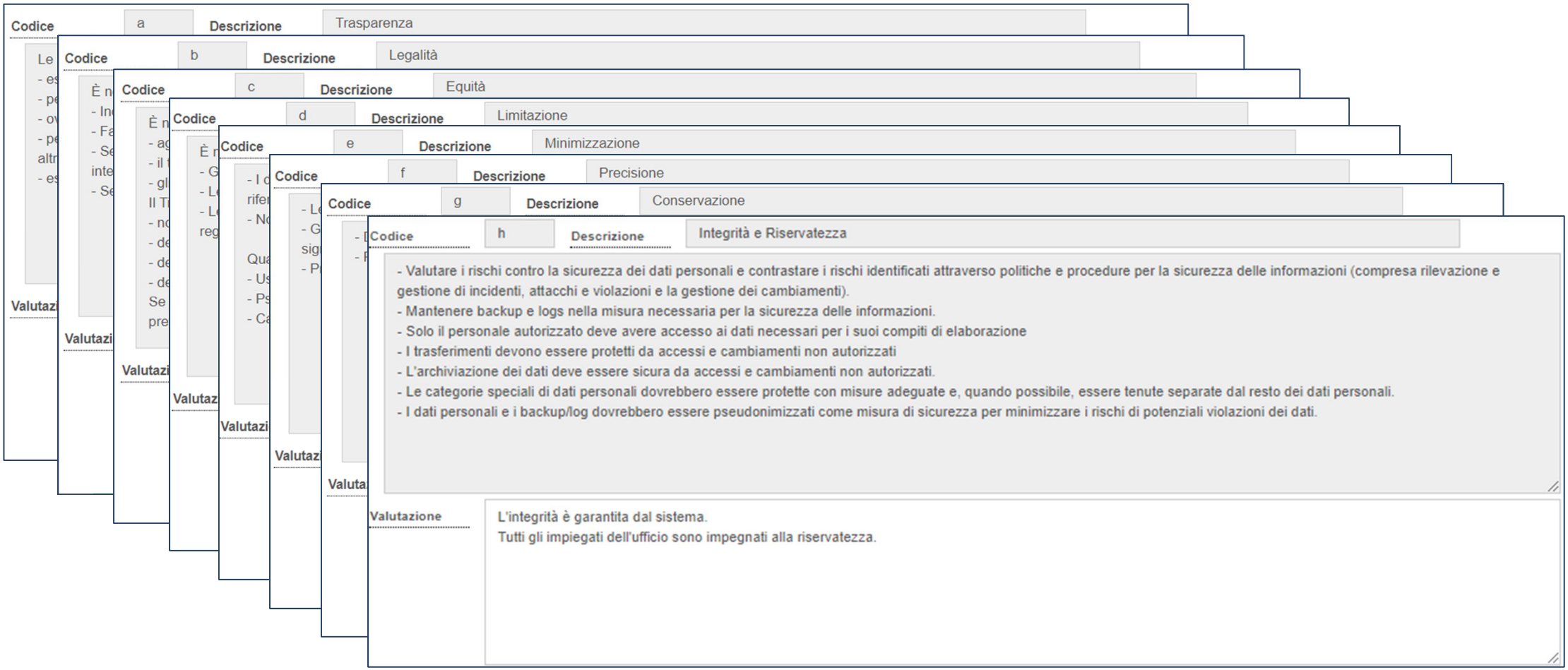
Registro dei Trattamenti (esteso)

Dettagli per ogni Trattamento – Art. 25



Registro dei Trattamenti (esteso)

Dettagli per ogni Trattamento – Art. 25



Registro dei Trattamenti (esteso)

Dettagli per ogni Trattamento – Necessità Valutazione Impatto

N27_Trattamenti_PIA_1N Valutazione Impatto Privacy (PIA)

Azione	Analisi del	Responsabile	Necessità	Valutazione
	01/05/18	Ark. Gianna Neri	Il Trattamento non rientra fra quelli espressamente esclusi dall'Autorità.Solo il...	Non si ritiene necessario, ad oggi, effettuare una PIA
	01/01/18	Ark. Gianna Neri	Per adesso non sembra necessaria verrà valutato fra qualche mese.	Non si ritiene necessario effettuare una PIA

Trattamento > PIA

Analisi del: 01/05/2018 — Responsabile: Ark. Gianna Neri

Necessità PIA: Il Trattamento non rientra fra quelli espressamente esclusi dall'Autorità.
Solo il criterio sulla gestione di dati sensibili può essere ritenuto significativo e quindi non si ritiene necessario effettuare la PIA.

Valutazione: c: Non si ritiene necessario, ad oggi, effettuare una PIA — Mesi fra cui rieseguire la valutazione [0=Mai]: 24

Codice	Descrizione
00	PIA esclusa per lo specifico trattamento
01	Valutazione o assegnazione di un punteggio
02	Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
03	Monitoraggio sistematico
04	Dati sensibili o dati aventi carattere altamente personale
05	Trattamento di dati su larga scala
06	Creazione di corrispondenze o combinazione di insiemi di dati
07	Dati relativi a soggetti vulnerabili
08	Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative
09	Impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto
10	Altro

9 criteri previsti dalle Linee Guida 4/10/17

Trattamento > PIA > Criteri

Codice: 04 — Descrizione: Dati sensibili o dati aventi carattere altamente personale

Questo criterio include dati personali di categorie particolari, relativi a condanne penali o reati, comunque legati ad attività a carattere personale o domestico oppure perché influenzano l'esercizio di un diritto fondamentale oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato. A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi.

Dettagli: Potenzialmente il trattamento potrebbe coinvolgere dati particolari.

Significativo per il trattamento in esame: b: Significativo

La valutazione d'impatto sulla protezione dei dati va **riesaminata continuamente** e **rivalutata con regolarità**. [WP29]

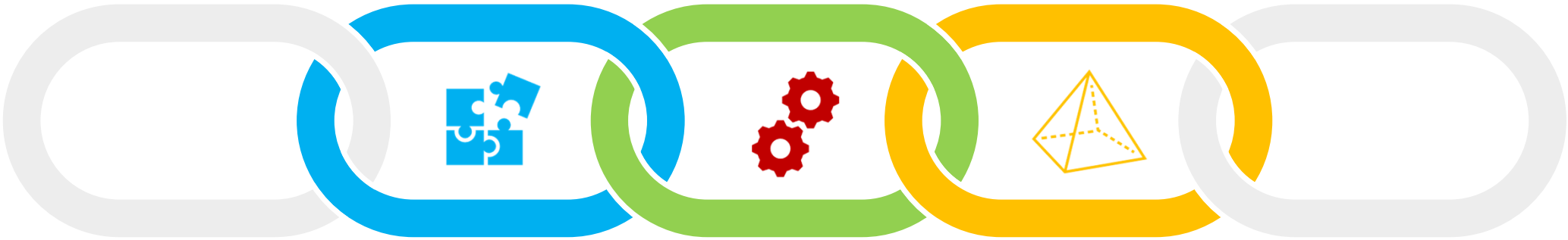
Registro dei Trattamenti

Esteso

Permette una analisi completa del trattamento.

Semplificato

Elementi essenziali



Intermedio

Elementi suggeriti dalle autorità europee

Registro dei Trattamenti (Intermedio)

Francia

Modèle de fiche de registre à compléter

Cet onglet est un modèle de fiche opérationnelle à reprendre, adapter et compléter selon votre activité pour chaque traitement.
Dans certains cas, des commentaires seront proposés pour vous aider à compléter votre registre (triangle rouge dans la cellule).

Description du traitement				
Nom du traitement				
N° / RÉF	ref-001			
Date de création du traitement				
Mise à jour du traitement				
Acteurs	**Nom**	**Adresse**	**Code Postal**	**Ville**
Responsable du traitement				
Délégué à la protection des données				
Société du DPO (si celui-ci est externe)				

Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Belgio

Registre des activités de traitement

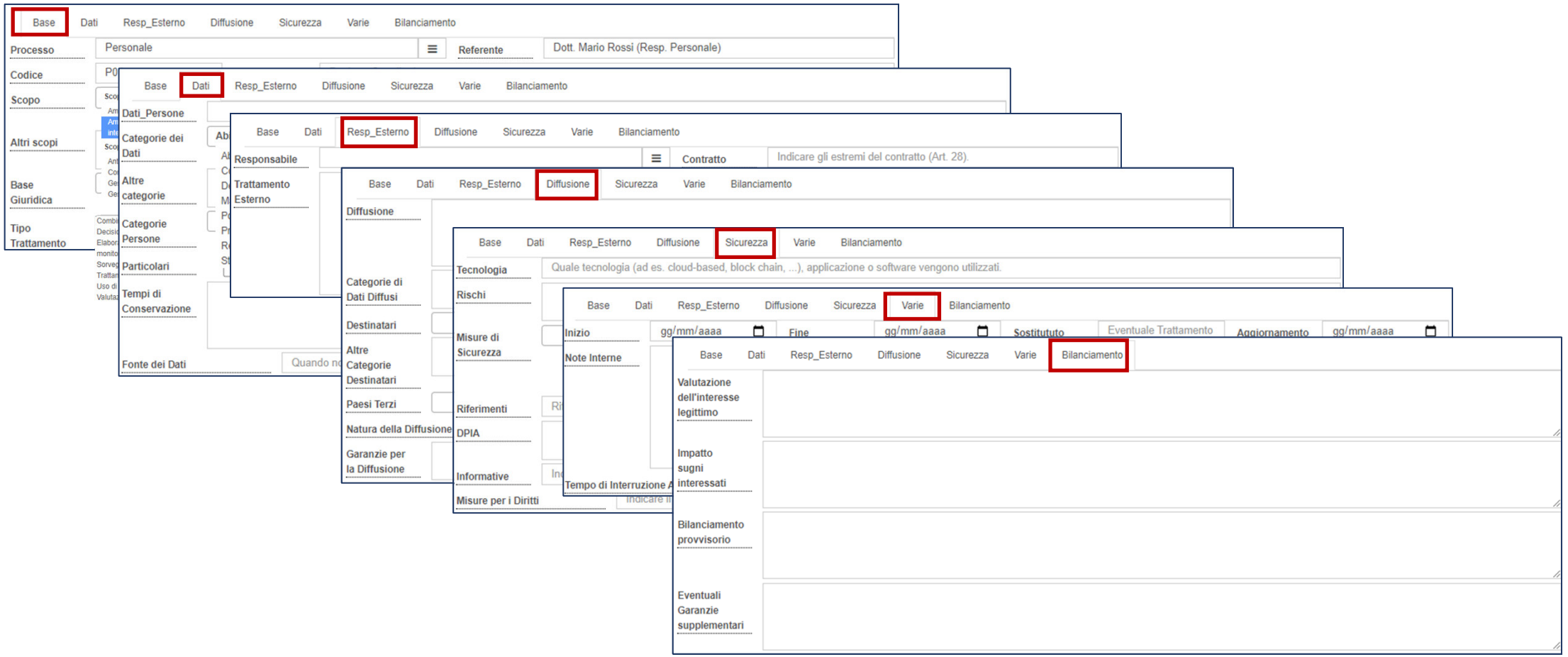
Responsable du traitement :

Délégué à la protection des données :

***Elenchi dettagliati** (Finalità, Categorie dati, Elaborazioni, Destinatari, ecc.)*

processus opérationnel/traitement	description fonctionnelle du traitement	données utilisées et personnes concern	sous-traitant	échange de donné
identification du processus opérationnel *nom, propriétaire du processus* *(dans la colonne ci-dessous, on reprend le nom du traitement en fonction de la lisibilité de la version électronique du registre)*	identification et information au sujet du traitement *numéro , , description fonctionnelle, , finalité, fondement du traitement, type de traitement et description fonctionnelle*	détails sur les données traitées et sur les personnes concernées dont les données sont traitées *catégorie fonctionnelle, catégorie sensible de traitement de données, catégorie de personne concernée, niveau de classification, délai de conservation, source authentique*	identification du sous-traitant (externe à l'organisation) impliqué dans le traitement *nom, n° du contrat de traitement de données*	informations au sujet d'un avec des tierces parties. catégorie(s) de données, c *pays tiers/organisation inte* *garanties appropriées*

Registro dei Trattamenti (Intermedio)



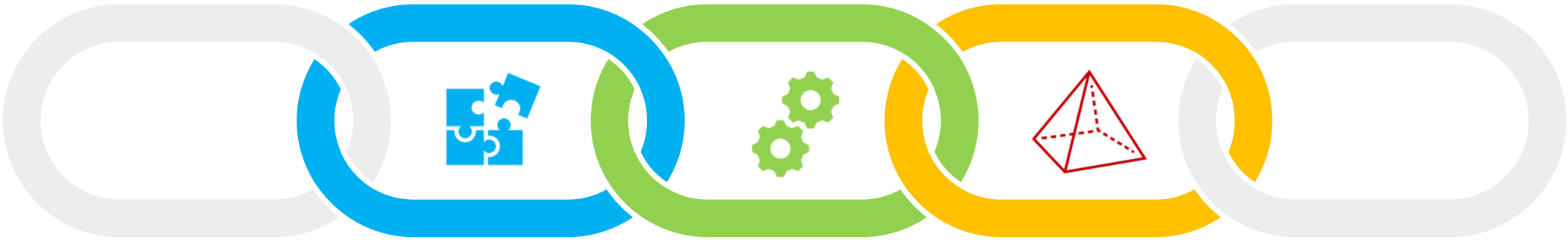
Registro dei Trattamenti

Esteso

Permette una analisi completa del trattamento.

Semplificato

Elementi essenziali



Intermedio

Elementi suggeriti dalle autorità europee

Registro semplificato

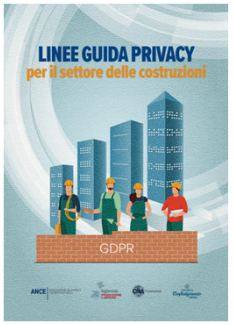
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*

RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE



Base | Interni | Legittimo_Interesse

Codice	T01	Area	Gestione Personale
Dettaglio	Assunzione, Rapporti Interinali e Contratti di collaborazione	Significatività	d: Media
Finalità	Raccolta e Archiviazione dati del lavoratore per stipula del contratto.		
Categorie Interessati	Dipendenti / Collaboratori continuativi		
Categorie Dati Personali	Dati personali ed identificativi.		
Categorie Particolari Dati	Dati sulla salute e iscrizione sindacale.		
Liceità: lettere del comma 1 Art.6	b, c.	Liceità: lettere del comma 2 Art.9 (Particolari)	b.
Incaricati	Ufficio Personale	Responsabili Esterni	Agenzie interinali.
Destinatari Esterni	Inail, INPS e altri enti di previdenza sociale.	Trasferimento verso paesi terzi	Nessuno
Termini per Cancellazione	5 anni dalla conclusione del rapporto.	Misure di Sicurezza	Sicurezza Sistema Informatico. Sicurezza nella gestione dei docum
Modalità trasmissione Informativa	Informativa Dipendenti. Informativa Collaboratori.	Modalità richiesta Consenso (se necessario)	

Azione	Codice	Area	Dettaglio
	T01	Gestione Personale	Assunzione, Rapporti Interinali e Contratti di collaborazione
	T02	Gestione Personale	Buste Paga e documentazione fiscale del lavoratore
	T03	Gestione Personale	Definizione mansioni
	T04	Gestione Personale	Sanzioni Disciplinari
	T05	Gestione Personale	Visite Mediche
	T06	Gestione Personale	Formazione
	T07	Gestione Personale	Dimissione
	T08	Gestione Personale	Infortuni
	T09	Gestione Personale	Richieste dirette del personale (Permessi, ferie, 104 ecc.)
	T10	Gestione Personale	Curricula
	T11	Gestione Clienti (Persone fisiche)	Gestione Anagrafica Clienti
	T12	Gestione Clienti (Persone fisiche)	Richieste "sensibili" Clienti
	T13	Gestione Fornitori	Gestione Anagrafica Fornitori (Persone fisiche)
	T14	Gestione Fornitori	Controllo Regolarità subappalti
	T15	Gestione Fornitori	Sanzioni ai Fornitori (con dati persone fisiche)

SQuadra-Privacy

A **IL PROGETTO SQUADRA-EDILIZIA**
Dal 2008 uno strumento a disposizione delle imprese associate.

B **IL REGISTRO DEI TRATTAMENTI**
Elemento essenziale per l'analisi dei trattamenti effettuati.

C **CONFORMITÀ E MINACCE**
Autovalutazione della situazione di partenza e degli obiettivi.

D **CONTROLLI**
Utilizzo delle migliori pratiche per tenere sotto controllo i sistemi informatici.

E **ALTRI STRUMENTI**
Documenti aggiuntivi e gestione degli incidenti e delle violazioni.

F **SICUREZZA DELLE INFORMAZIONI**
Problematiche tipiche e specifiche relative all'utilizzo delle nuove tecnologie.

Conformità

Valutazione | Misure_Aggiuntive

Codice: F10 | Tipologia: F.Risorse umane

Argomento: Verifica dei controlli sull'utilizzo dei sistemi informatici.

Sede/Oggetto: Sede e Cantieri pluriennali

Significatività: e: Alta

Conformità: c: Parzialmente conforme

Misure:
Vengono utilizzati indirizzi mail con riferimento ai lavoratori e i lavoratori sono stati invitati ad un uso solo aziendale. Non è prevista la gestione in caso di cessazione del rapporto.
Vengono registrati i log di navigazione per la sicurezza dell'infrastruttura IT ma non sono definiti i limiti temporali e non è stata data adeguata informazione ai lavoratori.
Non vengono registrate operazioni massive sui dati personali (es esportazione su excel di tutte le anagrafiche).

Note: Es. Uso delle mail con

Valutazione | Misure_Aggiuntive

Misure Aggiuntive:
Devono essere definite le regole per il corretto utilizzo degli indirizzi mail individualizzati con particolare riferimento al mantenimento dei dati aziend in caso di cessazione del rapporto.
I log di navigazione per la sicurezza dell'infrastruttura IT verranno raccolti, normalmente, senza l'informazione del singolo utente. Solo in caso di anomalie si potrà effettuare una raccolta più mirata.
Devono essere individuate le operazioni "anomale" (es. copia massive di dati personali) per le quali mantenere il tracciamento.

Responsabile per le Misure aggiuntive: Resp. Sistemi Informatici

Risorse: Utilizzo delle indicazioni presenti sul Manuale prodotto da SQuadra.

Tempi: Entro dicembre 2018

Criteri per la Valutazione dei risultati: Audit da parte di un consulente esterno.

Conformità attesa: a: Totalmente conforme

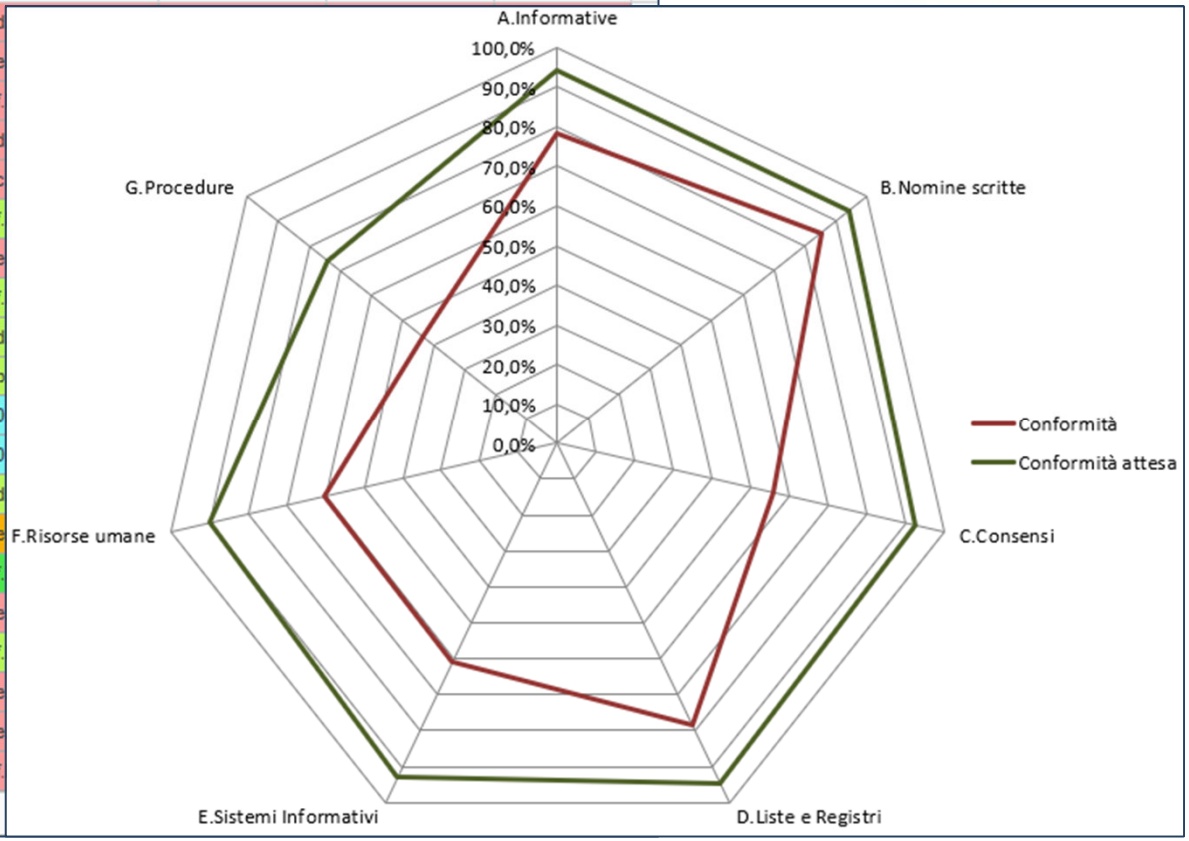
Analisi della conformità (63 elementi suggeriti)

- Informative
- Nomine
- Consensi
- Liste e Registri
- Sistema informativo
- Risorse umane
- Procedure

Conformità

Tipologia	Argomento	Oggetto	Significativo	Conformità	Note	Stato
E.Sistemi Inform...	E09: Periodicità della scadenza delle password		d			
E.Sistemi Inform...	E10: Garanzie contrattuali per errori o negligenze da parte di fornitori IT		e			
E.Sistemi Inform...	E11: Certificazione ISO 27001 per fornitori i servizi Cloud o di rete.		f.			
E.Sistemi Inform...	E12: Rispetto del principio di privacy by design e by default per i sistemi		d			
F.Risorse umane	F01: Controllo delle referenze per tutti i dipendenti e consulenti esterni che h...		c			
F.Risorse umane	F02: Formazione periodica degli autorizzati al trattamento dei dati personali.		f.			
F.Risorse umane	F03: Formazione periodica del titolare del trattamento dei dati personali e dei...		e			
F.Risorse umane	F04: Verifica formazione Responsabile del Sistema Informatico.		f.			
F.Risorse umane	F05: Verifica gestione pre-assunzione.		d			
F.Risorse umane	F06: Verifica gestione automezzi in uso al personale.		b			
F.Risorse umane	F07: Verifica gestione videosorveglianza.		0			
F.Risorse umane	F08: Verifica gestione utilizzo dei dispositivi personali.		0			
F.Risorse umane	F09: Verifica dati particolari ricavabili indirettamente.		d			
F.Risorse umane	F10: Verifica dei controlli sull'utilizzo dei sistemi informatici.	Sede e Cantieri ...	e			
G.Procedure	G01: Policy aziendale per l'utilizzo dei sistemi informativi.		f.			
G.Procedure	G02: Procedura per l'aggiornamento periodico delle informative privacy, diritti...		e			
G.Procedure	G03: Procedura per limitate l'accesso ai dati personali solo alle persone autor...		f.			
G.Procedure	G04: Procedura per il trasferimento dei dati personali su memorie esterne (U...		e			
G.Procedure	G05: Procedura relativa alla cessazione del rapporto di lavoro / collaborazione.		e			
G.Procedure	G06: Procedure per la gestione di Disaster Recovery e/o di Business Continu...		f.			

Pagina 3 di 4 20



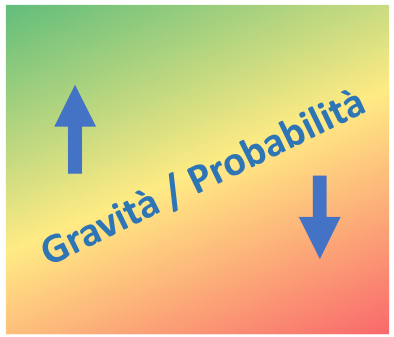
Minacce

Probabilità
A-Trascurabile (Accadimento sporadico)
B-Molto bassa (2-3 volte ogni 5 anni)
C-Bassa (< di una volta l'anno)
D-Media (< di una volta ogni 6 mesi)
E-Alta (< di una volta al mese)
F-Molto alta (> di una volta al mese)

Gravità
A-Insignificante (Di impatto minimo)
B-Minore (Non richiede sforzi extra per il ripristino, nessun accesso non autorizzato ai dati)
C-Significativo (Danno di entità tangibile che richiede sforzi extra per il ripristino e/o accesso ai dati non autorizzati limitato)
D-Serio (Danno che richiede un significativo impiego di risorse o all'immagine ed alla credibilità aziendale)
E-Molto serio (Danno esteso che comporta la compromissione di una grande quantità di dati o servizi)
F-Grave (Compromissione completa)

Rischio		Frequenza						
		Non significativo	Accadimento sporadico	2-3 volte ogni 5 anni	< di una volta l'anno	< di una volta ogni 6 mesi	< di una volta al mese	> di una volta al mese
Gravità	Non significativo	Trascurabile	Trascurabile	Trascurabile	Trascurabile	Trascurabile	Trascurabile	Trascurabile
	Di impatto minimo	Trascurabile	Trascurabile	Basso	Basso	Basso	Medio	Medio
	Non richiede sforzi extra per il ripristino, nessun accesso non autorizzato ai dati	Trascurabile	Basso	Medio	Medio	Medio	Alto	Alto
	Danno di entità tangibile che richiede sforzi extra per il ripristino e/o accesso ai dati non autorizzati limitato	Trascurabile	Medio	Alto	Alto	Alto	Critico	Critico
	Danno che richiede un significativo impiego di risorse o all'immagine ed alla credibilità aziendale	Trascurabile	Alto	Critico	Critico	Critico	Estremo	Estremo
	Danno esteso che comporta la compromissione di una grande quantità di dati o servizi	Trascurabile	Critico	Estremo	Estremo	Estremo	Estremo	Estremo
	Compromissione completa	Trascurabile	Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

Impatto	Probabilità minaccia: Basso	Medio	Alto
Basso	Basso	Basso	Medio
Medio	Basso	Medio	Alto
Alto	Medio	Alto	Alto



Linea Guida ENISA / Impatto	Probabilità minaccia: Basso	Medio	Alto
Basso	Basso	Basso	Medio
Medio	Medio	Medio	Alto
Alto	Alto	Alto	Alto

Minacce

Tipologia	Minacce
A.Eventi naturali	Incendi, Allagamenti, Nevicate. Terremoti. Fulmini.
B.Fisici intenzionali	Furto di apparati e/o supporti informatici. Distruzione di apparati e/o supporti informatici. Furto di documenti. Accesso non autorizzato ai locali. Manomissione e falsificazione di documenti. Copia non autorizzata di documenti. Lettura non autorizzata di dati da schermate video. Attacchi terroristici.
C.Problemi tecnici	Perdita di energia (o sbalzi di tensione). Rottura i sulle linee TLC. Saturazione dei sistemi IT. Guas IT. Perdita o distruzione dei dati su arc i inform massa). Errori di manutenzione hardware e softw componente della rete.
D.Tecnici intenzionali	Elusione dei meccanismi di login o furto di identit su archivi informatici. Copia non autorizzata di da autorizzato agli elaboratori, software di base e ap programmi applicativi. Copia illegale di software. dati di business. Infiltrazione virus. Lettura non au
E.Organizzativi	Mancata o insufficiente definizione di ruoli e resp delle procedure. Trattamenti non conformi alle fin dipendenti e/o esterni. Inadempienza da parte de (malattie, sciopero, eccetera).
F.Compromis- sioni informazioni	Intercettazione (inclusa analisi del traffico), infiltra da origini non affidabili. Recupero di informazioni di informazioni (da parte del personale).
G.Servizi offerti	Uso dei servizi da parte di persone non autorizza

Codice	Tipologia	Minaccia	Probabilità	Gravità	Rischio	Misure	Note	Riserv	Integrit	Dispon	Resp.Mis.Agg.
A01	A.Eventi naturali	Incendi, Allagamenti, Nevicate	Trascurabile (Ac...	Molto serio (...	Critico	Nella sede s...		No	No	Si	Resp. Sistemi In...
A02	A.Eventi naturali	Terremoti	Non significativo	Molto serio (	Trascurabile	La sede non...		No	No	Si	
A03	A.Eventi naturali	Fulmini	Bassa (< di una ...	Significativo ...	Alto	La sede è pr...		No	No	Si	
B01	B.Fisici intenzio...	Furto di apparati e/o supporti informa...	Trascurabile (Ac...	Serio (Dann...	Alto	La sede è d...		Si	No	Si	
B02	B.Fisici intenzio...	Distruzione di apparati e/o suppor						lo	No	Si	
B03	B.Fisici intenzio...	Furto di documenti						i	No	Si	
B04	B.Fisici intenzio...	Accesso non autorizzato ai locali						i	No	No	
B05	B.Fisici intenzio...	Manomissione e falsificazione di d						lo	Si	No	
B06	B.Fisici intenzio...	Copia non autorizzata di documen						i	No	No	
B07	B.Fisici intenzio...	Lettura non autorizzata di dati da						i	No	No	
B08	B.Fisici intenzio...	Attacchi terroristici						lo	No	Si	
C01	C.Problemi tecnici	Perdita di energia (o sbalzi di tens						lo	Si	Si	
C02	C.Problemi tecnici	Rottura impianti raffreddamento						lo	Si	Si	
C03	C.Problemi tecnici	Eccesso di traffico sulle linee TLC						lo	No	Si	
C04	C.Problemi tecnici	Saturazione dei sistemi IT	Molto bassa (2-...	Minore (Non...	Medio	I sistemi son...		No	No	Si	
C05	C.Problemi tecnici	Guasto o malfunzionamento della str...	Media (< di una ...	Minore (Non...	Medio	Per tutta la s...		No	No	Si	
C06	C.Problemi tecnici	Perdita o distruzione dei dati su archi...	Molto bassa (2-...	Significativo ...	Alto	Gli utenti ha...					
C07	C.Problemi tecnici	Degrado dei media (memorie di mas...	Trascurabile (Ac...	Significativo ...	Medio	Tutti i dati so...					
C08	C.Problemi tecnici	Errori di manutenzione hardware e s...	Trascurabile (Ac...	Serio (Dann...	Alto	La manuten...					
C09	C.Problemi tecnici	Errori da software	Bassa (< di una ...	Minore (Non...	Medio	I software re...		Si	Si	Si	

Collegate alle 45 minace proposte dalla Commissione Nazionale francese per l'Informatica e le Libertà:
23 relative alla Disponibilità
14 relative alla Riservatezza
8 relative alla Integrità

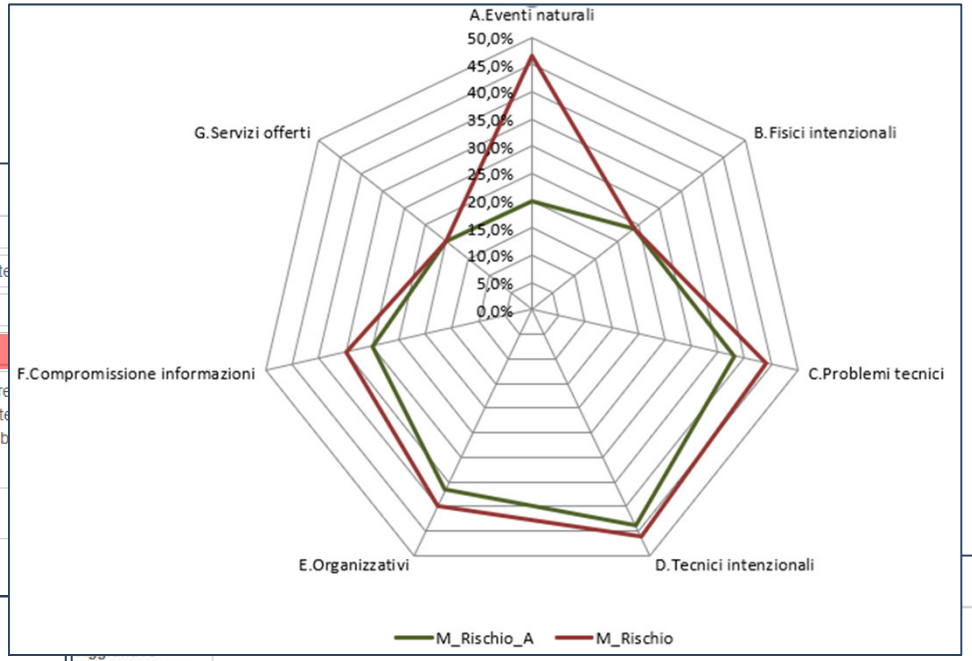
CNIL. Commission Nationale de l'Informatique et des Libertés

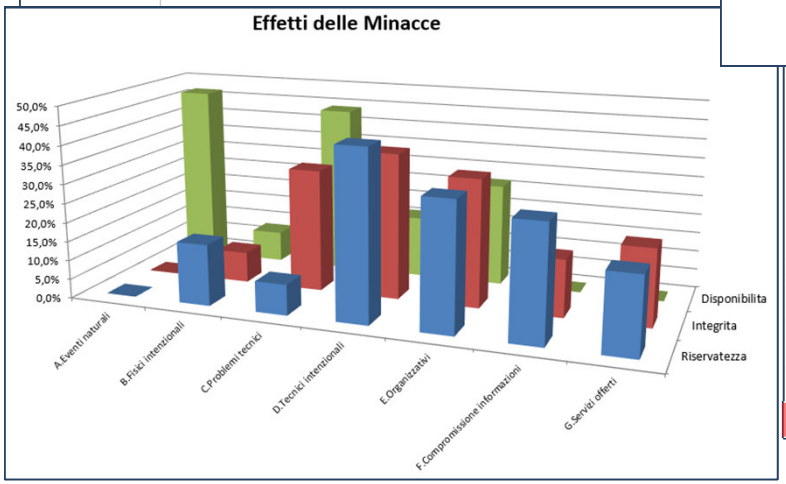
41 Minacce

Minacce

Base | Misure_Aggiuntive | CNIL

Codice	D04	Tipologia	D.Tecnici intenzionali
Minaccia	Accesso non autorizzato agli elaboratori, software di base e apparati di rete		
Oggetto			
Probabilità		Gravità	
Misure	es: La sala Server è chiusa a chiave. Gli armadi di rete sono collocati in are I dispositivi di rete sono configurati in modo da limitare gli accessi ai soli ute Tutte le password di sistema sono note unicamente al RSI ed ai suoi collab conservata in busta chiusa dall'Amministratore Delegato.		
Riservatezza	✔	Integrità	✔
Disponibilità	✔		
Note			





Responsabile per le Misure aggiuntive	Resp. Sistemi Informatici		
Risorse			
Tempi	Entro il prossimo anno		
Criteri per la Valutazione dei risultati			
Probabilità_attesa	B: Molto bassa (2-3 volte ogni 5 anni)	Gravità_attesa	B: Minore (Non richiede sforzi extra per il ripristino, nessun accesso non autorizzato ai dati)

Inventario

Apparati

Codice: Ser01 | Apparato: Server 01
Tipologia: Server | Sist.Op.: Small Business 2011
Funzioni: File e Exchange
Metodo Aggiornamento: Sito Microsoft
Criticità: Accesso alle cartelle del Server.
Posta
Continuità: Assistenza HP
Responsabile: Verdi Antonio. | Ultima Verifica: 10/01/2018 | Mesi Verifica
Note: Macchina da sostituire

N27_Sistema_Apparati_ALL — Allegati relativi all'Apparato: Server 01

Azione	Descrizione	Note
	Contratto di Manutenzione	

Data Base

N27_Sistema_DataBase — Data Base
Codice: DB-01 | Data Base: DB Amministrativo
Funzioni: Gestione di tutti i dati amministrativi
Tipologia: Dati contabili
Utenti abilitati: Ufficio Amministrativo
Necessità di Aggiornamento: Controllo dati inseriti
Responsabile: Resp. Sistemi Informatici | Ultima Verifica: 01/03/2019 | Mesi Verifica: 12
Note

Prodotti

Codice: Word | Prodotto: Microsoft WORD
Tipologia: Produttività Individuale
Funzioni: Gestione testi
Metodo Aggiornamento: Sito Microsoft
Responsabile: Verdi Antonio. | Ultima Verifica: gg/mm/aaaa
Note

N27_Sistema_Prodotti_ALL — Allegati relativi al Prodotto: Microsoft WORD

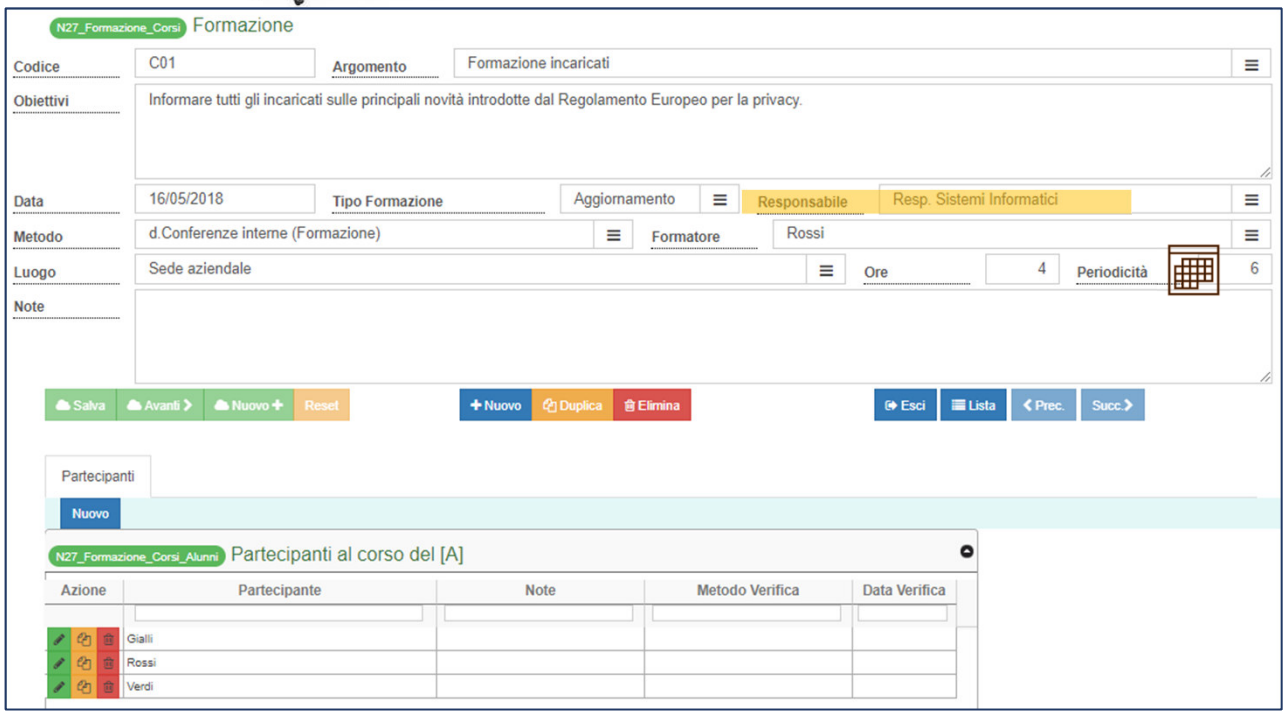
Azione	Descrizione	Note
	a. Licenza d'uso	
	b. Contratto di assistenza	

Dispositivi mobili

N27_Sistema_DispMob — Dispositivi Mobili
Codice: CELL01 | Apparato: Cellulare 1
Assegnatario: Antonio Verdi | Aziendale: ✓
Applicazioni: Posta aziendale.
DropBox con accesso completo.
Responsabile: Resp. Sistemi Informatici | Ultima Verifica: gg/mm/aaaa | Mesi Verifica
Note

Informazioni sul SGSI e Dati personali

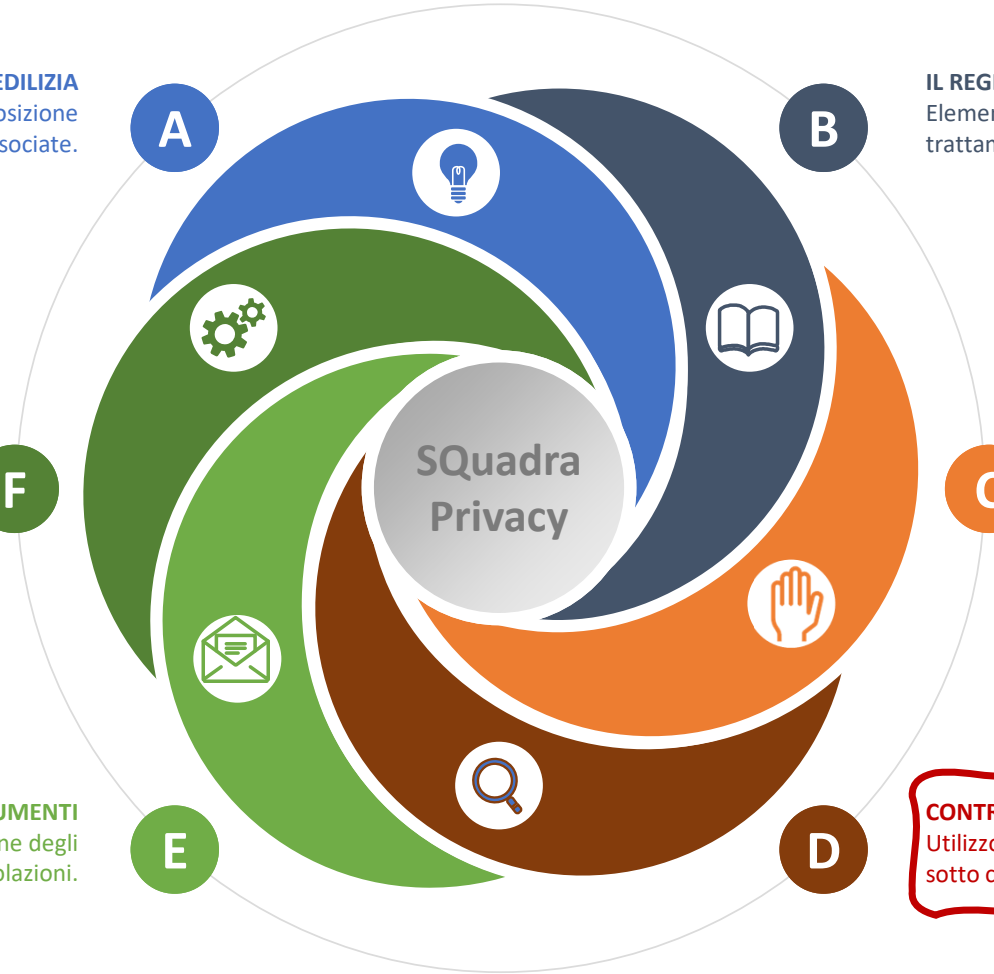
Chiunque abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso (Art. 29)



SQuadra-Privacy

IL PROGETTO SQUADRA-EDILIZIA
Dal 2008 uno strumento a disposizione delle imprese associate.

IL REGISTRO DEI TRATTAMENTI
Elemento essenziale per l'analisi dei trattamenti effettuati.



SICUREZZA DELLE INFORMAZIONI
Problematiche tipiche e specifiche relative all'utilizzo delle nuove tecnologie.

CONFORMITÀ E MINACCE
Autovalutazione della situazione di partenza e degli obiettivi.

ALTRI STRUMENTI
Documenti aggiuntivi e gestione degli incidenti e delle violazioni.

CONTROLLI
Utilizzo delle migliori pratiche per tenere sotto controllo i sistemi informatici.

Sicurezza delle informazioni

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Decreto legislativo 30 giugno 2003, n. 196

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Misure Minime

Misure Adeguate

European Commission

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

TITOLARE e RESPONSABILE, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto, delle finalità del trattamento e dei rischi (probabilità e impatto) per i diritti e le libertà degli interessati, devono mettere in atto MISURE per garantire un livello di sicurezza ADEGUATO (Art.32).

MISURE TECNICHE

Pseudonimizzazione, Cifratura, Anonimizzazione.

MISURE ORGANIZZATIVE

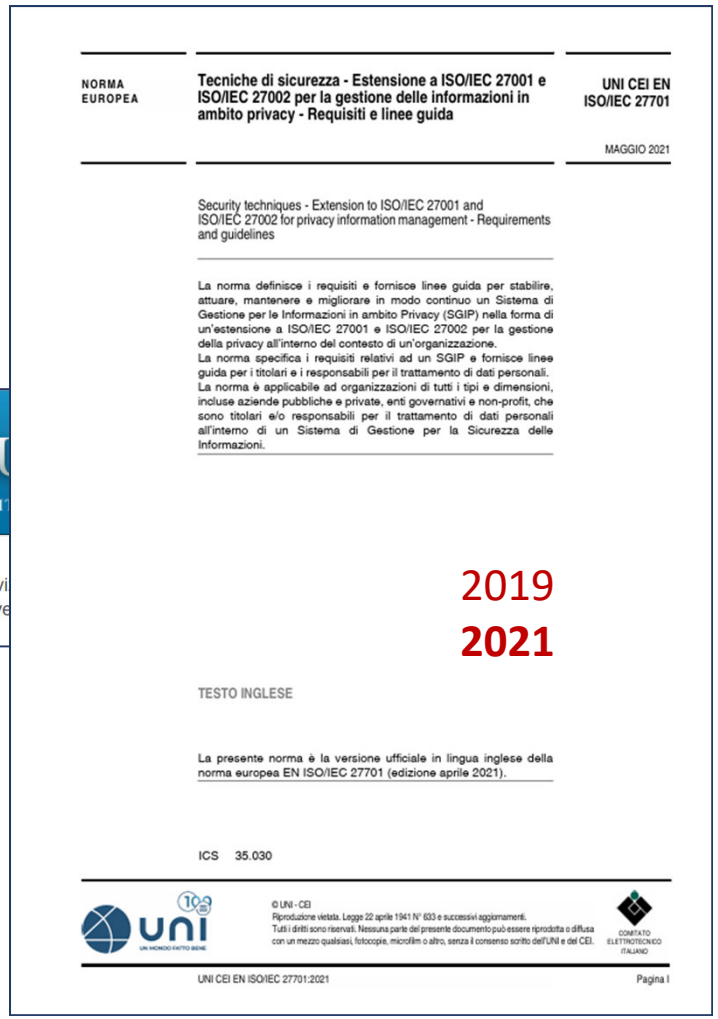
Provare, verificare e valutare periodicamente le misure tecniche.

Assicurare la continua riservatezza, integrità e resilienza dei sistemi e dei servizi.

Ripristinare tempestivamente la disponibilità in caso di incidenti.

Misure minime – Migliori prassi (2018)

Misure minime – Migliori prassi (2024)



Riferimenti

INTERNATIONAL STANDARD **ISO/IEC 27002**

Third edition 2022-02 — Corrected version 2022-03

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

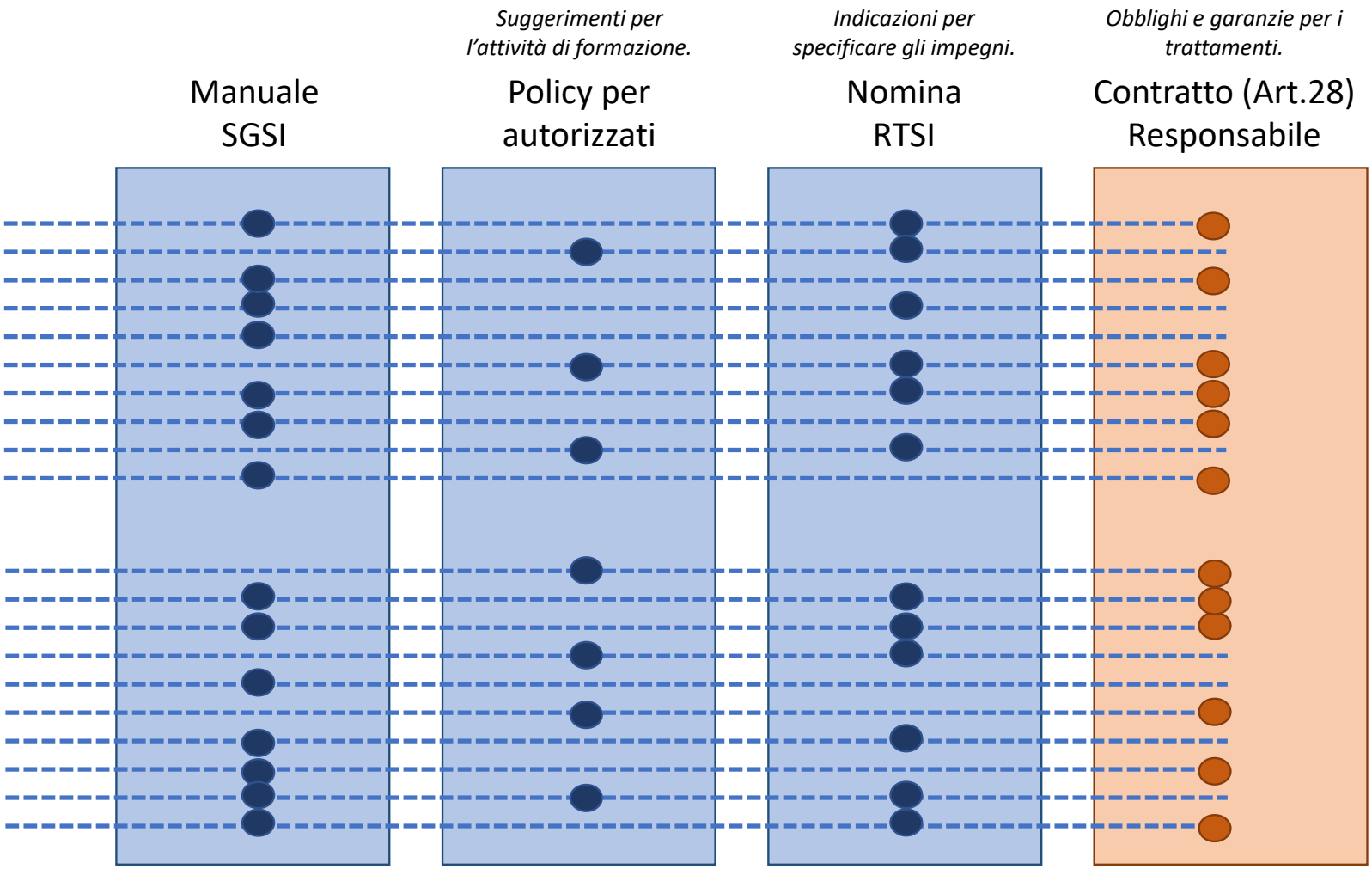
Reference number ISO/IEC 27002:2022(E)

INTERNATIONAL STANDARD **ISO/IEC 27701**

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

Reference number ISO/IEC 27701:2019(E)



Riferimenti fra i vari controlli

Agenzia per l'Italia Digitale

CIS SAPIENZA
Cyber Intelligence and Information Security

2015 Italian Cyber Security Report

Un Framework Nazionale per la Cyber Security

Research Center of Cyber Intelligence and Information Security
Sapienza Università di Roma

Laboratorio Nazionale CINI di Cyber Security
Consorzio Interuniversitario Nazionale per l'Informatica

Versione 1.0
Febbraio 2016

cini Cyber Security National Lab

CIS SAPIENZA
Cyber Intelligence and Information Security

2016 Italian Cybersecurity Report

Controlli Essenziali di Cybersecurity

Research Center of Cyber Intelligence and Information Security
Sapienza Università di Roma

Laboratorio Nazionale CINI di Cybersecurity
Consorzio Interuniversitario Nazionale per l'Informatica

Versione 1.0
Marzo 2017

cini Cybersecurity National Lab

Controlli


International Organization for Standardization
ISO
27001
AGID
PMI

Controlli


International Organization for Standardization
ISO
27001
AGID
PMI

Controlli 27001

Guida attuativa

Nell'uso dei dispositivi portatili dovrebbe essere prestata particolare attenzione per assicurare che le informazioni di business non vengano compromesse. La politica per i dispositivi portatili dovrebbe prendere in considerazione i rischi creati dal lavoro con dispositivi portatili in ambienti non protetti.

La politica per i dispositivi portatili dovrebbe considerare:

- *a) la registrazione dei dispositivi portatili;*
- *b) i requisiti per la loro protezione fisica;*
- *c) le limitazioni all'installazione di software;*
- *d) i requisiti per il software dei dispositivi portatili e per l'applicazione di patch;*
- *e) la limitazione della connessione a servizi informatici;*
- *f) i controlli di accesso;*
- *g) le tecniche crittografiche;*
- *h) la protezione da malware;*
- *i) la disabilitazione, cancellazione o il blocco remoti;*
- *j) i backup;*
- *k) l'uso di servizi e applicazioni web.*

Dovrebbe essere prestata attenzione nell'impiego di dispositivi portatili in aree pubbliche, sale riunioni e altre zone non protette. Dovrebbero essere presenti protezioni per evitare l'accesso non autorizzato o la divulgazione delle informazioni memorizzate ed elaborate da tali dispositivi, per esempio utilizzando tecniche crittografiche (vedere punto 10) e impostando la richiesta di informazioni segrete per l'autenticazione (vedere punto 9.2.4).

I dispositivi portatili dovrebbero anche essere protetti fisicamente contro il furto, in particolar modo quando lasciati, ad esempio, in automobili o altri mezzi di trasporto, camere di albergo, centri conferenze e luoghi di riunione. Dovrebbe essere stabilita una specifica procedura che tenga in considerazione i requisiti cogenti, assicurativi e altri requisiti di sicurezza dell'organizzazione per i casi di furto o smarrimento dei dispositivi portatili. I dispositivi che trasportano informazioni di business importanti o critiche non dovrebbero essere lasciati incustoditi e, quando possibile, dovrebbero essere bloccati fisicamente o chiusi a chiave con lucchetti speciali.

Base | Misure_Aggiuntive | Suggerimenti

Area A.06: Organizzazione della sicurezza delle informazioni

Obiettivo 2.Dispositivi portatili e telelavoro

Codice 1 **Descrizione** Politica per i dispositivi portatili

Controllo Deve essere adottata una politica e delle misure di sicurezza a suo supporto per la gestione dei rischi introdotti dall'uso di dispositivi portatili.

Misure Attualmente non viene utilizzata la crittografia.
Gli autorizzati al trattamento sono formati sulla necessità di non memorizzare dati riservati sui dispositivi portati

Note

Riferimenti MSI: Politica della Sicurezza. - Criteri per l'uso della crittografia. / Policy e Prescri

Significatività 0: Non Significativa **Valutazione** c: Parzialmente applicato

Valutazione Esiste un programma di gestione e controllo del rischio tale che controlli, politiche
principali cambiamenti organizzativi/di processo. L'efficacia operativa delle attività
Un processo di divulgazione degli eventi è attuato e adeguatamente documentato

Valutazione attesa a: Applicato e formalizzato **Conformità attesa**

Base | Misure_Aggiun

Misure Aggiuntive Dovrà es

Responsabile per le Misure a

Risorse Utilizzo

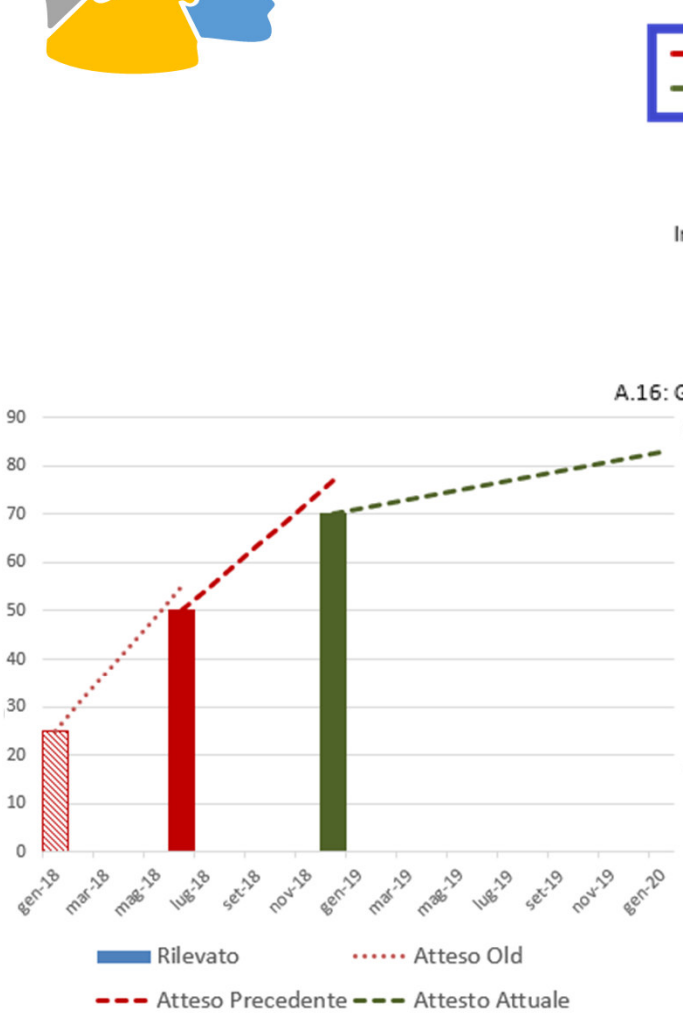
Tempi Entro la

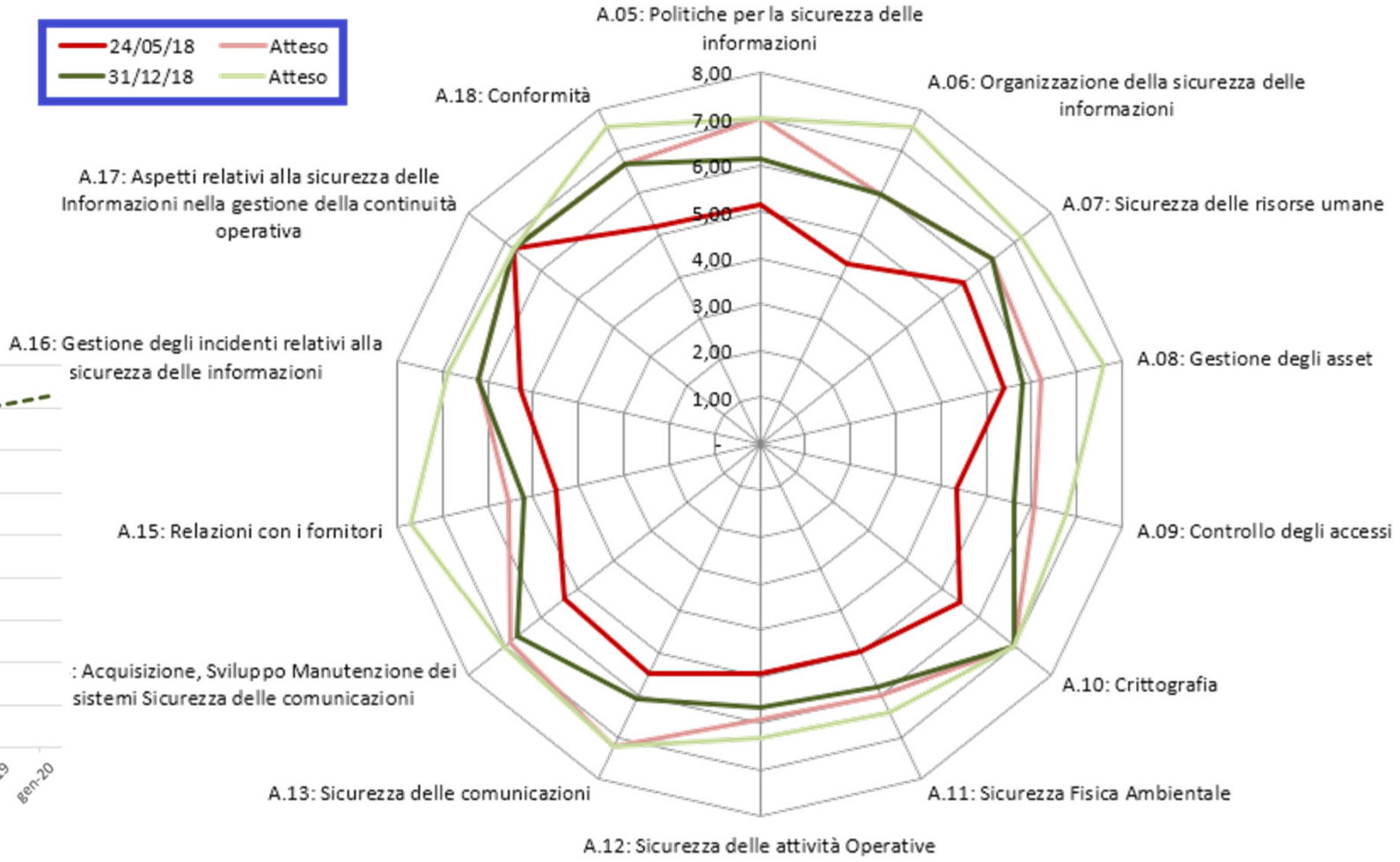
Criteri per la Valutazione dei risultati

Azione	Area	Obiettivo	C	Descrizione	Controllo	Misure	Riferimento	Note	Significativi	Valutazione	Resp.Mis.A
	A.05: Politi…	1.Indirizzi d…	1	Politiche per la sicurezza delle infor…	Un insieme di politiche per la sicurez…	Manuale dei Sist…	Manuale		d.Alta	a.Applicato …	Resp. Siste…
	A.05: Politi…	1.Indirizzi d…	2	Riesame delle politiche per la sicure…	Le politiche per la sicurezza delle inf…	Riesame della D…	MSI: Politica…		e.Molto Alta	b.Applicato …	
	A.06: Orga…	1.Organizz…	1	Ruoli e responsabilità per la sicurezz…	Tutte le responsabilità relative alla si…	SQuadra GDPR:…	MSI: Descriz…		d.Alta	a.Applicato …	
	A.06: Orga…	1.Organizz…	2	Separazione dei compiti	I compiti e le aree di responsabilità in…	n.a.			0.Non Signifi…	0.Non applic…	
	A.06: Orga…	1.Organizz…	3	Contatti con le autorità	Devono essere mantenuti appropriati…	n.a.			b.Bassa	0.Non applic…	
	A.06: Orga…	1.Organizz…	4	Contatti con gruppi specialistici	Devono essere mantenuti appropriati…	Aggiornamenti s…	MSI: Respo…		d.Alta	c.Parzialme…	
	A.06: Orga…	1.Organizz…	5	Sicurezza delle informazioni nella ge…	La sicurezza delle informazioni deve …	Programmi appli…	MSI: Respo…		d.Alta	d.Previsto m…	
	A.06: Orga…	2.Dispositiv…	1	Politica per i dispositivi portatili	Deve essere adottata una politica e …	Attualmente non…	MSI: Politica…		0.Non Signifi…	c.Parzialme…	Resp. Siste…
	A.06: Orga…	2.Dispositiv…	2	Telelavoro	Devono essere attuate una politica e…	Policy e Prescriz…	MSI: Politica…		e.Molto Alta	b.Applicato …	Resp. Siste…
	A.07: Sicur…	1.Prima del…	1	Screening	Devono essere svolti dei controlli per…	n.a.			f.Altissima	0.Non applic…	
	A.07: Sicur…	1.Prima del…	2	Termini e condizioni di impiego	Gli accordi contrattuali con il persona…	Nomina degli inc…			f.Altissima	c.Parzialme…	
	A.07: Sicur…	2.Durante l'…	1	Responsabilità della direzione	La direzione deve richiedere a tutto il…	Policy e Prescriz…	Policy		d.Alta	b.Applicato …	Resp. Siste…
	A.07: Sicur…	2.Durante l'…	2	Consapevolezza, istruzione, formazi…	Tutto il personale dell'organizzazione…	Tutto il personal…	MSI: Formaz…		d.Alta	d.Previsto m…	
	A.07: Sicur…	2.Durante l'…	3	Processo disciplinare	Deve essere istituito un processo dis…	Contratto di lavo…			e.Molto Alta	c.Parzialme…	
	A.07: Sicur…	3.Cessazio…	1	Cessazione o variazione delle respo…	Le responsabilità e i doveri relativi all…	Policy: Cessazio…	MSI: Respo…		f.Altissima	c.Parzialme…	
	A.08: Gesti…	1.Respons…	1	Inventario degli asset	Tutti gli asset associati alle informazi…	SQuadra GDPR:…			b.Bassa	e.Non prese…	
	A.08: Gesti…	1.Respons…	2	Responsabilità degli asset	Gli asset censiti nell'inventario devon…	SQuadra GDPR:…			b.Bassa	e.Non prese…	
	A.08: Gesti…	1.Respons…	3	Utilizzo accettabile degli asset	Le regole per l'utilizzo accettabile del…	Policy: Utilizzo d…			b.Bassa	c.Parzialme…	
	A.08: Gesti…	1.Respons…	4	Restituzione degli asset	Tutto il personale e gli utenti di parti …	Policy: Cessazio…			0.Non Signifi…	d.Previsto m…	
	A.08: Gesti…	2.Classifica…	1	Classificazione delle informazioni	Le informazioni devono essere classi…	SQuadra GDPR:…			b.Bassa	a.Applicato …	

Pagina 1 di 6 20 Righe 1 - 20 di 114

Analisi conformità





ISO 27701

Estensione
a ISO/IEC 27001
e ISO/IEC 27002
per la gestione delle informazioni sulla privacy

PIMS-specific guidance related to ISO/IEC 27002
6.1 General
6.2 Information security policies
6.2.1 Management direction for information security
6.3 Organization of information security
6.3.1 Internal organization
6.3.2 Mobile devices and teleworking
6.4 Human resource security
6.4.1 Prior to employment
6.4.2 During employment
6.4.3 Termination and change of employment
6.5 Asset management
6.5.1 Responsibility for assets
6.5.2 Information classification
6.5.3 Media handling
6.6 Access control
6.6.1 Business requirements of access control
6.6.2 User access management
6.6.3 User responsibilities
6.6.4 System and application access control
6.7 Cryptography
6.7.1 Cryptographic controls
6.8 Physical and environmental security
6.8.1 Secure areas
6.8.2 Equipment
6.9 Operations security
6.9.1 Operational procedures and responsibilities
6.9.2 Protection from malware
6.9.3 Backup
6.9.4 Logging and monitoring
6.9.5 Control of operational software
6.9.6 Technical vulnerability management
6.9.7 Information systems audit considerations
6.10 Communications security
6.10.1 Network security management
6.10.2 Information transfer
6.11 Systems acquisition, development and maintenance
6.11.1 Security requirements of information systems
6.11.2 Security in development and support processes
6.11.3 Test data
6.12 Supplier relationships
6.12.1 Information security in supplier relationships
6.12.2 Supplier service delivery management
6.13 Information security incident management
6.13.1 Management of information security incidents and improvements
6.14 Information security aspects of business continuity management
6.14.1 Information security continuity
6.14.2 Redundancies
6.15 Compliance
6.15.1 Compliance with legal and contractual requirements
6.15.2 Information security reviews

Additional ISO/IEC 27002 guidance for PII controllers
7.1 General
7.2 Conditions for collection and processing
7.2.1 Identify and document purpose
7.2.2 Identify lawful basis
7.2.3 Determine when and how consent is to be obtained
7.2.4 Obtain and record consent
7.2.5 Privacy impact assessment
7.2.6 Contracts with PII processors
7.2.7 Joint PII controller
7.2.8 Records related to processing PII
7.3 Obligations to PII principals
7.3.1 Determining and fulfilling obligations to PII principals
7.3.2 Determining information for PII principals
7.3.3 Providing information to PII principals
7.3.4 Providing mechanism to modify or withdraw consent
7.3.5 Providing mechanism to object to PII processing
7.3.6 Access, correction and/or erasure
7.3.7 PII controllers' obligations to inform third parties
7.3.8 Providing copy of PII processed
7.3.9 Handling requests
7.3.10 Automated decision making
7.4 Privacy by design and privacy by default
7.4.1 Limit collection
7.4.2 Limit processing
7.4.3 Accuracy and quality
7.4.4 PII minimization objectives
7.4.5 PII de-identification and deletion at the end of processing
7.4.6 Temporary files
7.4.7 Retention
7.4.8 Disposal
7.4.9 PII transmission controls
7.5 PII sharing, transfer, and disclosure
7.5.1 Identify basis for PII transfer between jurisdictions
7.5.2 Countries and international organizations to which PII can be transferred
7.5.3 Records of transfer of PII
7.5.4 Records of PII disclosure to third parties
Additional ISO/IEC 27002 guidance for PII processors
8.1 General
8.2 Conditions for collection and processing
8.2.1 Customer agreement
8.2.2 Organization's purposes
8.2.3 Marketing and advertising use
8.2.4 Infringing instruction
8.2.5 Customer obligations
8.2.6 Records related to processing PII
8.3 Obligations to PII principals
8.3.1 Obligations to PII principals
8.4 Privacy by design and privacy by default
8.4.1 Temporary files
8.4.2 Return, transfer or disposal of PII
8.4.3 PII transmission controls
8.5 PII sharing, transfer, and disclosure
8.5.1 Basis for PII transfer between jurisdictions
8.5.2 Countries and international organizations to which PII can be transferred
8.5.3 Records of PII disclosure to third parties
8.5.4 Notification of PII disclosure requests
8.5.5 Legally binding PII disclosures
8.5.6 Disclosure of subcontractors used to process PII
8.5.7 Engagement of a subcontractor to process PII
8.5.8 Change of subcontractor to process PII

ISO 27002:2022

A.5 Politiche per la sicurezza delle informazioni		
A.5.1 Indirizzi della direzione per la sicurezza delle informazioni		
Obiettivo: Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni in accordo con i requisiti di business, con le leggi e co i regolamenti pertinenti.		
A.5.1.1	Politiche per la sicurezza delle informazioni	*Controllo* Un insieme di politiche per la sicurezza delle informazioni deve essere definito approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti.
A.5.1.2	Riesame delle politiche per la sicurezza delle informazioni	*Controllo* Le politiche per la sicurezza delle informazioni devono essere riesaminate ad intervalli pianificati o nel caso in cui si siano verificati cambiamenti significativi al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.
A.6 Organizzazione della sicurezza delle informazioni		
A.6.1 Organizzazione interna		
Obiettivo: Stabilire un quadro di riferimento gestionale per intraprendere e controllare l'attuazione e l'esercizio della sicurezza delle informazioni all'interno dell'organizzazione.		
A.6.1.1	Ruoli e responsabilità per la sicurezza delle informazioni	*Controllo* Tutte le responsabilità relative alla sicurezza delle informazioni devono essere definite e assegnate.
A.6.1.2	Separazione dei compiti	*Controllo* I compiti e le aree di responsabilità in conflitto tra loro devono essere separati per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset dell'organizzazione.
A.6.1.3	Contatti con le autorità	*Controllo* Devono essere mantenuti appropriati contatti con le autorità pertinenti.
A.6.1.4	Contatti con gruppi specialistici	*Controllo* Devono essere mantenuti appropriati contatti con gruppi specialistici o altri forum ed associazioni professionali frequentate da specialisti della sicurezza delle informazioni.
A.6.1.5	Sicurezza delle informazioni nella gestione dei progetti	*Controllo* La sicurezza delle informazioni deve essere indirizzata nell'ambito della gestione dei progetti, a prescindere dal tipo di progetto.
A.6.2 Dispositivi portatili e telelavoro		
Obiettivo: Assicurare la sicurezza del telelavoro e nell'uso di dispositivi portatili		
A.6.2.1	Politica per i dispositivi portatili	*Controllo* Deve essere adottata una politica e delle misure di sicurezza a suo supporto per la gestione dei rischi introdotti dall'uso di dispositivi portatili.
A.6.2.2	Telelavoro	*Controllo* Devono essere attuate una politica e delle misure di sicurezza a suo supporto per proteggere le informazioni consultate, elaborate o memorizzate presso siti di telelavoro.

Organizational controls

5.1	Policies for information security
5.2	Information security roles and responsibilities
5.3	Segregation of duties
5.4	Management responsibilities
5.5	Contact with authorities
5.6	Contact with special interest groups
5.7	Threat intelligence
5.8	Information security in project management
5.9	Inventory of information and other associated assets
5.10	Acceptable use of information and other associated assets
5.11	Return of assets
5.12	Classification of information
5.13	Labelling of information
5.14	Information transfer
5.15	Access control
5.16	Identity management
5.17	Authentication information
5.18	Access rights
5.19	Information security in supplier relationships
5.20	Addressing information security within supplier agreements
5.21	Managing information security in the ICT supply chain
5.22	Monitoring, review and change management of supplier services
5.23	Information security for use of cloud services
5.24	Information security incident management planning and preparation
5.25	Assessment and decision on information security events
5.26	Response to information security incidents
5.27	Learning from information security incidents
5.28	Collection of evidence
5.29	Information security during disruption
5.30	ICT readiness for business continuity
5.31	Legal, statutory, regulatory and contractual requirements
5.32	Intellectual property rights
5.33	Protection of records
5.34	Privacy and protection of PII
5.35	Independent review of information security
5.36	Compliance with policies, rules and standards for information security
5.37	Documented operating procedures

People controls

6.1	Screening
6.2	Terms and conditions of employment
6.3	Information security awareness, education and training
6.4	Disciplinary process
6.5	Responsibilities after termination or change of employment
6.6	Confidentiality or non-disclosure agreements
6.7	Remote working
6.8	Information security event reporting

Physical controls

7.1	Physical security perimeters
7.2	Physical entry
7.3	Securing offices, rooms and facilities
7.4	Physical security monitoring
7.5	Protecting against physical and environmental threats
7.6	Working in secure areas
7.7	Clear desk and clear screen
7.8	Equipment siting and protection
7.9	Security of assets off-premises
7.10	Storage media
7.11	Supporting utilities
7.12	Cabling security
7.13	Equipment maintenance
7.14	Secure disposal or re-use of equipment

Technological controls

8.1	User endpoint devices
8.2	Privileged access rights
8.3	Information access restriction
8.4	Access to source code
8.5	Secure authentication
8.6	Capacity management
8.7	Protection against malware
8.8	Management of technical vulnerabilities
8.9	Configuration management
8.10	Information deletion
8.11	Data masking
8.12	Data leakage prevention
8.13	Information backup
8.14	Redundancy of information processing facilities
8.15	Logging
8.16	Monitoring activities
8.17	Clock synchronization
8.18	Use of privileged utility programs
8.19	Installation of software on operational systems
8.20	Networks security
8.21	Security of network services
8.22	Segregation of networks
8.23	Web filtering
8.24	Use of cryptography
8.25	Secure development life cycle
8.26	Application security requirements
8.27	Secure system architecture and engineering principles
8.28	Secure coding
8.29	Security testing in development and acceptance
8.30	Outsourced development
8.31	Separation of development, test and production environments
8.32	Change management
8.33	Test information
8.34	Protection of information systems during audit testing

Aggiornamento delle Norme

ISO 27001

Codice	Desc
04.1	Comprendere l'organizzazione e il suo
04.2	Comprendere le necessità e le aspetta
04.3	Determinare il campo di applicazione
04.4	Sistema di gestione per la sicurezza d
05.1	Leadership e impegno
05.2	Politica
05.3	Ruoli, responsabilità e autorità nell'org
06.1.1	Azioni per affrontare rischi e opportuni
06.1.2	Valutazione del rischio relativo alla sic
06.1.3	Trattamento del rischio relativo alla sic
06.2	Obiettivi per la sicurezza delle informa
07.1	Risorse
07.2	Competenza
07.3	Consapevolezza
07.4	Comunicazione
07.5.1	Informazioni documentate - Generalità
07.5.2	Informazioni documentate - Creazione
07.5.3	Controllo delle informazioni document
08.1	Pianificazione e controllo operativi

Pagina 1 di 2 20 Righe 1 - 20 di 26

ISO 27002

Codi	Descrizione
5.01	Politiche per la sicurezza delle informazioni
5.02	Ruoli e responsabilità della sicurezza delle infor
5.03	Segregazione dei compiti
5.04	Responsabilità di gestione
5.05	Contatto con le autorità
5.06	Contatto con gruppi di interesse speciali
5.07	Informazioni sulle minacce
5.08	Sicurezza delle informazioni nella gestione dei
5.09	Inventario delle informazioni e di altri beni asso
5.10	Uso accettabile delle informazioni e di altri beni
5.11	Ritorno delle attività
5.12	Classificazione delle informazioni
5.13	Etichettatura delle informazioni
5.14	Trasferimento di informazioni
5.15	Controllo dell'accesso
5.16	Gestione dell'identità
5.17	Informazioni sull'autenticazione
5.18	Diritti di accesso
5.19	Sicurezza delle informazioni nelle relazioni con i fornitori

I processi e le procedure dovrebbero... Mantenere un livello concordato di sicurezza delle informazioni nelle relazioni con i fornitori.

Pagina 1 di 5 20 Righe 1 - 20 di 93

ISO 27701

Codice	Descrizione	Controllo
N6.02.1.1	Politiche per la sicurezza delle informazioni	Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e co...
N6.03.1.1	Ruoli e responsabilità per la sicurezza delle informazioni	Tutte le responsabilità relative alla sicurezza delle informazioni devono essere definite e assegnate.
N6.03.2.1	Politica per i dispositivi portatili	Deve essere adottata una politica e delle misure di sicurezza a suo supporto per la gestione dei rischi introdotti dall'uso di...
N6.04.2.2	Consapevolezza, istruzione, formazione e addestramento ...	Tutto il personale dell'organizzazione e, quando pertinente, i collaboratori, devono ricevere un'adeguata sensibilizzazione,...
N6.05.2.1	Classificazione delle informazioni	Le informazioni devono essere classificate in relazione al loro valore, ai requisiti cogenti e alla criticità, in caso di divulgazi...
N6.05.2.2	Etichettatura delle informazioni	Deve essere sviluppato e attuato un appropriato insieme di procedure per l'etichettatura delle informazioni in base allo sc...
N6.05.3.1	Gestione dei supporti rimovibili	Devono essere sviluppate procedure per il trattamento dei supporti rimovibili in base allo schema di classificazione adotta...
N6.05.3.2	Dismissione dei supporti	La dismissione dei supporti non più necessari deve avvenire in modo sicuro, attraverso l'utilizzo di procedure formali
N6.05.3.3	Trasporto dei supporti fisici	I supporti che contengono informazioni devono essere protetti da accessi non autorizzati, utilizzi impropri o manomissioni ...
N6.06.2.1	Registrazione e de-registrazione degli utenti	Deve essere attuato un processo formale di registrazione e de-registrazione per abilitare l'assegnazione dei diritti di acce...
N6.06.2.2	Provisioning degli accessi degli utenti	Deve essere attuato un processo formale per l'assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenz...
N6.06.4.2	Procedure di Logon sicure	Quando richiesto dalle politiche di controllo degli accessi, l'accesso a sistemi e applicazioni deve essere controllato da pr...
N6.07.1.1	Politica sull'uso dei controlli crittografici	Deve essere sviluppata e attuata una politica sull'uso dei controlli crittografici per la protezione delle informazioni.
N6.08.2.7	Dismissione sicura o riutilizzo delle apparecchiature	Tutte le apparecchiature contenenti supporti di memorizzazione devono essere controllate per assicurare che ogni dato cr...
N6.08.2.9	Politica di schermo e scrivania puliti	Devono essere adottate sia una politica di "scrivania pulita" per i documenti ed i supporti di memorizzazione rimovibili, sia...
N6.09.3.1	Backup delle informazioni	Devono essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte ...
N6.09.4.1	Raccolta di Log degli Eventi	La registrazione dei LOG degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativ...
N6.09.4.2	Protezione delle informazioni di log	Le strutture per la raccolta dei LOG e le informazioni di log devono essere protette da manomissioni e accessi non autoriz...
N6.10.2.1	Politiche e procedure per il trasferimento delle informazioni	Devono esistere politiche, procedure e controlli formali a protezione del trasferimento delle informazioni attraverso l'uso di...

Pagina 1 di 2 20 Righe 1 - 20 di 32

ISO 27002

Obiettivo	5: Controlli organizzativi
Codice	5.01
Descrizione	Politiche per la sicurezza delle informazioni
Controllo	La politica di sicurezza delle informazioni e le politiche specifiche per ogni argomento dovrebber… riconosciute dal personale pertinente e dalle parti interessate, e riviste a intervalli programmati e…
Scopo	Assicurare la continua idoneità, adeguatezza, efficacia della direzione e del supporto per la sicu… statutari, normativi e contrattuali.
Note	

5 Controlli organizzativi

5.1 Politiche per la sicurezza delle informazioni

Tipo di controllo	Proprietà di sicurezza delle informazioni	Concetti di cybersicurezza	Capacità operative	Domini di sicurezza
#Preventivo	#Confidenzialità #Integrità #Disponibilità	#Identificare	#Governo	#Governance_e_Ecosistema #Resilienza

Controllo

La politica di sicurezza delle informazioni e le politiche specifiche per ogni argomento dovrebbero essere definite, approvate dalla direzione, pubblicate, comunicate e riconosciute dal personale pertinente e dalle parti interessate, e riviste a intervalli programmati e se si verificano cambiamenti significativi.

Scopo

Assicurare la continua idoneità, adeguatezza, efficacia della direzione e del supporto per la sicurezza delle informazioni in conformità con i requisiti aziendali, legali, statutari, normativi e contrattuali.

Guida

Al livello più alto, l'organizzazione dovrebbe definire una "politica di sicurezza delle informazioni" che sia approvata dal top management e che stabilisca l'approccio dell'organizzazione alla gestione della sua sicurezza delle informazioni.

La politica di sicurezza delle informazioni dovrebbe prendere in considerazione i requisiti derivati da:

a) strategia e requisiti aziendali;
b) regolamenti, legislazione e contratti;
c) i rischi e le minacce attuali e previsti per la sicurezza delle informazioni.

La politica di sicurezza delle informazioni dovrebbe contenere dichiarazioni riguardanti:

a) definizione di sicurezza delle informazioni;
b) obiettivi di sicurezza dell'informazione o il quadro di riferimento per fissare obiettivi di sicurezza dell'informazione;
c) principi per guidare tutte le attività relative alla sicurezza delle informazioni;
d) impegno a soddisfare i requisiti applicabili relativi alla sicurezza delle informazioni;
e) impegno al miglioramento continuo del sistema di gestione della sicurezza delle informazioni;
f) assegnazione di responsabilità per la gestione della sicurezza delle informazioni a ruoli definiti;
g) procedure per la gestione di esenzioni ed eccezioni.

L'alta direzione deve approvare qualsiasi modifica alla politica di sicurezza delle informazioni.

Ad un livello più basso, la politica di sicurezza delle informazioni dovrebbe essere supportata da politiche specifiche per argomento, se necessario, per rendere ulteriormente obbligatoria l'implementazione dei controlli di sicurezza delle informazioni. Le politiche specifiche per ogni argomento sono tipicamente strutturate per rispondere alle esigenze di determinati gruppi target all'interno di un'organizzazione o per coprire determinate aree di sicurezza. Le politiche specifiche dell'argomento dovrebbero essere allineate e complementari alla politica di sicurezza delle informazioni dell'organizzazione.

Esempi di tali argomenti includono:

a) controllo degli accessi;
b) sicurezza fisica e ambientale;

…rse;
…nformazioni;
…gestione sicura dei dispositivi endpoint degli utenti;
…denti di sicurezza delle informazioni;
…one delle chiavi;
…rattamento delle informazioni;
…nerabilità tecniche;

…lo sviluppo, la revisione e l'approvazione delle politiche specifiche …e essere assegnata al personale pertinente in base al loro appropriato livello …a tecnica. La revisione dovrebbe includere la valutazione delle opportunità …politica di sicurezza delle informazioni dell'organizzazione e delle politiche …o e la gestione della sicurezza delle informazioni in risposta ai cambiamenti:
…iness dell'organizzazione;
… dell'organizzazione;
…ti, leggi e contratti;
…zza delle informazioni;
… e previsto di minacce alla sicurezza delle informazioni;
… eventi e incidenti di sicurezza delle informazioni.

…a di sicurezza delle informazioni e delle politiche specifiche per argomento …nsiderazione i risultati delle revisioni e degli audit di gestione. La revisione …re politiche correlate dovrebbero essere considerati quando una politica …tenere la coerenza.

…elle informazioni e le politiche specifiche per argomento dovrebbero essere … pertinente e alle parti interessate in una forma che sia rilevante, accessibile …ettore previsto. Ai destinatari delle politiche dovrebbe essere richiesto di …bite e di essere d'accordo a rispettarle, ove applicabile. L'organizzazione può … e i nomi di questi documenti di politica che soddisfano le esigenze …lcune organizzazioni, la politica di sicurezza delle informazioni e le politiche …to possono essere in un unico documento. L'organizzazione può nominare …he dell'argomento come standard, direttive, politiche o altro.

Se la politica di sicurezza delle informazioni o qualsiasi politica specifica di un argomento viene distribuita all'esterno dell'organizzazione, si deve fare attenzione a non divulgare impropriamente informazioni riservate.

La tabella 1 illustra le differenze tra la politica di sicurezza delle informazioni e la politica specifica dell'argomento.

Tabella1-Differenze tra la politica di sicurezza dell'informazione e la politica specifica del tema

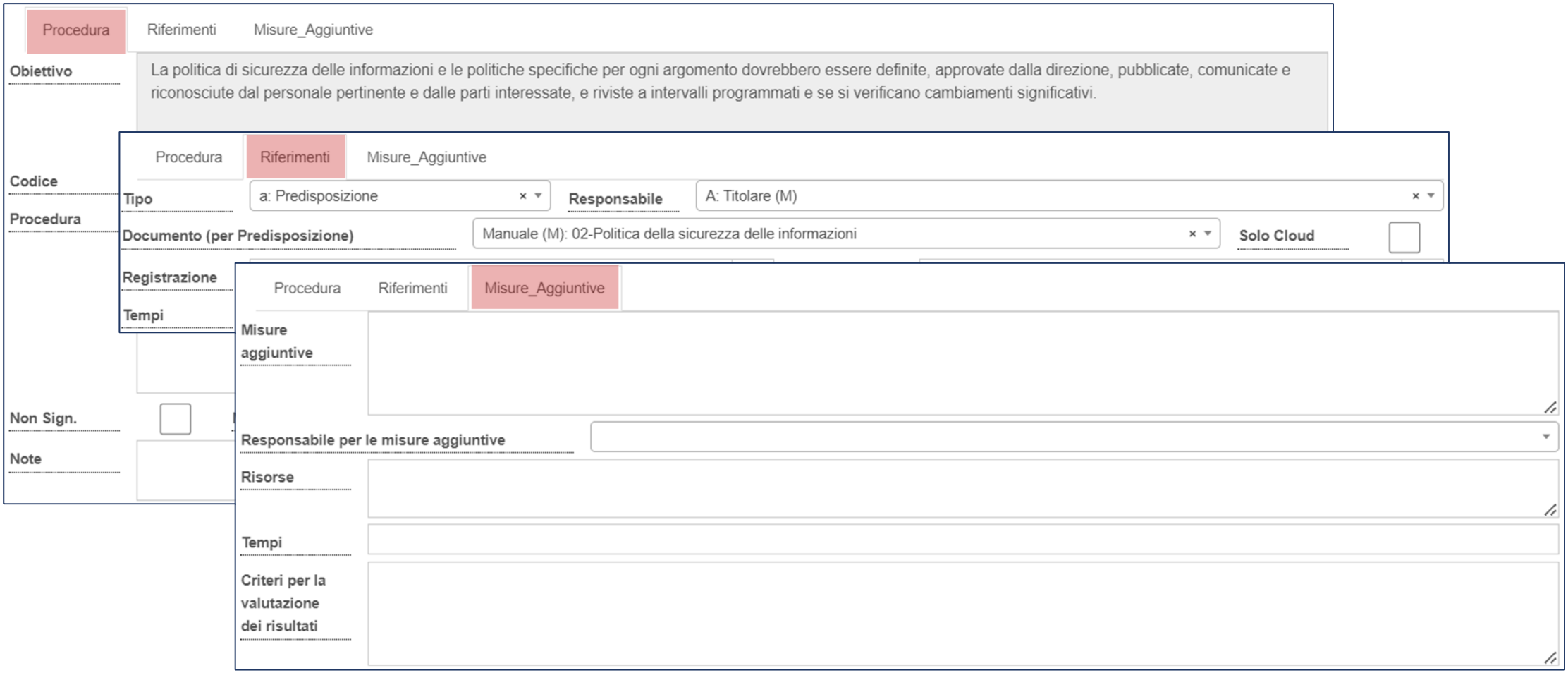
	Politica di sicurezza delle informazioni	Politica specifica dell'argomento
Livello di dettaglio	Generale o di alto livello	Specifico e dettagliato
Documentato e formalmente approvato da	Top management	Livello di gestione appropriato

Altre informazioni

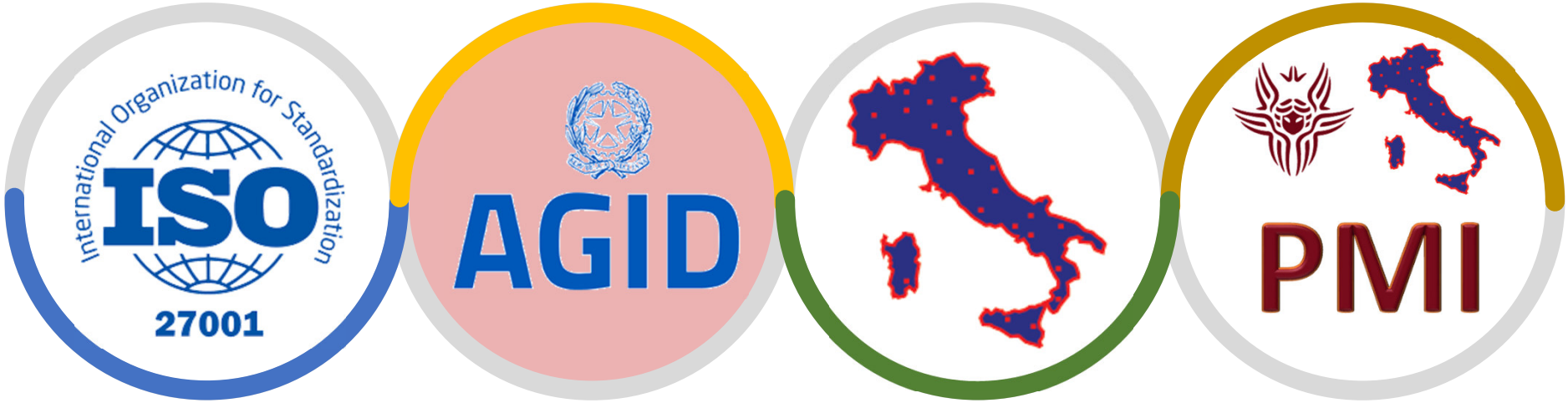
Le politiche specifiche dell'argomento possono variare da un'organizzazione all'altra.

Titolo	Responsabile	Cosa
a: Politica per la sicurezza (requisiti)	Titolare (M)	Definire ed approvare una "Politica per la sicurezza delle informazioni" che prenda in considerazione:>> strategia e requisiti aziendali;>> r…
b: Politica per la sicurezza (dichiarazioni)	Referente per la Sicurezza…	Definire una "Politica per la sicurezza delle informazioni" che contenga dichiarazioni riguardanti:>> definizione di sicurezza delle informazi…
c: Politiche specifiche	Referente per la Sicurezza…	Assicurare che le politiche specifiche includano:>> controllo degli accessi;>> sicurezza fisica e ambientale;>> gestione delle risorse;>> tra…
d: Revisione delle Politiche	Referente per la Sicurezza…	Verificare che le politiche siano revisionate in funzione di:>> la strategia di business dell'organizzazione;>> l'ambiente tecnico dell'organizz…

ISO 27001 – 27002 - 27701



Controlli


International Organization for Standardization
ISO
27001
AGID
PMI

Misure minime di sicurezza ICT

Agenzia per l'Italia Digitale

Aprile 2016

121 Misure

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

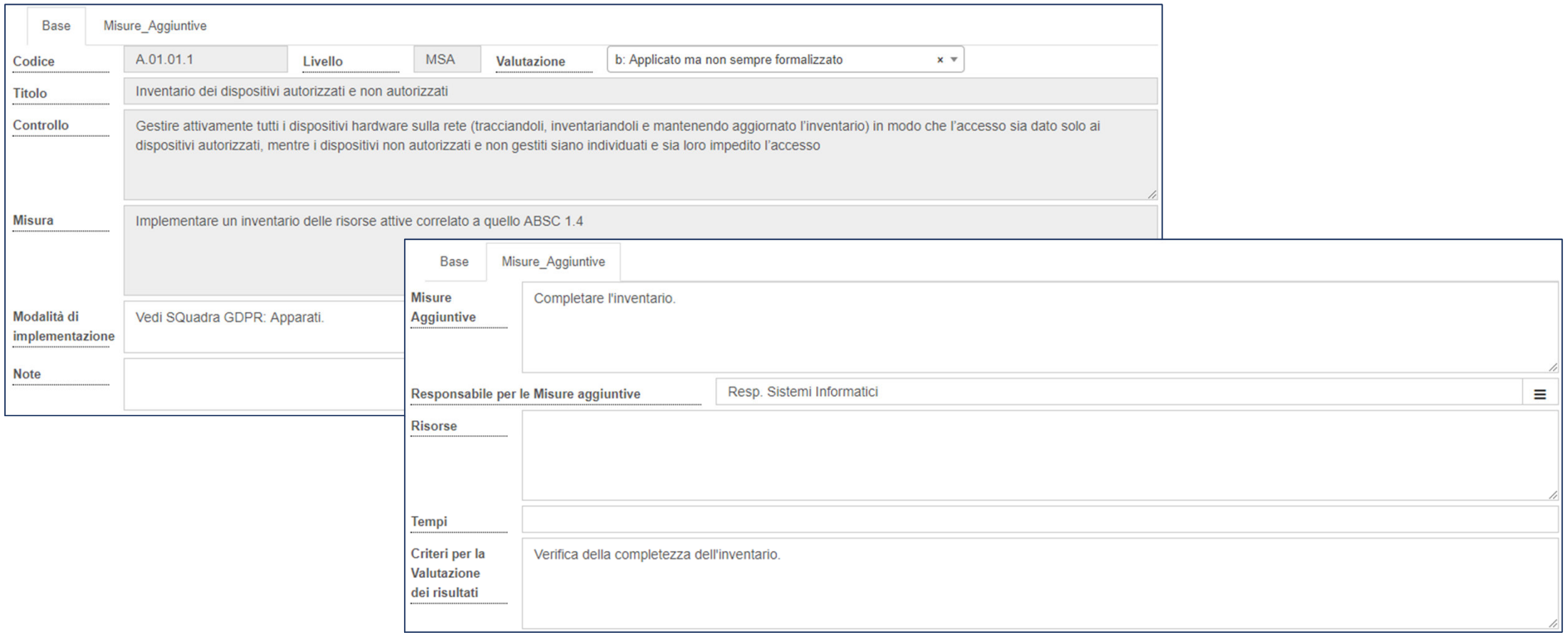
Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non

ABSC_ID #			Descrizion
1	1	1	Implementare un inventario delle risorse attive corr
		2	Implementare ABSC 1.1.1 attraverso uno strumento
		3	Effettuare il discovery dei dispositivi collegati alla r
		4	Qualificare i sistemi connessi alla rete attraverso l'a
	2	1	Implementare il "logging" delle operazione del serv
		2	Utilizzare le informazioni ricavate dal "logging" DH sorse e identificare le risorse non ancora censite.
	3	1	Aggiornare l'inventario quando nuovi dispositivi ap
		2	Aggiornare l'inventario con uno strumento automat vengono collegati in rete.
	4	1	Gestire l'inventario delle risorse di tutti i sistemi col stessi, registrando almeno l'indirizzo IP.
		2	Per tutti i dispositivi che possiedono un indirizzo IP macchine, la funzione del sistema, un titolare respo L'inventario delle risorse creato deve inoltre includ vo sia portatile e/o personale.
		3	Dispositivi come telefoni cellulari, tablet, laptop e a memorizzano o elaborano dati devono essere identi meno alla rete dell'organizzazione.

Azione	Codice	Titolo	Controllo	Livello	Misura	Modalità	Valutazione
	A.01.01.1	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	MSA	Implementare un inventario delle ris...	Vedi SQuadra GDPR: Apparati.	b.Applicato ma n...
	A.01.01.2	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	SA	Implementare ABSC 1.1.1 attraverso...		
	A.01.01.3	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	A	Effettuare il discovery dei dispositivi ...		
	A.01.01.4	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	A	Qualificare i sistemi connessi alla ret...		
	A.01.02.1	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	SA	Implementare il "logging" delle opera...		
	A.01.02.2	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	SA	Utilizzare le informazioni ricavate dal...		
	A.01.03.1	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	MSA	Aggiornare l'inventario quando nuovi...	Aggiornamento tramite scadenziario ...	a.Applicato e for...
	A.01.03.2	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	SA	Aggiornare l'inventario con uno stru...		
	A.01.04.1	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	MSA	Gestire l'inventario delle risorse di tu...		e.Non presente/...
	A.01.04.2	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	SA	Per tutti i dispositivi che possiedono ...		
	A.01.04.3	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	A	Dispositivi come telefoni cellulari, tab...		
	A.01.05.1	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	A	Installare un'autenticazione a livello ...		
	A.01.06.1	Inventario dei di...	Gestire attivamente tutti i dispositivi ...	A	Utilizzare i certificati lato client per v...		
	A.02.01.1	Inventario dei so...	Gestire attivamente (inventariare, tra...	MSA	Stilare un elenco di software autorizz...	SQuadra GDRP: Prodotti.	a.Applicato e for...
	A.02.02.1	Inventario dei so...	Gestire attivamente (inventariare, tra...	SA	Implementare una "whitelist" delle a...		
	A.02.02.2	Inventario dei so...	Gestire attivamente (inventariare, tra...	SA	Per sistemi con funzioni specifiche (...		
	A.02.02.3	Inventario dei so...	Gestire attivamente (inventariare, tra...	A	Utilizzare strumenti di verifica dell'int...		
	A.02.03.1	Inventario dei so...	Gestire attivamente (inventariare, tra...	MSA	Eseguire regolari scansioni sui siste...		d.Previsto ma no...
	A.02.03.2	Inventario dei so...	Gestire attivamente (inventariare, tra...	SA	Mantenere un inventario del softwar...		
	A.02.03.3	Inventario dei so...	Gestire attivamente (inventariare, tra...	A	Installare strumenti automatici d'inve...		

Pagina 1 di 7 20 Righe 1 - 20 di 121

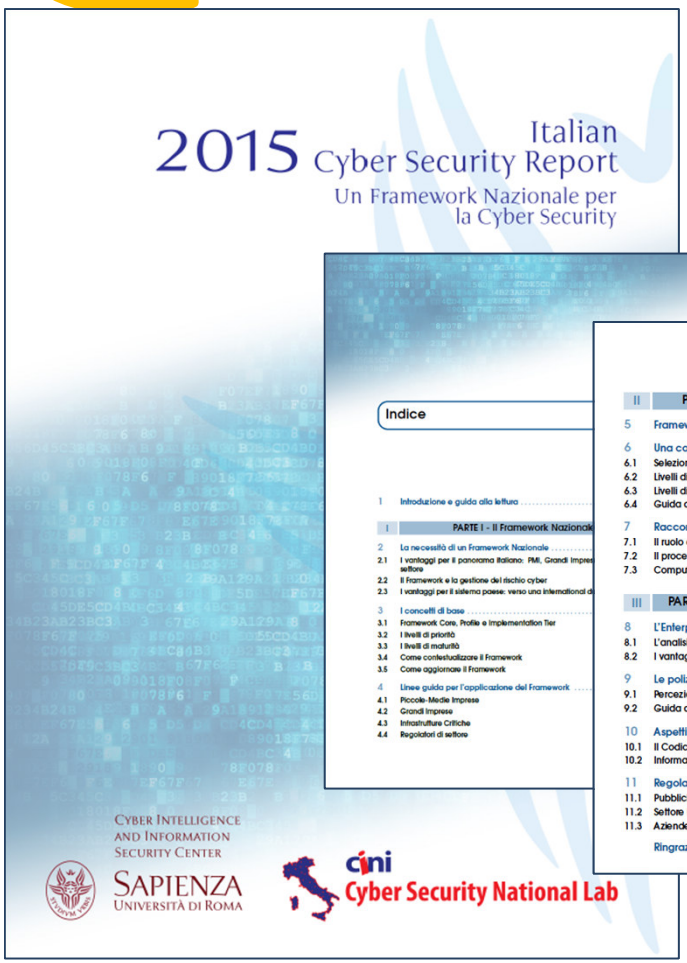
Misure minime di sicurezza ICT



Controlli


International Organization for Standardization
ISO
27001
AGID
PMI

Italian Cyber Security Report



98 Sottocategorie

Function	Category	Subcategory	Informative References
	Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con	ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8
		partner esterni	· NIST SP 800-53 Rev. 4 PM-1, PS-7

Codice	Funzione	Titolo	Categoria	Sottocategoria	Misure	Valutazione
ID.AM-01	Identificare	Gestione del patrimonio	I dati, il personale, i dispositi...	Sono censiti i sistemi e gli apparati fisici in u...	Vedi SQuadra G...	a.Applicato e for...
ID.AM-02	Identificare	Gestione del patrimonio	I dati, il personale, i dispositi...	Sono censite le piattaforme e le applicazioni...		b.Applicato ma n...
ID.AM-03	Identificare	Gestione del patrimonio	I dati, il personale, i dispositi...	I flussi di dati e comunicazioni inerenti l'orga...		c.Parzialmente a...
ID.AM-04	Identificare	Gestione del patrimonio	I dati, il personale, i dispositi...	I sistemi informativi esterni all'organizzazion...		a.Applicato e for...
ID.AM-05	Identificare	Gestione del patrimonio	I dati, il personale, i dispositi...	Le risorse (es: hardware, dispositivi, dati e s...		d.Previsto ma n...
ID.AM-06	Identificare	Gestione del patrimonio	I dati, il personale, i dispositi...	Sono definiti e resi noti ruoli e responsabilità...		a.Applicato e for...
ID.BE-01	Identificare	Contesto aziendale	La mission dell'organizzazio...	Il ruolo dell'organizzazione all'interno della ...		a.Applicato e for...
ID.BE-02	Identificare	Contesto aziendale	La mission dell'organizzazio...	Il ruolo dell'organizzazione come infrastruttu...		c.Parzialmente a...
ID.BE-03	Identificare	Contesto aziendale	La mission dell'organizzazio...	Sono definite e rese note delle priorità per q...		
ID.BE-04	Identificare	Contesto aziendale	La mission dell'organizzazio...	Sono identificate e rese note interdipendenz...		
ID.BE-05	Identificare	Contesto aziendale	La mission dell'organizzazio...	Sono identificati e resi noti i requisiti di resili...		
ID.GV-01	Identificare	Governance	Le politiche, le procedure e i...	E' indetificata e resa nota una policy di sicur...		
ID.GV-02	Identificare	Governance	Le politiche, le procedure e i...	Ruoli e responsabilità inerenti la sicurezza d...		
ID.GV-03	Identificare	Governance	Le politiche, le procedure e i...	I requisiti legali in materia di cybersecurity, c...		
ID.GV-04	Identificare	Governance	Le politiche, le procedure e i...	La governante ed i processi di risk manage...		
ID.RA-01	Identificare	Valutazione dei rischi	L'impresa comprende il risc...	Le vulnerabilità delle risorse (es. sistemi, loc...		
ID.RA-02	Identificare	Valutazione dei rischi	L'impresa comprende il risc...	L'organizzazione riceve informazioni su min...		
ID.RA-03	Identificare	Valutazione dei rischi	L'impresa comprende il risc...	Le minacce, sia interne che esterne, sono id...		
ID.RA-04	Identificare	Valutazione dei rischi	L'impresa comprende il risc...	Sono identificati i potenziali impatti sul busin...		

Italian Cyber Security Report

98 → 117 Sottocategorie

FUNCTION	CATEGORY	SUBCATEGORY
IDENTIFY (ID)	**Asset Management (ID.AM)**: I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**DP-ID.AM-7:** Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)
		DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente all'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**DP-ID.RA-7:** Viene effettuata una valutazione di impatto sulla protezione dei dati personali
	Data Management (DP-ID.DM): i dati personali sono trattati attraverso processi definiti, in coerenza con le normative di riferimento.	**DP-ID.DM-1:** Il ciclo di vita dei dati è definito e documentato
		DP-ID.DM-2: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati
		DP-ID.DM-3: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati
		DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato
		DP-ID.DM-5: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale
RESPOND (RS)	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**DP-RS.CO-6:** Gli incidenti che si configurano come violazioni di dati personali sono documentati ed eventualmente vengono informati le autorità di riferimento e gli interessati

Priorità per il GDPR

	Categoria	Sottocategoria	Misu	Valutazione	Res.I	Priorità	P_PMI	P_GDP	Ann	Liv
pat...	dati, il personal...	Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione		a.Applicato e for...		A.Alta	A.Alta	N.Non...	2015	
pat...	I dati, il personal...	Sono censite le piattaforme e le applicazioni software in uso nell'or...		b.Applicato ma n...		A.Alta	A.Alta	N.Non...	2015	
pat...	I dati, il personal...	I flussi di dati e comunicazioni inerenti l'organizzazione sono identifi...		c.Parzialmente a...		B.Bassa	B.Bassa	N.Non...	2015	
pat...	I dati, il personal...	I sistemi informativi esterni all'organizzazione sono catalogati		d.Previsto ma n...		N.Non sel...	N.Non...	N.Non...	2015	
pat...	I dati, il personal...	Le risorse (es: hardware, dispositivi, dati e software) sono prioritizz...		e.Non presente/...		M.Media	M.Media	N.Non...	2015	
pat...	I dati, il personal...	Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecuri...		0.Non applicabile		A.Alta	A.Alta	N.Non...	2015	
pat...	I dati, il personal...	Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento ...				A.Alta		A.Alta	2019	
pat...	I dati, il personal...	I trattamenti di dati personali sono identificati e catalogati				A.Alta		A.Alta	2019	
end...	La mission dell'o...	Il ruolo dell'organizzazione all'interno della filiera produttiva è identif...		a.Applicato e for...		N.Non sel...	N.Non...	N.Non...	2015	
end...	La mission dell'o...	Il ruolo dell'organizzazione come infrastruttura critica e nel settore i...		b.Applicato ma n...		N.Non sel...	N.Non...	N.Non...	2015	
end...	La mission dell'o...	Sono definite e rese note delle priorità per quanto riguarda la missi...		b.Applicato ma n...		M.Media	M.Media	N.Non...	2015	
end...	La mission dell'o...	Sono identificate e rese note interdipendenze e funzioni fondament...		b.Applicato ma n...		M.Media	M.Media	N.Non...	2015	
end...	La mission dell'o...	Sono identificati e resi noti i requisiti di resilienza a supporto della f...		c.Parzialmente a...		M.Media	M.Media	N.Non...	2015	
	Le politiche, le p...	E' indetificata e resa nota una policy di sicurezza delle informazioni		a.Applicato e for...		M.Media	M.Media	N.Non...	2015	
	Le politiche, le p...	Ruoli e responsabilità inerenti la sicurezza delle informazioni sono ...		c.Parzialmente a...		M.Media	M.Media	N.Non...	2015	
	Le politiche, le p...	I requisiti legali in materia di cybersecurity, con l'inclusione degli ob...		a.Applicato e for...		A.Alta	A.Alta	A.Alta	2015	
	Le politiche, le p...	La governante ed i processi di risk management includono la gesti...		b.Applicato ma n...		B.Bassa	B.Bassa	N.Non...	2015	
dei r...	L'impresa compr...	Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'orga...		b.Applicato ma n...		M.Media	M.Media	N.Non...	2015	
dei r...	L'impresa compr...	L'organizzazione riceve informazioni su minacce e vulnerabilità da f...		a.Applicato e for...		B.Bassa	B.Bassa	N.Non...	2015	

Pagina 1 di 6 20 Righe 1 - 20 di 117

Cybersecurity

FUNCTION	CATEGORY	SUBCATEGORY
IDENTIFY (ID)	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**DP-ID.AM-7:** Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)
		DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente all'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**DP-ID.RA-7:** Viene effettuata una valutazione di impatto sulla protezione dei dati personali
	Data Management (DP-ID.DM): i dati personali sono trattati attraverso processi definiti, in coerenza con le normative di riferimento.	**DP-ID.DM-1:** Il ciclo di vita dei dati è definito e documentato
		DP-ID.DM-2: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati
		DP-ID.DM-3: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati
		DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato
		DP-ID.DM-5: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale
RESPOND (RS)	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**DP-RS.CO-6:** Gli incidenti che si configurano come violazioni di dati personali sono documentati ed eventualmente vengono informati le autorità di riferimento e gli interessati

Nuove category e subcategory introdotte nel Framework Nazionale per la Cybersecurity e la Data Protection.

Allegato B del **DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 14 aprile 2021, n. 81**

Per ogni misura è fornita una specifica più dettagliata dell'implementazione minima attesa, nonché delle modalità richieste al fine di descriverne l'adozione e dimostrarne l'attuazione.

2. IDENTIFICAZIONE (IDENTIFY)

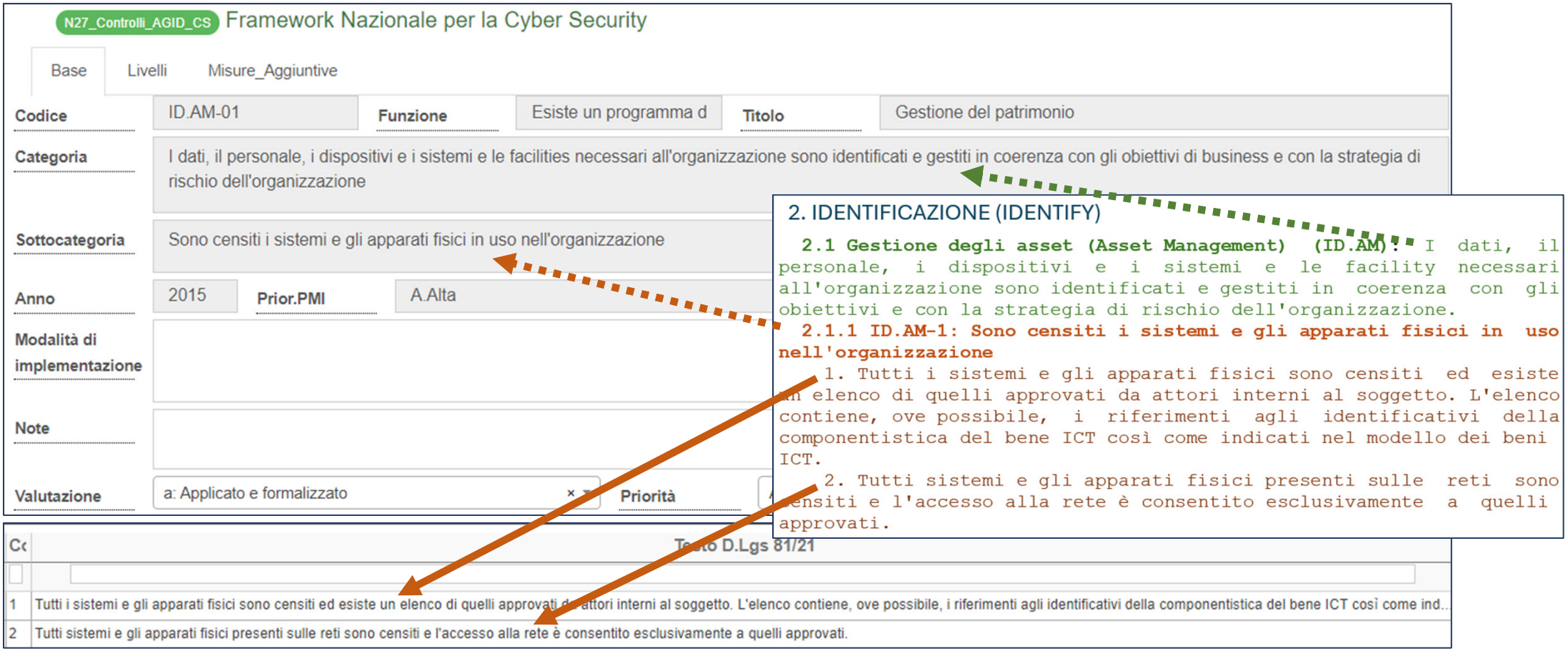
2.1 Gestione degli asset (Asset Management) (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facility necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.

2.1.1 ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione

1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto. L'elenco contiene, ove possibile, i riferimenti agli identificativi della componentistica del bene ICT cosi' come indicati nel modello dei beni ICT.

2. Tutti sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete e' consentito esclusivamente a quelli approvati.

Cyber Security & D.Lgs. 81/2021



Controlli


International Organization for Standardization
ISO
27001
AGID
PMI

Misure essenziali (2016)

Codice	Area	Misure	Valutazione
CE16-01	1.Inventario dispositivi e software	es. MSI: Descrizione del sistema informatico. SQuadra: Apparati e Prodotti.	a.Applicato e for...
CE16-02	1.Inventario dispositivi e software	es. MSI: Responsabilità RSI. Gestione delle utenze ai vari servizi sul web.	b.Applicato ma n...
CE16-03	1.Inventario dispositivi e software	es. SQuadra: Trattamenti.	a.Applicato e for...
CE16-04	1.Inventario dispositivi e software	es. MSI: Responsabilità RSI.	c.Parzialmente a...
CE16-05	2.Governance	es. MSI: Responsabilità RSI. Conformità ai requisiti cogenti e contrattuali.	d.Previsto ma n...
CE16-06	3.Protezione da malware	es. MSI: Responsabilità RSI. Protezione da malware.	a.Applicato e for...
CE16-07	4.Gestione password e account	es. Policy: Password.	d.Previsto ma n...
CE16-08	4.Gestione password e account	es. MSI: Responsabilità RSI. Autorizzazioni per utente.	a.Applicato e for...
CE16-09	4.Gestione password e account	es. MSI: Responsabilità RSI. Autorizzazioni per utente.	b.Applicato ma n...
CE16-10	5.Formazione e consapevolezza	es. MSI: Formazione.	c.Parzialmente a...
CE16-11	6.Protezione dei dati	es. MSI: Responsabilità RSI. Configurazioni.	b.Applicato ma n...
CE16-12	6.Protezione dei dati	es. MSI: Politica per la sicurezza. Criteri per il backup ed il ripristino.	
CE16-13	7.Protezione delle reti	es. MSI: Responsabilità RSI. Protezione delle Reti.	
CE16-14	8.Prevenzione e mitigazione	es. Policy: Segnalazione dei problemi.	
CE16-15	8.Prevenzione e mitigazione	es. MSI: Responsabilità RSI. Aggiornamento software.	

15 Misure

Misure essenziali (2016)

1.Inventario dispositivi e software

La quantità di dispositivi che al giorno d'oggi possono essere veicolo di attacchi informatici è enorme: non solo PC, smartphone e tablet, ma anche videocamere di sorveglianza, smart-TV, ecc. Praticamente tutti i dispositivi personali e aziendali sono connessi a internet o ad altre reti e un attaccante potrebbe sfruttare uno qualsiasi di questi dispositivi per condurre un attacco. Solo i dispositivi autorizzati dovrebbero poter accedere alla rete (si veda anche il controllo 13), ed è necessario far sì che i dispositivi non autorizzati e non gestiti possano essere prontamente individuati in modo che sia loro impedito l'accesso. È quindi fondamentale, al fine di instaurare una buona politica di gestione della sicurezza informatica, creare un inventario di tutti quei dispositivi che in qualche modo fanno parte dell'azienda o della propria vita digitale. Non bisogna limitarsi ai dispositivi fisici, cioè all'hardware, ma occorre inventariare anche i programmi, cioè i software, e tutte le applicazioni e i sistemi in uso (anche se forniti da terze parti come servizi). Gli inventari devono essere aggiornati quando nuovi dispositivi o nuovi software sono installati e/o collegati alla rete e il loro contenuto deve essere verificato periodicamente.

Nell'identificazione delle risorse dovrebbe rientrare anche un processo di gestione delle utenze (account) ai vari servizi sul web come posta elettronica, cloud computing e social network. È buona norma eliminare/disattivare gli account non più utilizzati poiché potrebbero contenere informazioni importanti (e le relative credenziali raramente verranno aggiornate). La registrazione a servizi esterni offerti da terze parti dovrebbe essere fatta esclusivamente utilizzando le e-mail aziendali e mai credenziali personali. Nel momento in cui si accede a servizi web come i social network, sistemi cloud o di immagazzinamento e condivisione dei file, è necessario considerare i rischi collegati al trasferimento, invio e condivisione di dati dell'azienda e del personale verso terze parti. Una attenta lettura dei documenti riportanti le condizioni di utilizzo del servizio può fornire informazioni fondamentali per capire come e in quale modo i dati aziendali verranno gestiti dal provider del servizio una volta che questi saranno usciti dal perimetro aziendale.

Qualsiasi azienda, a prescindere dal settore, individua quali siano i dati e le informazioni più rilevanti e critici sulla base del proprio business, tenendo presente che la mancata protezione di tali asset potrebbe comportare sanzioni, perdite economiche, interruzione del business o perdita di vantaggio competitivo. I dati e le informazioni devono essere classificati secondo un criterio che tenga in considerazione la loro criticità (es. dati pubblici, dati solo per uso commerciale, dati riservati, dati segreti). In fase di inventario si dovrebbe identificare e registrare la mappatura delle dipendenze tra il dato, informazione, software, dispositivo, sistema (anche esterno) e infrastruttura con il relativo servizio/processo di business. In questo modo è possibile determinare il grado di criticità di un singolo sottosistema e il suo potenziale impatto in caso di incidente di sicurezza sulla totalità del sistema e sugli obiettivi di business dell'azienda.

È infine necessario che l'azienda nomini un responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici. All'interno di aziende medio-grandi questo ruolo è spesso affidato ai Chief Information Security Officer (CISO) e Security Manager.

Nei casi in cui non sia possibile, per motivi dimensionali o di risorse, identificare una persona dedicata esclusivamente a tale ruolo è comunque opportuno e necessario che sia nominato un responsabile che nel suo ruolo si occupi di garantire la corretta messa in opera di tutte le procedure necessarie per la protezione dell'azienda dai rischi legati alla cybersecurity.

2.Governance

3.Protezione da malware

4.Gestione password e account

5.Formazione e consapevolezza

6.Protezione dei dati

7.Protezione delle reti

8.Prevenzione e mitigazione

La prevenzione degli incidenti di sicurezza parte dall'applicazione di buone pratiche per la messa in sicurezza dei sistemi informativi e dei computer, siano essi personali o aziendali. Su tutti i dispositivi è presente software, sotto forma di applicazioni e sistemi operativi, che deve essere aggiornato costantemente nel tempo per sanare vulnerabilità note. Le vulnerabilità sono rappresentate da difetti ed errori, involontariamente inseriti nel software dal produttore durante la sua realizzazione. Questi rappresentano dei punti deboli sfruttabili da criminali per compromettere il funzionamento dei sistemi o accedere illecitamente a informazioni e dati aziendali. All'identificazione di una vulnerabilità in un software segue normalmente il rilascio di un aggiornamento da parte del produttore. L'applica¬zione dell'aggiornamento risolve la vulnerabilità e impedisce che la stessa possa essere sfruttata da cyber-criminali per future intrusioni.

Per tutti i motivi sopra citati è opportuno pertanto che:

L'azienda disponga delle licenze per il software impiegato in modo da poter accedere agli aggiornamenti offerti dal produttore in maniera tempestiva;

Laddove possibile e ragionevole sia configurato l'aggiornamento automatico del software. Questo, in particolare, per i personal computer utilizzati dai dipendenti, che rappresentano spesso uno tra i bersagli più semplici da compromettere;

Su tutti i sistemi sui quali non sia possibile un aggiornamento automatico, è opportuno che venga predisposto un processo di acquisizione delle patch, identificazione di quelle critiche e la loro successiva applicazione. La tempestività di questo processo è un fattore determinante, dato che nuove vulnerabilità possono essere sfruttate dagli attaccanti nel giro di poche ore dal momento del loro annuncio pubblico;

Sia pianificata la dismissione del software non più supportato dal produttore e la sua sostituzione con prodotti per i quali gli aggiornamenti vengano garantiti.

Laddove l'aggiornamento non fosse possibile (per motivi di continuità del servizio, economici, o altro) è necessario accettare il rischio residuo, possibilmente documentandolo, ed eventualmente porre in essere opportune azioni di mitigazione (es. isolamento o distacco dalla rete del software non sicuro).

Non si può escludere che i sistemi possano essere compromessi o violati anche nel caso di applica¬zione degli aggiornamenti. Questo potrebbe, ad esempio, accadere nel caso in cui una vulnerabilità fosse nota a cyber-criminali prima del rilascio del relativo aggiornamento da parte del produttore del software. In questo caso, la vulnerabilità prende il nome di 0-day, e risulta particolarmente pericolosa, proprio per l'assenza di una chiara strategia di protezione. In questi casi (relativamente rari) si possono adottare temporaneamente delle misure di mitigazione e contenimento, in attesa del rilascio di un aggiornamento che risolva la vulnerabilità.

Qualora le misure preventive non siano state sufficienti e si verifichi un incidente, il personale deve essere in grado di rispondere tempestivamente e adeguatamente in modo da limitarne i danni. A tal fine è opportuno che:

Tutto il personale sia informato su chi debba essere contattato nel caso si identifichino indicatori di un potenziale incidente informatico, come ad esempio il funzionamento anomalo di un computer, l'impossibilità di accedere al sistema o ai dati in esso contenuti, ecc. Una opportuna campagna di formazione dovrebbe aver messo il personale in grado di riconoscere tali indicatori.

Tutto il personale sia educato a non porre in essere azioni estemporanee sui sistemi una volta che abbiano identificato un incidente, in modo da non compromettere le successive attività di risposta. Le azioni devono essere effettuate solo sotto indicazione di personale qualificato o di opportuno supporto tecnico esterno qualora non si disponga internamente di tale personale;

Il responsabile della sicurezza, laddove opportuno, contatti le forze dell'ordine preposte alla lotta contro la cyber-criminalità;

Sia identificato il personale tecnico interno o gli eventuali fornitori incaricati di intervenire per analizzare, rispondere ed eventualmente ripristinare i sistemi.

Misure essenziali (2016)

Base | Misure_Aggiuntive

Codice	CE16-01	Area	1.Inventario dispositivi e software
Titolo	Inventario		
Descrizione	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.		
Misure	MSI: Descrizione del sistema informatico. SQuadra: Apparati e Prodotti.		
Valutazione	a: Applicato e formalizzato	Priorità	B: Bassa
Conformità	5	Conformità Attesa	8
Note			

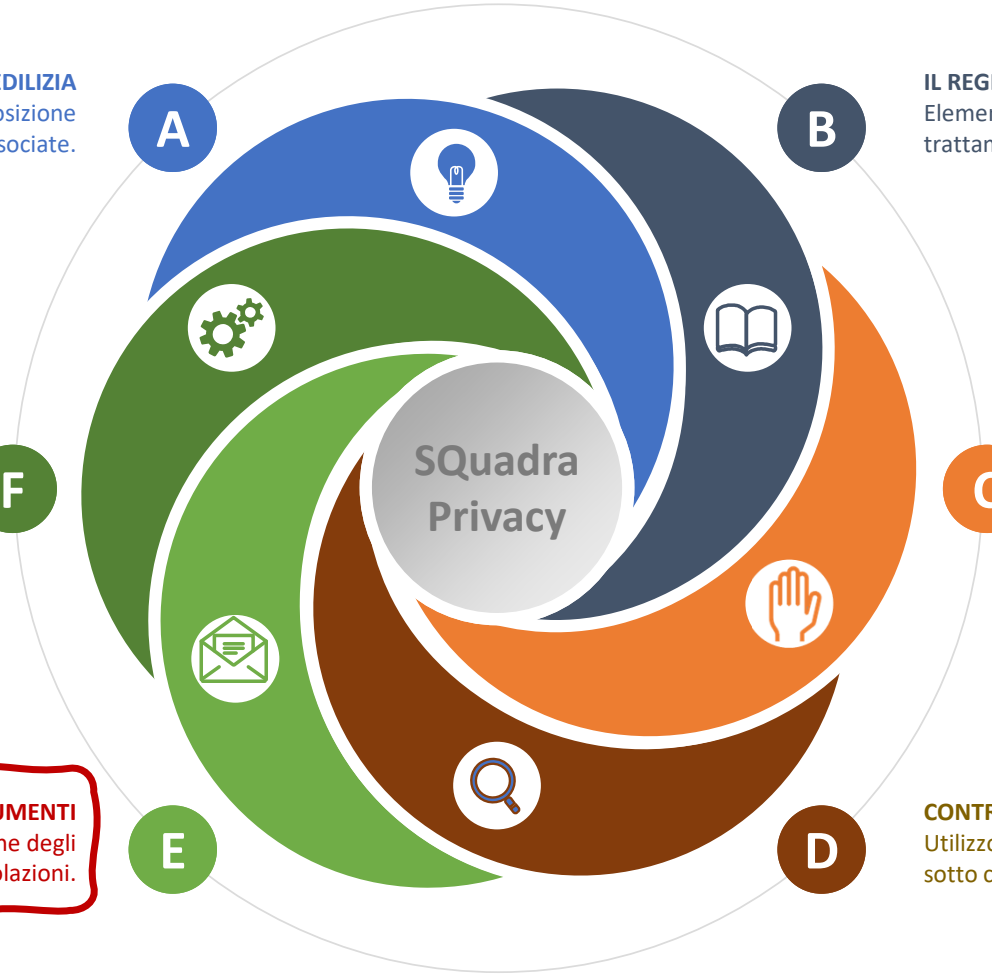
Base | Misure_Aggiuntive

Misure Aggiuntive	SQuadra GDPR Prodotti
Responsabile per le Misure aggiuntive	Resp. Sistemi Informatici
Risorse	
Tempi	
Criteri per la Valutazione dei risultati	

SQuadra-Privacy

A **IL PROGETTO SQUADRA-EDILIZIA**
Dal 2008 uno strumento a disposizione delle imprese associate.

B **IL REGISTRO DEI TRATTAMENTI**
Elemento essenziale per l'analisi dei trattamenti effettuati.



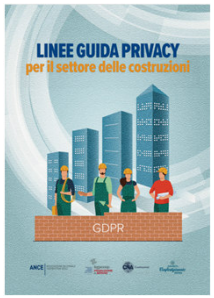
C **CONFORMITÀ E MINACCE**
Autovalutazione della situazione di partenza e degli obiettivi.

D **CONTROLLI**
Utilizzo delle migliori pratiche per tenere sotto controllo i sistemi informatici.

E **ALTRI STRUMENTI**
Documenti aggiuntivi e gestione degli incidenti e delle violazioni.

F **SICUREZZA DELLE INFORMAZIONI**
Problematiche tipiche e specifiche relative all'utilizzo delle nuove tecnologie.

Altri Documenti



tiglio | Manuale del Sistema di gestione della Sicurezza delle informazioni

Sommario

1 Premessa ... 2
1.1 Responsabilità ... 2
1.2 Dati Aziendali ... 4
1.3 Controlli sulle attività degli utenti ... 6
2 Politica della sicurezza delle informazioni ... 7
2.1 Risposta alle emergenze ... 8
2.2 Criteri per la continuità ... 8
2.3 Criteri per il backup e il ripristino ... 9
2.4 Protezione da malware ... 9
2.5 Aggiornamento del software a fronte di vulnerabilità ... 10
2.6 Configurazione dei dispositivi ... 10
2.7 Dispositivi mobili ... 10
2.8 Criteri per la salvaguardia delle informazioni nelle reti ... 11
2.9 Criteri per la riduzione delle funzionalità ... 11
2.10 Gestione utenti ... 11
2.11 Programmi applicativi ... 14
2.12 Criteri per l'uso della crittografia ... 14
2.13 Manutenzione delle apparecchiature ... 14
2.14 Criteri per la dismissione o il riutilizzo delle apparecchiature ... 14
2.15 Politica sul Controllo Accessi ... 15
2.16 Criteri per la comunicazione delle Informazioni ... 16
2.17 Aggiornamenti alle Politiche per la Sicurezza delle Informazioni ... 16
3 Descrizione del sistema informatico ... 16
3.1 Apparati e Prodotti ... 16
3.2 Caratteristiche del Sistema Informatico ... 16
4 Compiti del Referente per la sicurezza delle informazioni (RSI) ... 18
4.1 Ruoli per la sicurezza delle informazioni ... 18
4.2 Amministratori del sistema ... 18
4.3 Procedure documentate ... 19
4.4 Apparati all'esterno delle sedi aziendali ... 19
4.5 Aggiornamento sugli sviluppi della tecnologia e legali ... 19
4.6 Riesame della sicurezza delle informazioni ... 19
4.7 Gestione delle utenze ai vari servizi sul web ... 19
4.8 Aggiornamento dei Sistemi Informatici ... 20
4.9 Controllo delle attività di terze parti ... 20
4.10 Controlli sulle operazioni pianificate ... 21
4.11 Protezione della documentazione di sistema ... 21
4.12 Conformità ai requisiti cogenti e contrattuali ... 21
5 Documenti Cartacei ... 21
5.1 Gestione corrispondenza in ingresso ... 21
5.2 Archivi cartacei ... 21
6 Formazione ... 21

tiglio | Procedure per i Consulenti IT

Sommario

1 Premessa ... 2
2 Politica della sicurezza ... 2
2.1 Risposta alle emergenze ... 2
2.2 Criteri per la continuità ... 2
2.3 Criteri per il backup e il ripristino ... 3
2.4 Protezione da malware ... 4
2.5 Aggiornamento del software a fronte di vulnerabilità ... 4
2.6 Configurazione dei dispositivi ... 4
2.7 Dispositivi mobili ... 4
2.8 Criteri per la salvaguardia delle informazioni nelle reti ... 5
2.9 Criteri per la riduzione delle funzionalità ... 5
2.10 Creazione nuovi utenti ... 5
2.11 Autorizzazioni per utente ... 5
2.12 Disattivazione utenti ... 6
2.13 Programmi applicativi ... 6
2.14 Criteri per l'uso della crittografia ... 8
2.15 Manutenzione delle apparecchiature ... 8
2.16 Criteri per la dismissione o il riutilizzo delle apparecchiature ... 8
3 Descrizione del sistema informatico ... 8
3.1 Inventari ... 8
3.2 Caratteristiche del Sistema Informatico ... 8
4 Supporto al Referente per la Sicurezza delle Informazioni ... 9
4.1 Amministratori del sistema ... 9
4.2 Procedure documentate ... 10
4.3 Aggiornamento sugli sviluppi della tecnologia e legali ... 10
4.4 Riesame della sicurezza delle informazioni ... 10
4.5 Aggiornamento dei Sistemi Informatici ... 10
4.6 Controllo delle attività di terze parti ... 11
4.7 Conformità ai requisiti cogenti e contrattuali ... 11

tiglio | Responsabile della Sicurezza delle Informazioni

Sommario

1 Compiti del Responsabile della Sicurezza delle Informazioni ... 1
1.1 Assegnazione delle Responsabilità ... 1
1.2 Attività di formazione ... 2
1.3 Sicurezza delle informazioni ... 2
1.4 Rapporti con terze parti ... 2
1.5 Sistema disciplinare ... 3
1.6 Altre attività ... 3
1.7 Riesame del sistema ... 4

1 Compiti del Responsabile della Sicurezza delle Informazioni

1.1 Assegnazione delle Responsabilità

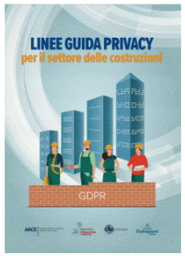
Al fine di garantire la sicurezza delle informazioni il RSI ha assegnato le responsabilità al personale per assicurare che tutti i requisiti cogenti e contrattuali e gli interessi aziendali siano garantiti.
Le responsabilità sono registrate su SQuadra-Privacy dove è anche presente la data dell'ultima verifica effettuata.
Il RSI ha, inoltre, predisposto i punti di contatto interni, in caso di Sua assenza, nel caso di incidenti alla Sicurezza delle informazioni e ha istaurato contatti con consulenti esterni per la risposta agli incidenti con la necessaria competenza per mitigare e rispondere ad eventi avversi e per gestire un incidente e mantenere la sicurezza delle informazioni.

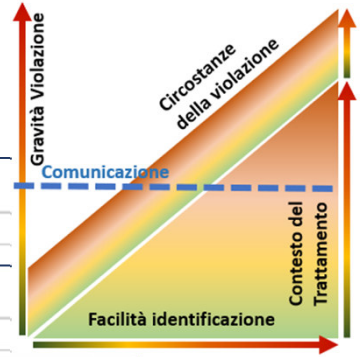
In funzione dell'importanza del ruolo per la sicurezza delle informazioni RSI effettua delle verifiche sui collaboratori che dovranno accedere ad informazioni riservate (referenze, verifica curriculum vitae, riscontro dei titoli di studio e professionali dichiarati, ecc.).
RSI concorda con i vari Referenti Privacy i livelli di autorizzazione per i nuovi utenti o per utenti che cambiano mansione garantendo, per quanto possibile la segregazione delle principali operazioni evitando che chi attiva sia colui che autorizza.
È cura del RSI, eventualmente con la collaborazione dei consulenti IT, definire le modalità per la fornitura, in modo sicuro delle password temporanee, per il primo accesso.

RSI provvede, direttamente o tramite i consulenti informatici, alla rimozione dei diritti di accesso agli utenti che hanno lasciato l'organizzazione ed alla loro eliminazione da eventuali liste di accesso di gruppo. Queste attività possono essere anticipate, per evitare azioni indesiderate, su richiesta del Referente Privacy dell'ufficio di appartenenza dell'utente.

RSI verifica che nella nomina ad incaricati del trattamento dei dati siano gestiti gli aspetti di sicurezza delle informazioni in caso di cessazione del rapporto di lavoro, gestendo eventuali responsabilità ancora valide dopo la cessazione del rapporto. Sara cura del RSI valutare la necessità

Archiviazione Incidenti e Violazioni





Rilevazione | Valutazione | Misure | Non_Comunicazione | ENISA

Codice 18-02 Descrizione Accesso ai locali

Rilevazione | **Valutazione** | Misure | Non_Comunicazione | ENISA

N°_Interessati 50 N°Registrazioni 200 Categoria Registrazioni Importo paghe

Classificazione: Perdita (i dati non sono più presenti sui sistemi del titolare ma vi p

Valutazione: Pochi dati e non "sensibili".

Rischio: Nessun rischio significativo.

Livello di Rischio: b: Molto Basso

Rilevazione | Valutazione | **Misure** | Non_Comunicazione | ENISA

Misure

Rilevazione | Valutazione | Misure | **Non_Comunicazione** | ENISA

Misure di Protezione dei Dati

Rilevazione | Valutazione | Misure | Non_Comunicazione | **ENISA**

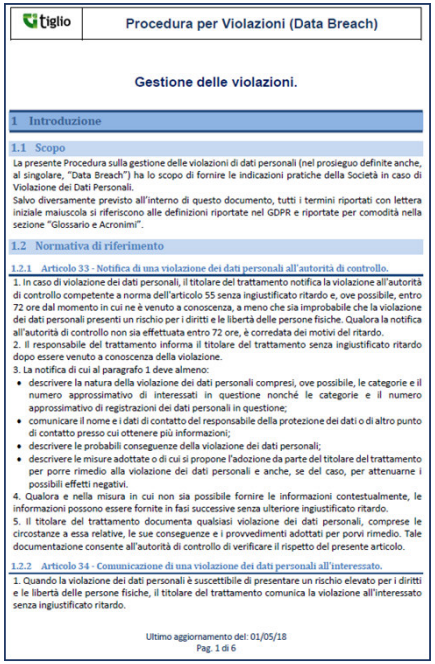
Contesto e incrementi/diminuzioni (0-4) 3,00 Facilità Identificazione (0,25-1) 1,00 Circostanze ed intenzionalità (0-0,5) 0,00

Recommendations for a methodology of the assessment of severity of personal data breaches

Working Document, v1.0, December 2013

enisa

European Union Agency for Network and Information Security www.enisa.europa.eu



tiglio | Procedura per Violazioni (Data Breach)

Gestione delle violazioni.

1 Introduzione

1.1 Scopo

La presente Procedura sulla gestione delle violazioni di dati personali (nel prosieguo definite anche, al singolare, "Data Breach") ha lo scopo di fornire le indicazioni pratiche della Società in caso di Violazione dei Dati Personali.
Salvo diversamente previsto all'interno di questo documento, tutti i termini riportati con lettera iniziale maiuscola si riferiscono alle definizioni riportate nel GDPR e riportate per comodità nella sezione "Glossario e Acronimi".

1.2 Normativa di riferimento

1.2.1 Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo.

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

1.2.2 Articolo 34 - Comunicazione di una violazione dei dati personali all'interessato.

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Ultimo aggiornamento del: 01/05/18
Pag. 1 di 6

Dati particolari (ex sensibili)

Qualsiasi tipo di dati sensibili (es. salute, affiliazione politica, vita sessuale).

4	Punteggio di base preliminare: quando la violazione coinvolge "dati sensibili" e il Titolare non è a conoscenza di fattori di diminuzione.
1	Il punteggio potrebbe essere diminuito a 1, ad esempio quando la natura del set di dati non fornisce alcuna visione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti pubblicamente disponibili (ad esempio la combinazione di informazioni da ricerche sul web).
2	Il punteggio potrebbe essere diminuito di 2, per esempio quando la natura dei dati può portare a supposizioni generali.
3	Il punteggio potrebbe essere diminuito di 1, ad esempio quando la natura dei dati può portare a supposizioni su informazioni sensibili.

Punteggio	Livello	Descrizione
G < 2	Basso	Gli individui non saranno interessati o potranno incontrare qualche inconveniente, che supereranno senza problemi (tempo speso a reinserire informazioni, fastidi, irritazioni, ecc.).
2 ≤ G < 3	Medio	Gli individui possono incontrare disagi significativi, che saranno in grado di superare nonostante alcune difficoltà (costi extra, negazione dell'accesso ai servizi commerciali, paura, mancanza di comprensione, stress, piccoli disturbi fisici, ecc.)
3 ≤ G < 4	Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento nella lista nera delle banche, danni materiali, perdita del lavoro, citazione in giudizio, peggioramento della salute, ecc.)
4 ≤	Molto alto	Gli individui possono andare incontro a conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come debiti sostanziali o incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.)

Supporto in caso di Violazioni

Comunicazione all'interessato della violazione dei dati.

(Ai sensi dell'art. 34 del Regolamento UE n. 679/2016)

Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) 679/2016, AZIENDA M S.p.A., titolare del trattamento, con la presente è a comunicarLe, l'intervenuta violazione dei Suoi dati personali (data breach) di cui è venuta a conoscenza alle ore [V_ORE] del [V_DATA_CONOSCENZA] che si è verificata, presumibilmente, in data [V_DATA_VIOLAZIONE].

Descrizione della violazione:
[V_NATURA]

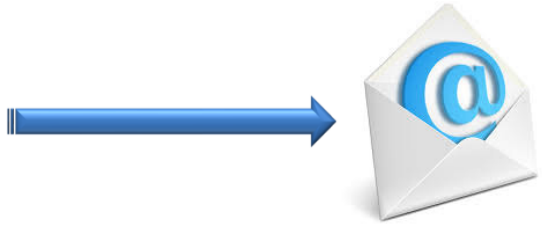
La violazione è classificabile come: [V_CLASSIFICAZIONE] [V_VALUTAZIONE].
La violazione presenta rischi relativi a: [V_RISCHIO]
Tale violazione è suscettibile di presentare un rischio [V_LIV_RISCHIO] per Suoi diritti e le libertà.

Per porre rimedio alla violazione e per contenere la violazione dei dati o per attenuarne i possibili effetti negativi sono state assunte le seguenti misure tecniche ed organizzative:
[V_MISURE]

Per poter ottenere maggiori informazioni relativamente alla violazione in oggetto, può contattare [V_CONTATTO] al seguente indirizzo: [V_MAIL_CONTATTO].

Distinti saluti

[V_CONTATTO]



P

mercoledì 11/07/2018 08:38

privacy@iltigliosrl.it

Da AZIENDA M S.p.A. relativamente al Regolamento Europeo per la protezione dei dati personali

A Giuliano Marullo

Da AZIENDA M S.p.A. relativamente al Regolamento Europeo per la protezione dei dati personali

Gentile Rossi S.p.A.,

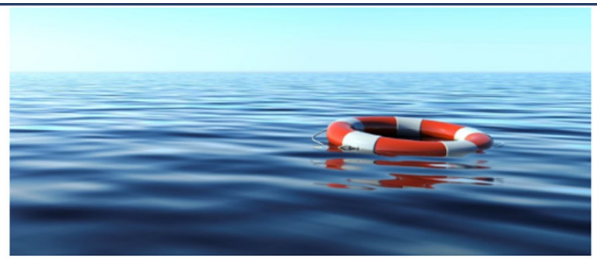
Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) 679/2016, La preghiamo di prendere visione della comunicazione relativa ad una violazione che potenzialmente ha coinvolto Suoi dati personali (data breach) da noi trattati.

La ringraziamo per la collaborazione.

AZIENDA M S.p.A.

Prema qui per visualizzare la Comunicazione relativa alla Violazione

SQuadra: Gestione Comunicazioni - Realizzata da Il Tiglio srl



Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) 679/2016, La preghiamo di prendere visione della comunicazione relativa ad una violazione che potenzialmente ha coinvolto Suoi dati personali (data breach) da noi trattati.
Nella comunicazione troverà tutte le informazioni sulla Violazione stessa ad oggi in nostro possesso e i dati per contattarci per avere eventuali chiarimenti.

La preghiamo di leggerla e quindi confermarne la presa visione.

Visualizza la Comunicazione

Presa visione dell'informativa

Dopo aver letto il documento allegato dichiaro di aver preso visione della Comunicazione relativa ad una potenziale Violazione dei dati personali.

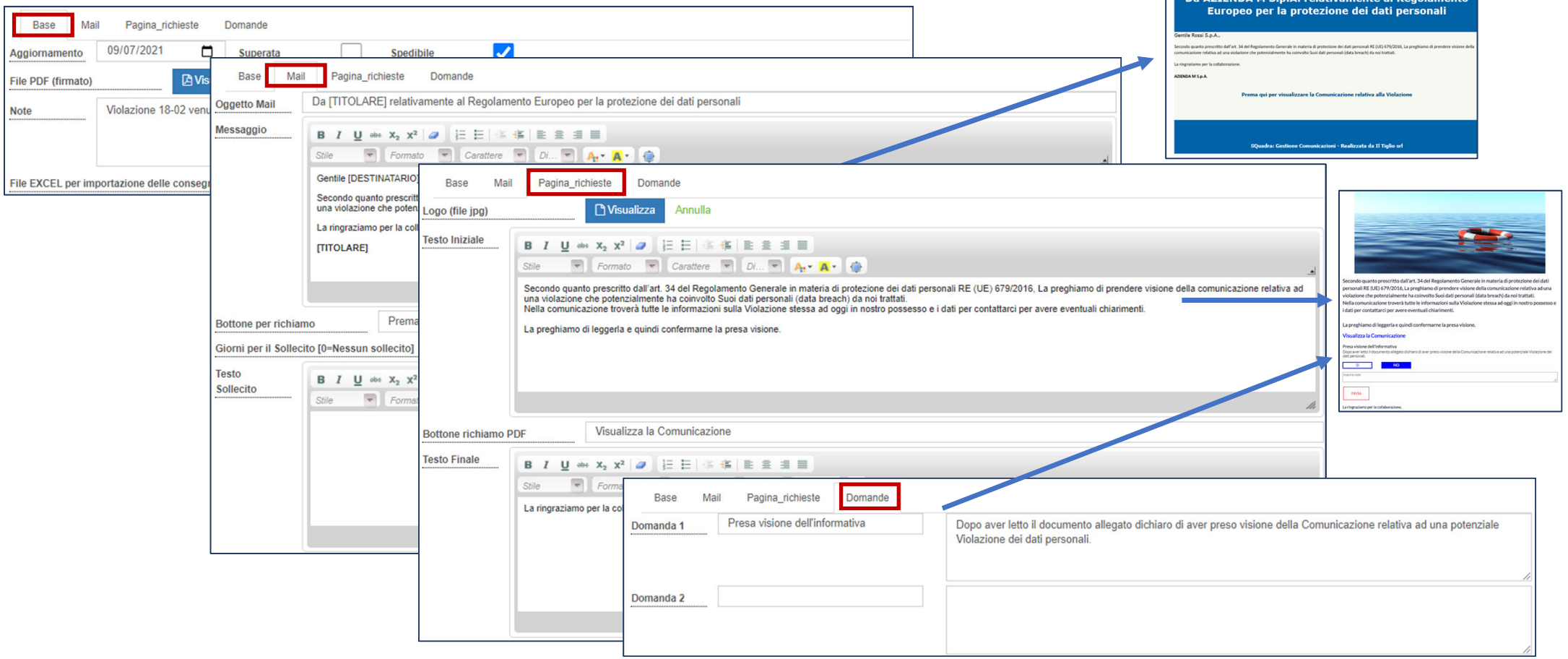
SI NO

Inserire note

INVIA

La ringraziamo per la collaborazione.

Predisposizione comunicazione violazione



Adeguatezza delle misure

FORMAZIONE

CONFORMITÀ

PREPARAZIONE AGLI INCIDENTI

TRATTAMENTI

INVENTARIO:
Apparati
Prodotti
Data Base
Dispositivi Mobili

SCADENZE

RESPONSABILITÀ

MINACCE

CONTROLLI

RIFERIMENTI
NORMATIVI

Art. 24: «… essere in grado di dimostrare..»

Scadenze

Responsabile	Attività	Misure	Risorse	Tempi	Criteri
Datore di Lavoro	Responsabili	Varificare adeguatezza di: Anna Bianchi			
Datore di Lavoro	Responsabili	Varificare adeguatezza di: Carlo Rosi			
Datore di Lavoro	Responsabili	Varificare adeguatezza di: Carlo Verdi			
Datore di Lavoro	Responsabili	Varificare adeguatezza di: Maria Gialli			
Resp. Personale	Trattamenti	T01.a - b. Personale: Gestione Paghe e note spese, rilevazione presenze e iscrizione a sindacati.		Prossima verifica 25/05/2019	
Resp. Personale	Trattamenti	T01.b - b. Personale: Valutazioni, prowedimenti disciplinari, licenziamenti.		Prossima verifica 25/05/2019	
Resp. Personale	Trattamenti	T01.c - b. Personale: Reclutamento, Curricula		Prossima verifica 25/05/2019	
Resp. Personale	Trattamenti	T01.d - b. Personale: Formazione ed addestramento		Prossima verifica 25/05/2019	
Resp. Personale	Trattamenti	T01.e - b. Personale: Sorveglianza sanitaria		Prossima verifica 25/05/2019	
Resp. Personale	Trattamenti	T01.f - d. Consulenti e collaboratori: Formazione		Prossima verifica 25/05/2019	
Resp. Sistemi Informatici	Formazione	Gialli	Formazione incaricati	Prossima formazione 16/11/2018	
Resp. Sistemi Informatici	Formazione	Rossi	Formazione incaricati	Prossima formazione 16/11/2018	
Resp. Sistemi Informatici	Formazione	Verdi	Formazione incaricati	Prossima formazione 16/11/2018	
Resp. Sistemi Informatici	Apparati	Verificare: Server 01 per:File e Exchange		Prossima verifica 10/01/2019	
Resp. Sistemi Informatici	Conformità	Verificare la conformità delle attuali informative con il Regolamento europeo	Supporto consulenziale	Entro Maggio 2018	Verifica con il consulente
Resp. Sistemi Informatici	Controlli	A.05.1:1: Verificare Politica			
Resp. Sistemi Informatici	Controlli	A.06.2:1: Dovrà essere applicata la crittografia a tutti i portatili.	Utilizzo dei consulenti IT	Entro la fine dell'anno.	
Resp. Sistemi Informatici	Controlli	A.06.2:2: Controllare telelavoro.			
Resp. Sistemi Informatici	Controlli	A.07.2:1: Controllare attività utenti			
Resp. Sistemi Informatici	Controlli	A.14.2:8: Effettuare test			
Resp. Sistemi Informatici	Controlli	A.18.1:1: Analizzare aggiornamenti GDPR			
Resp. Sistemi Informatici	Controlli	A.18.2:1: Far effettuare un riesame indipendente.			
Resp. Sistemi Informatici	Controlli	A.18.2:3: Riesame SI			
Resp. Sistemi Informatici	Controlli AgID	Completare l'inventario.			Verifica della completezza dell'inventario.
Resp. Sistemi Informatici	Controlli Cyber Security	Verificare inventario			
Resp. Sistemi Informatici	Controlli Cyber Security per PMI	Verificare gli asset			
Resp. Sistemi Informatici	Controlli Cyber Security: 2015-PMI	Appartati e Prodotti			
Resp. Sistemi Informatici	Controlli Cyber Security: 2016-Controlli	SQuadra GDPR Prodotti			
Resp. Sistemi Informatici	DataBase	Verificare: DB Amministrativo per:Gestione di tutti i dati amministrativi		Prossima verifica 01/03/2020	
Resp. Sistemi Informatici	DataBase	Verificare: DB Cantieri per:Gestione di tutti i dati Cantieri		Prossima verifica 01/03/2020	
Resp. Sistemi Informatici	Minacce	A01: Migliorare le misure antincendio.			
Resp. Sistemi Informatici	Minacce	D04: Prevedere l'installazione di una porta blindata.		Entro il prossimo anno	
Resp. Sistemi Informatici	Prodotti	Verificare: Microsoft WORD per:Gestione testi			
Resp. Sistemi Informatici	Responsabili	Varificare adeguatezza di: Mario Rossi		Prossima verifica 05/09/2019	
Resp. Sistemi Informatici	Tratt-Resp.Esterni	Verifica adeguatezza: Società Servizi Informatici		Prossima verifica 10/05/2019	
Resp. Sistemi Informatici	Trattamenti	T00.a - a. Sistema Informativo: Manutenzione del sistema informatico		Prossima verifica 25/05/2019	

SQuadra-Privacy

A **IL PROGETTO SQUADRA-EDILIZIA**
Dal 2008 uno strumento a disposizione delle imprese associate.

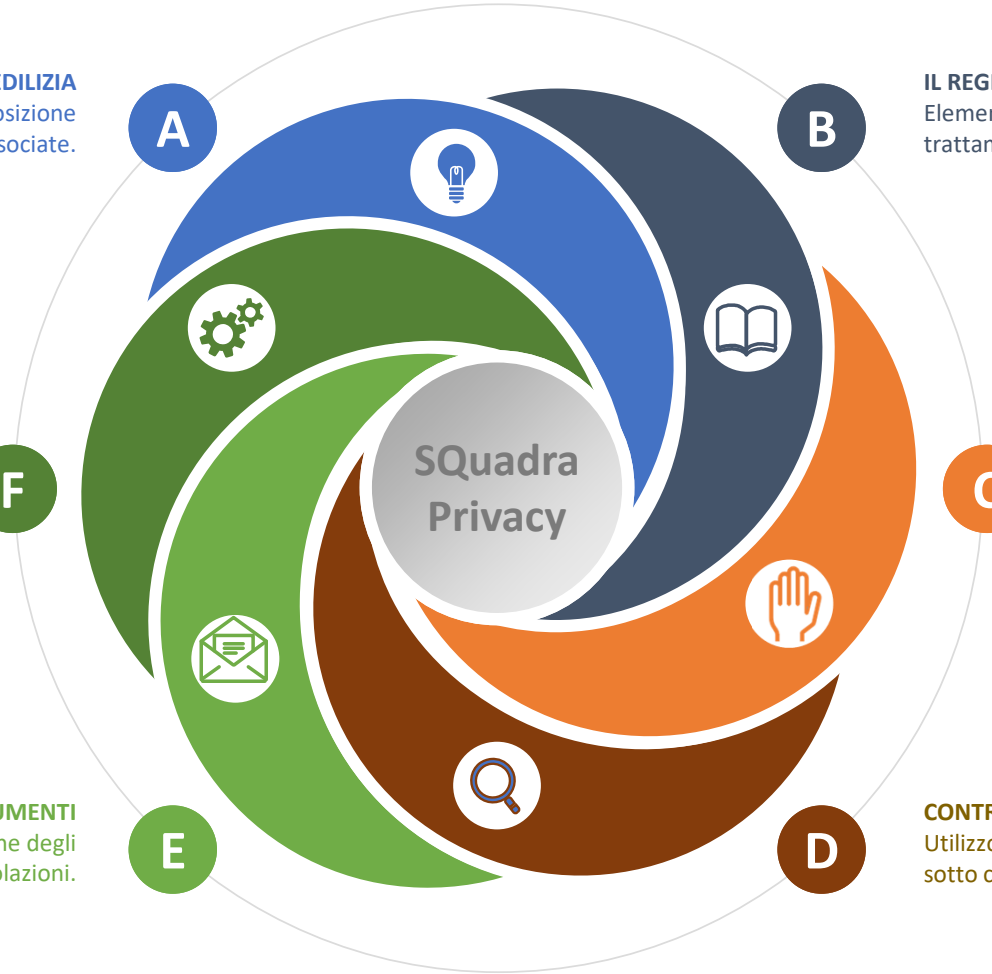
B **IL REGISTRO DEI TRATTAMENTI**
Elemento essenziale per l'analisi dei trattamenti effettuati.

C **CONFORMITÀ E MINACCE**
Autovalutazione della situazione di partenza e degli obiettivi.

D **CONTROLLI**
Utilizzo delle migliori pratiche per tenere sotto controllo i sistemi informatici.

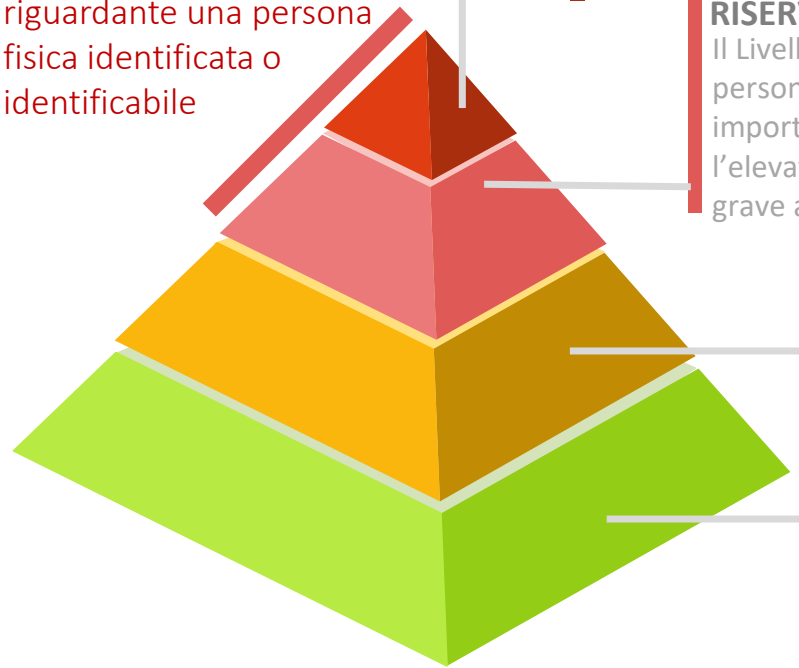
E **ALTRI STRUMENTI**
Documenti aggiuntivi e gestione degli incidenti e delle violazioni.

F **SICUREZZA DELLE INFORMAZIONI**
Problematiche tipiche e specifiche relative all'utilizzo delle nuove tecnologie.



Classificazione delle informazioni aziendali

Dato personale:
qualsiasi informazione riguardante una persona fisica identificata o identificabile



CONFIDENZIALE
Il Livello di classificazione “Confidenziale” si applica alle informazioni la cui diffusione potrebbe causare serio danno all’Azienda, comportando conseguenze economiche e legali significative e danneggiando seriamente la reputazione dell’azienda, delle società ad essa collegate o delle partecipate, con notevoli impatti su beni e asset aziendali. In genere solo un ristretto numero di persone, debitamente autorizzate, può accedere a queste informazioni.

RISERVATA
Il Livello di classificazione “Riservata” si applica alle informazioni il cui utilizzo è limitato a un gruppo di persone, come ad esempio un Ufficio. In genere le informazioni classificate Riservate sono considerate importanti ai fini della sicurezza aziendale, da un punto di vista gestionale, finanziario ed organizzativo, o per l’elevato contenuto tecnologico. La perdita, anche accidentale, di tali informazioni può causare un danno grave all’Azienda. La conoscenza di tali informazioni può costituire rilevante valore per la concorrenza.

INTERNA
Il Livello di classificazione “Interna” si applica alle informazioni il cui utilizzo è limitato ai dipendenti della Società e al personale di società esterne che svolgono lavori in outsourcing o attività di consulenza per l’Azienda. Questo livello di classifica si applica a quelle informazioni la cui compromissione potrebbe causare un danno lieve per la Società. In genere tali informazioni sono accessibili anche ai partner commerciali o industriali.

PUBBLICA
Il Livello di classificazione “Pubblica” si applica alle informazioni il cui utilizzo non può causare alcun danno all’Azienda. Tali informazioni possono essere considerate di pubblico dominio, essendo generalmente accessibili o disponibili al pubblico. Le informazioni che potrebbero essere pubblicate sul sito internet della Società, ad esempio, rientrano all’interno di tale categoria.

Obblighi - Opportunità

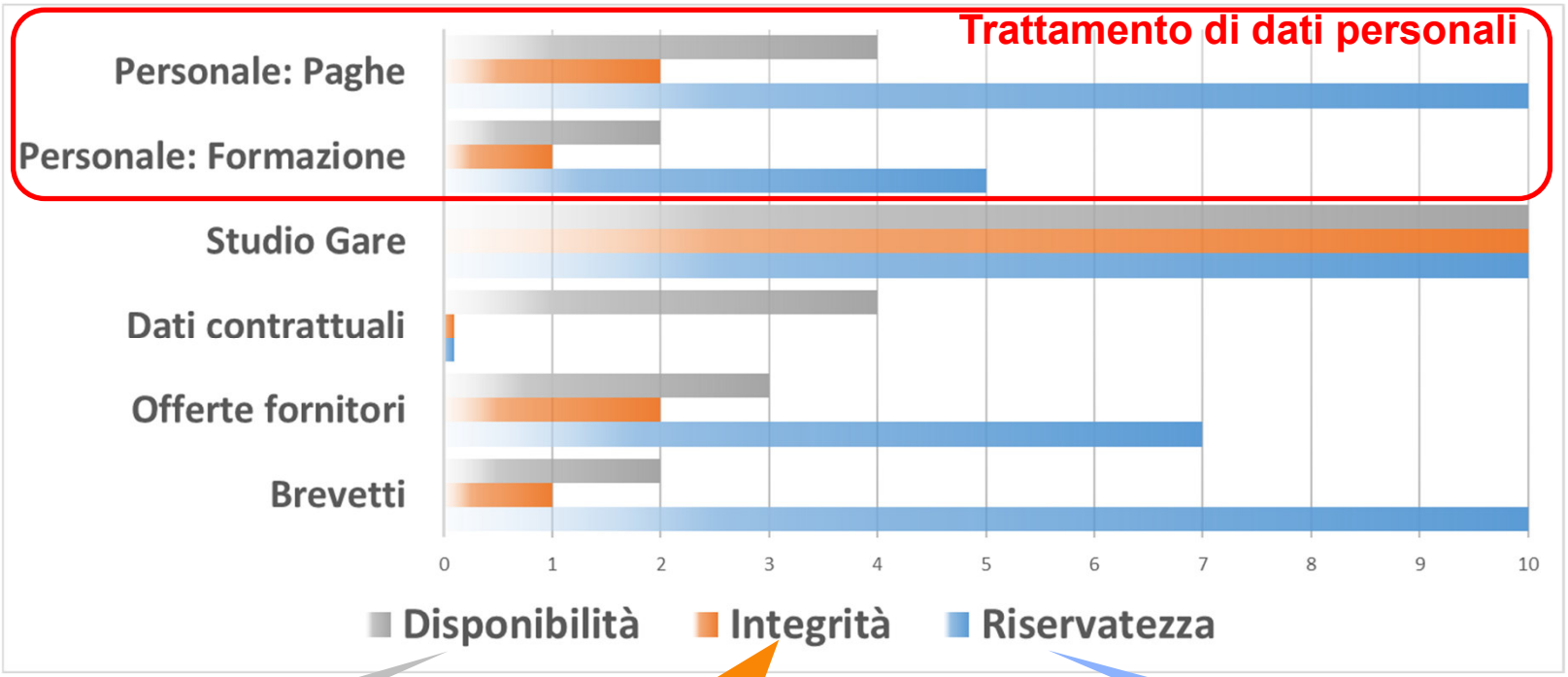
Evoluzione nell'uso delle nuove tecnologie
Scarsa consapevolezza sulla
Sicurezza delle informazioni Aziendali

Opportunità di miglioramento

Conformità al Regolamento per il Trattamento dei dati personali

Obblighi specifici

Criticità dei Trattamenti



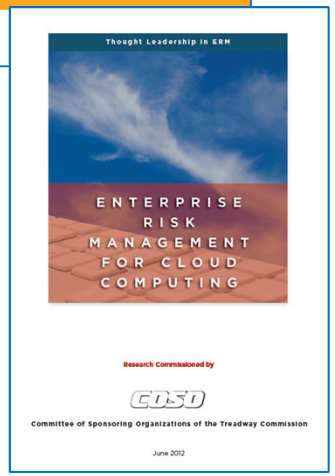
Quanto posso stare senza

Quanto impiego a recuperare i dati da altre fonti

Danno per la divulgazione

Criticità dei dati

	Diponibilità	Integrità	Riservatezza
Paghe	  **Anticipo + Saldo** 	  **Backup + Reinserimento** 	  **Sicurezza Informatica e sui dati cartacei**
Gare	 **Dati sul Cloud** *99,95% [4 ore/anno]*	 **Cronologia delle versioni**	 **Sicurezza Informatica**



Cloud e Password

Gestione non corretta delle PW

Server aziendale

Soluzione Cloud

Rischi connessi ad una non corretta gestione delle Password

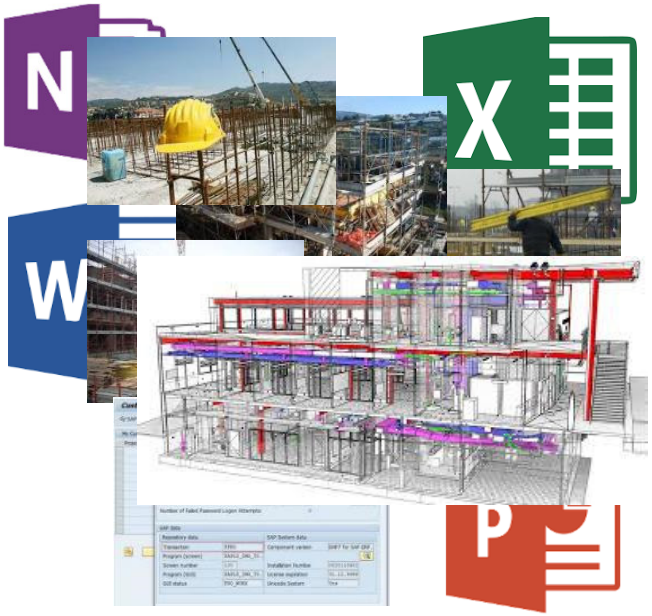
Cloud ed organizzazione

Soluzione Cloud

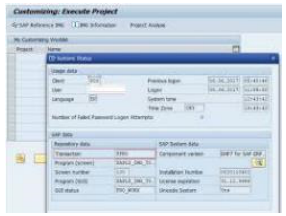
Google Drive Dropbox

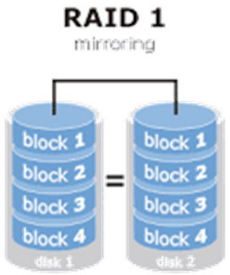
Soluzioni Cloud non richiedono competenze o investimenti.

Organizzazione dei dati



Classificazione dei dati





Dropbox Business

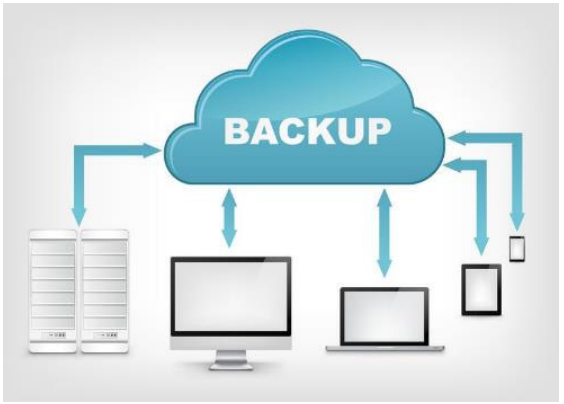
Microsoft Teams

- Etichette di conservazione e di riservatezza
- Definizione eventi (es. Cessazione del rapporto di lavoro, Conclusione commessa)

Google Drive

Dropbox

Backup



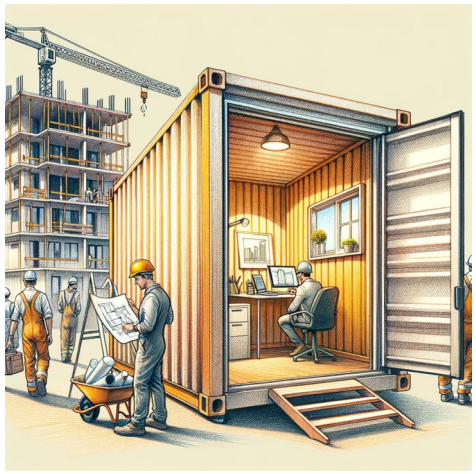
Utilizzo
Crittografia

Sicurezza
Supporti

Prove di ripristino

Accesso da remoto

Sicurezza informazioni in Cantiere



Ufficio di cantiere oggi quasi sempre dotato di PC, stampanti e connessione ad Internet.

APPALTATORE **SUBAPPALTATORE**

Concede l'uso del PC ad esterni

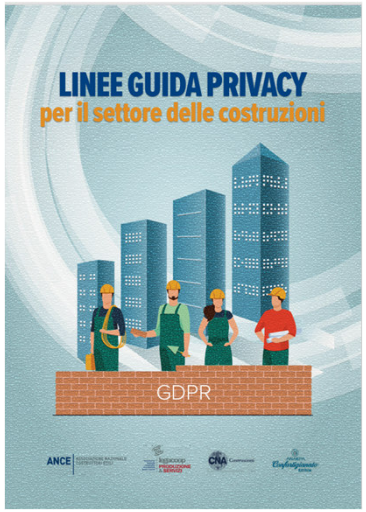
Utilizza un PC di altri

Concede l'uso della Rete

Utilizza la Rete

Concede l'uso del WiFi

Utilizza la Rete tramite WiFi



Se Appaltatore e Subappaltatore adottano le Linee Guida non andrà valutata l'adeguatezza delle misure di sicurezza ogni volta.

Documenti-Privacy

Gestione dei documenti via WEB

Documenti aggiornati

Gruppo di progetto centralizzato

Aggiornato

Titolare

Interessati

Preleva il documento proposto

Personalizzazioni effettuate dall'emissione

Personalizzazioni effettuate sull'originale

Modifiche apportate nell'aggiornamento

Emesso

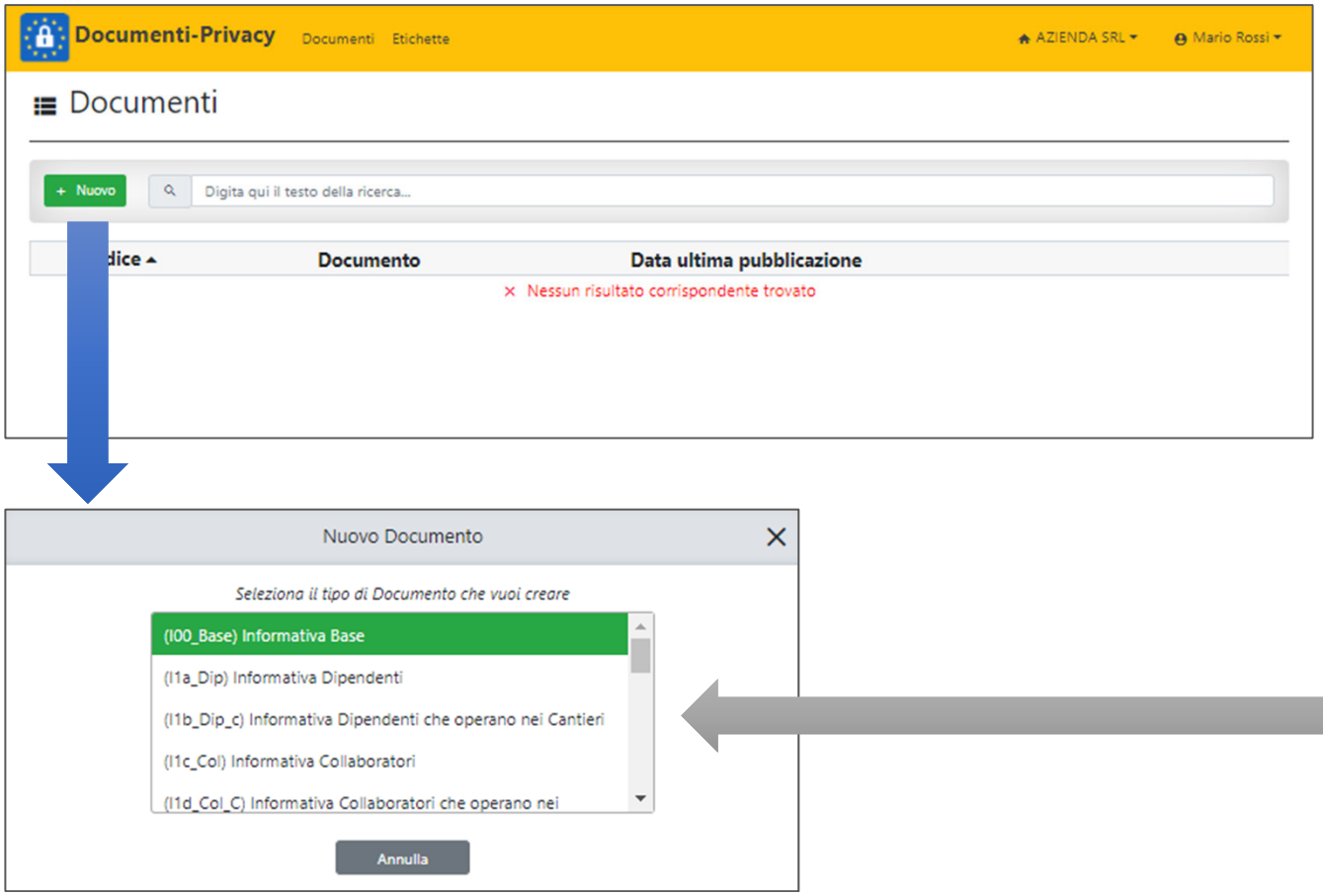
Emette il documento

Personalizzato

Personalizza il documento

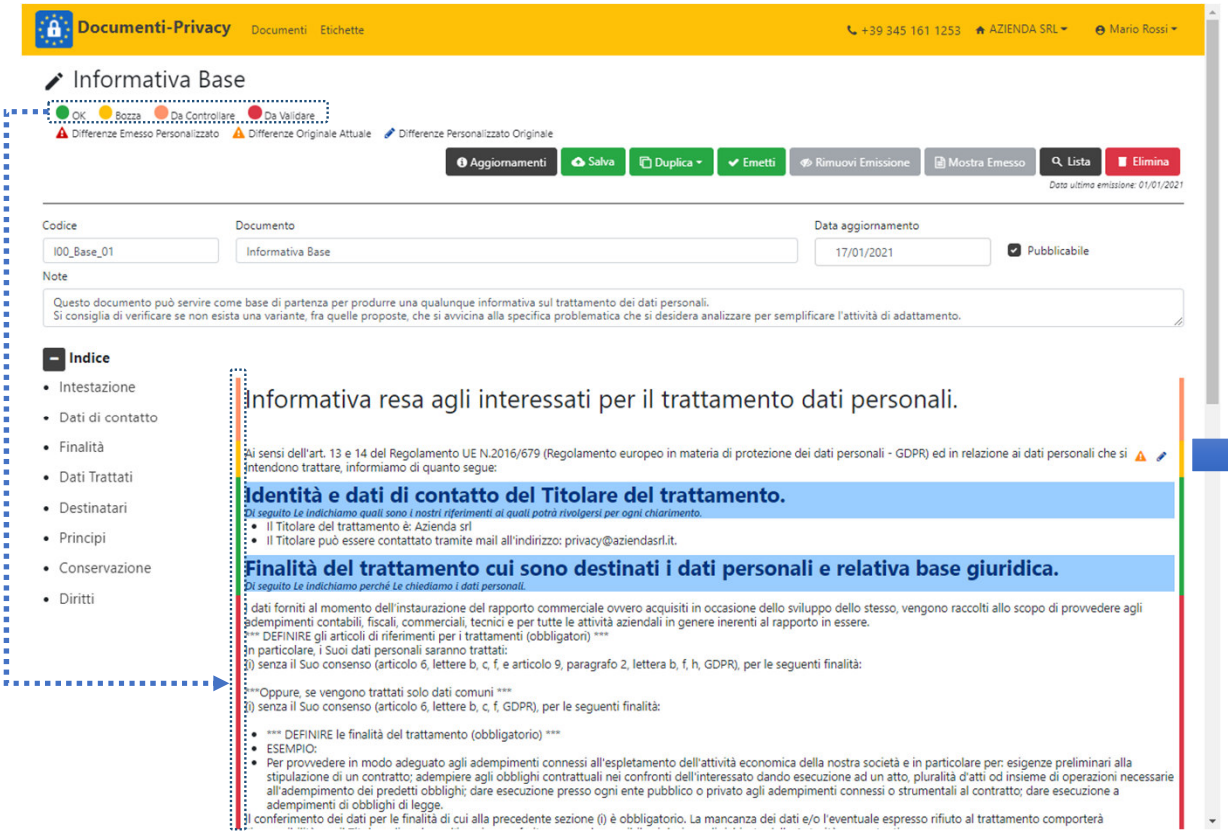
Originale

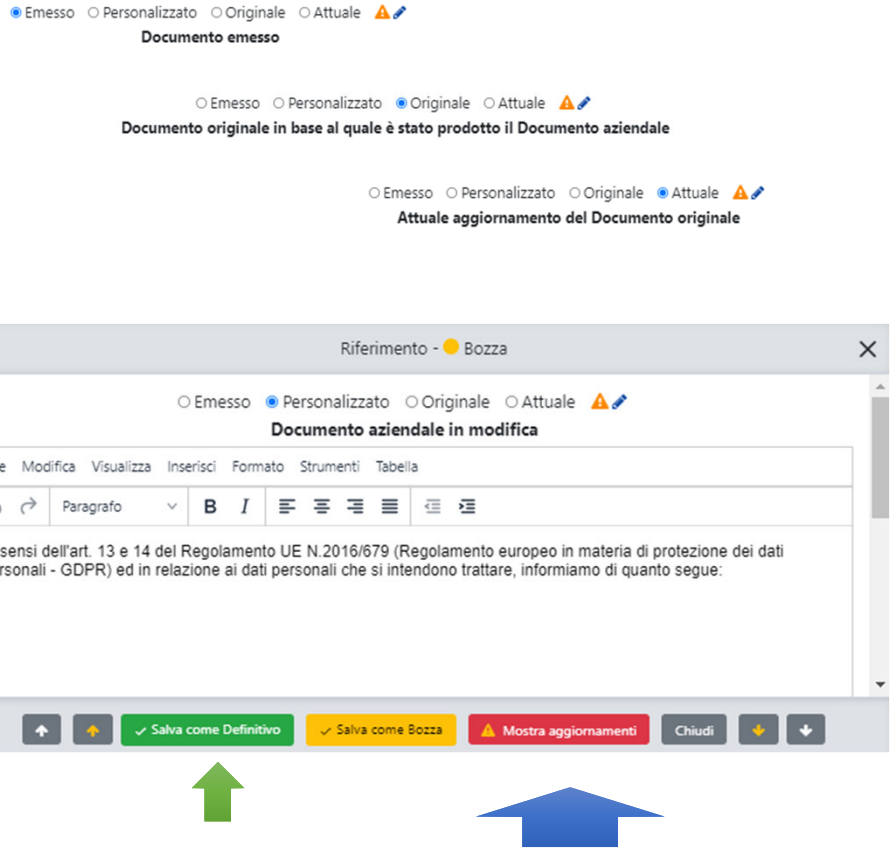
Documenti disponibili



Documenti di base forniti
Informativa Base
Informativa Dipendenti
Informativa Dipendenti che operano nei Cantieri
Informativa Collaboratori
Informativa Collaboratori che operano nei Cantieri
Informativa di Filiera
Informativa COVID-19 - Lavoratori
Informativa COVID-19 - Esterni
Informativa Curricula
Informativa Clienti (persone fisiche)
Informativa Clienti (società)
Informativa Committenti
Informativa Fornitori (persone fisiche)
Informativa Fornitori (società)
Informativa Supappaltatori
Informativa Sito
Informativa Sito con cookie
Informativa Mail
Valutazione Impatto per la Geolocalizzazione
Valutazione Impatto per la Videosorveglianza

Modifica del testo





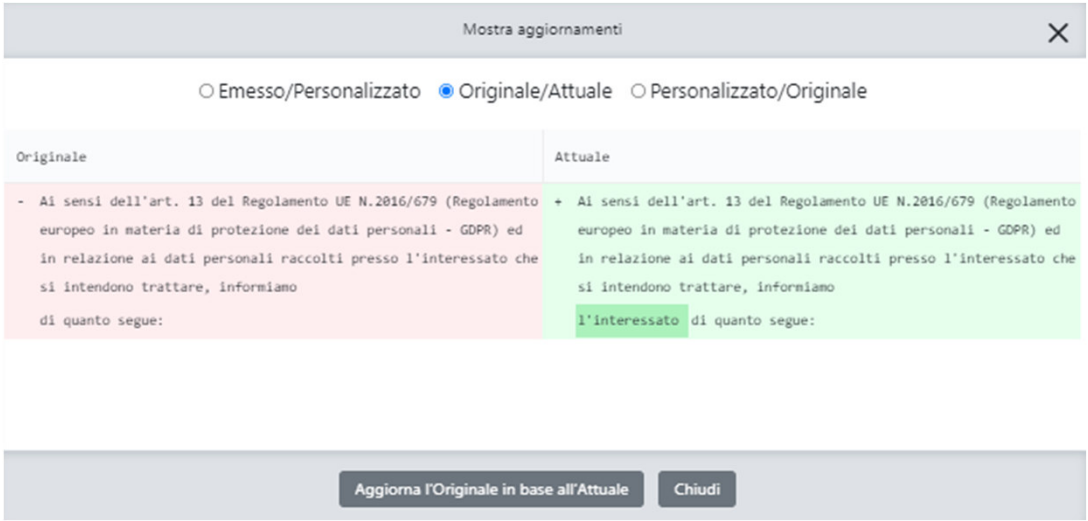
Analisi modifiche

Modifiche effettuate, a partire dall'originale disponibile all'epoca, per personalizzare il documento alle esigenze aziendali:

- *Aggiunto il riferimento all'Art. 14.*
- *Tolta la raccolta presso l'interessato.*

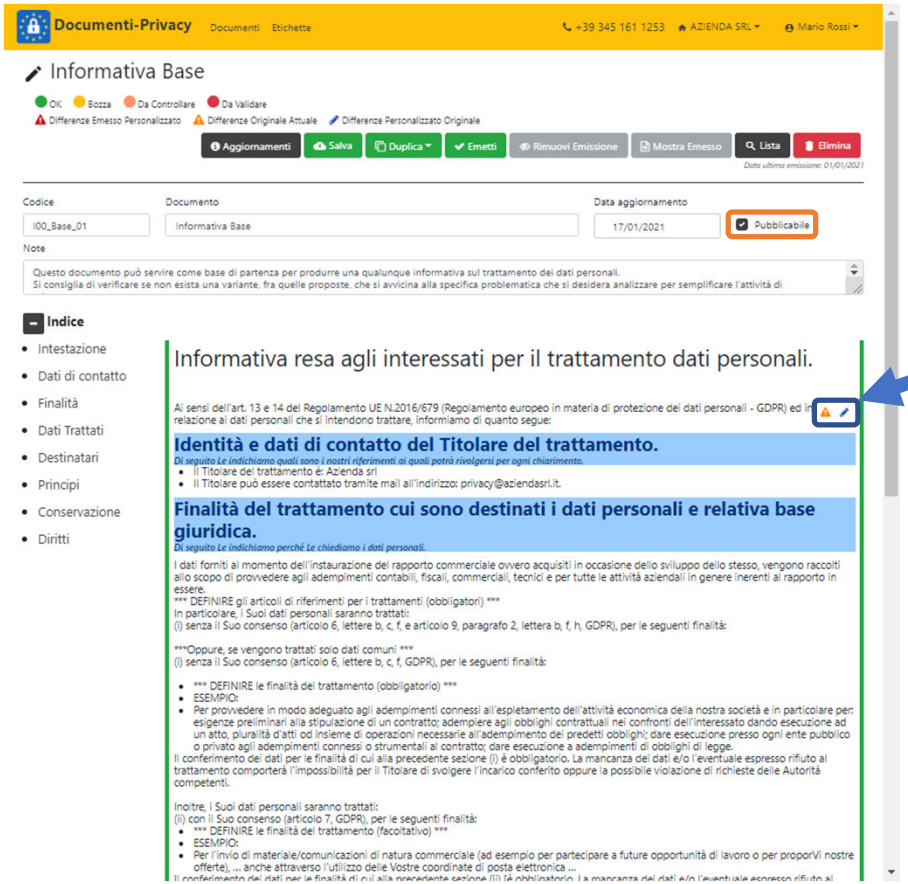
Modifiche effettuate ultimamente dal Gruppo di Progetto centrale per modifiche normative o miglioramenti:

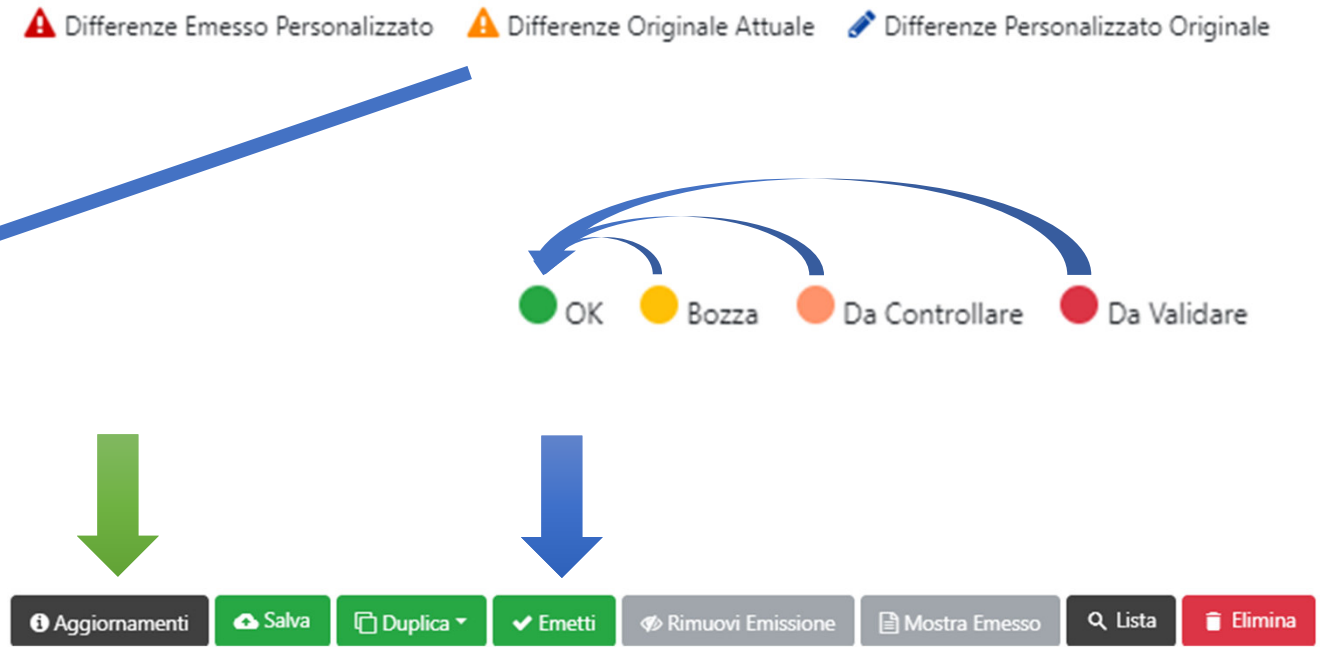
- *Aggiunto il riferimento all'interessato.*



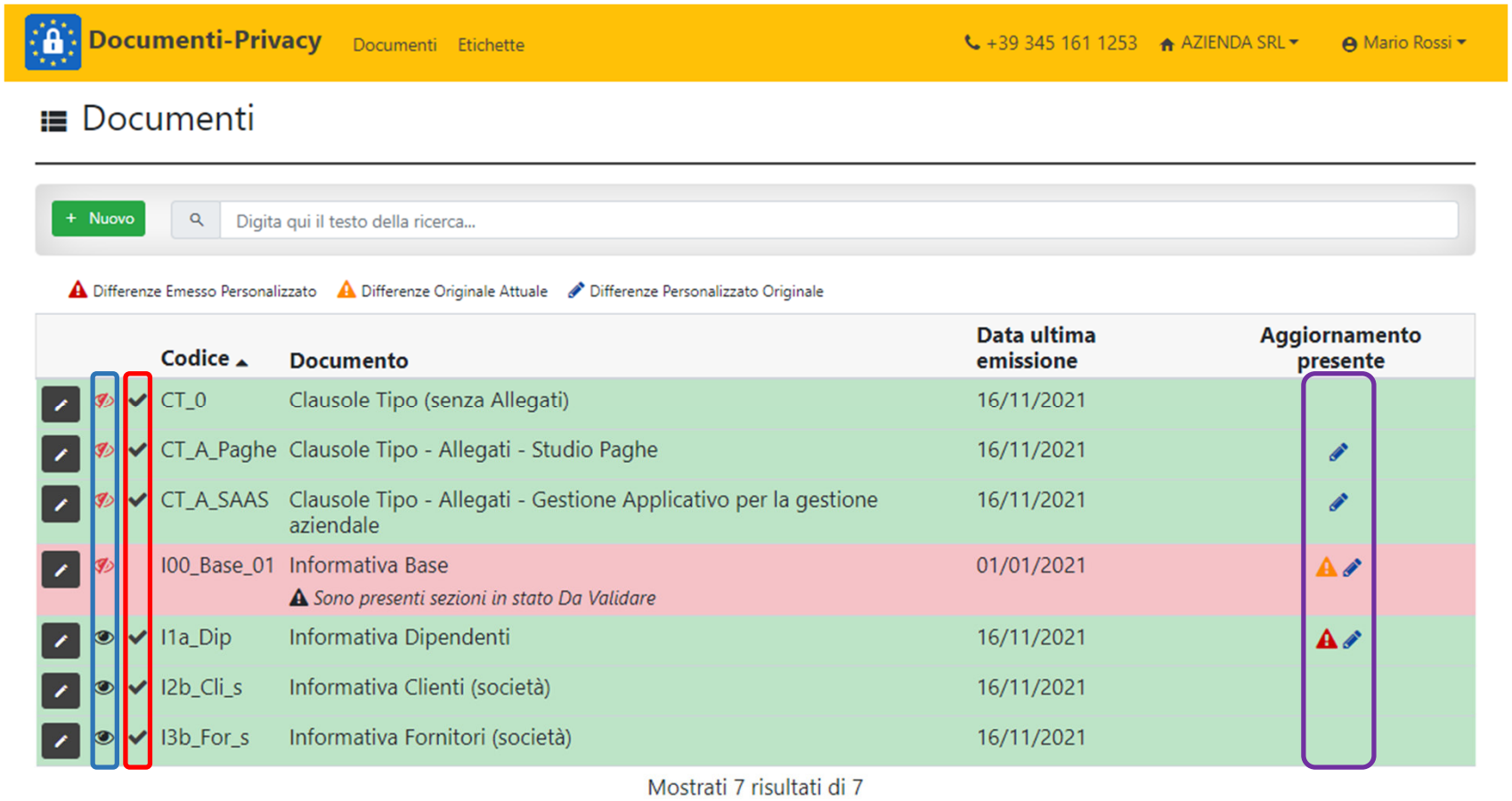
Una volta recepiti i nuovi suggerimenti.

Salvare le modifiche effettuate





Elenco Documenti



Emessi / Da emettere

Pubblicati sul WEB

Stato aggiornamenti

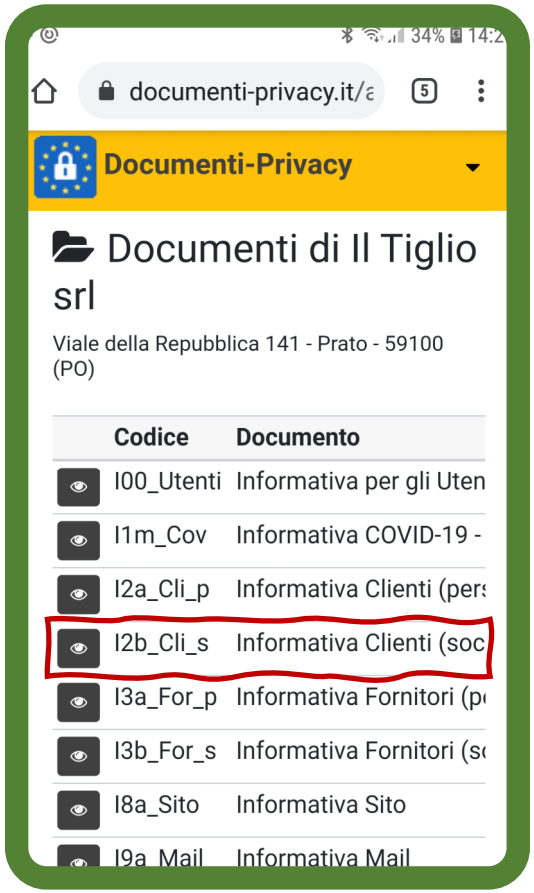
Consultazione Informative

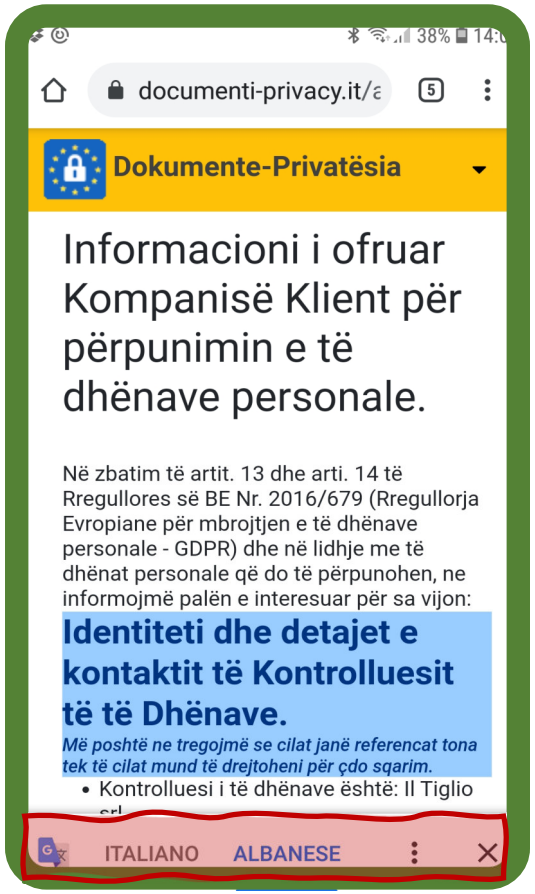
Molti lavoratori stranieri

Scrivendo l'indirizzo «documenti-privacy» nella carta intestata

Con l'inserimento della Partita IVA

Oppure da un LINK nel proprio SITO





SQuadra – Trattamento dei dati personali

Descrizione, Data ultima modifica.
Se sono presenti dati personali
Tempi di conservazione (dall'ultima modifica).
Per quelli legati ad un Lavoratore (tempi di conservazione dalla cessazione del rapporto).

SQuadra – Trattamento dei dati personali

Dati anagrafici e lavorativi

Documenti personali

Anonimizzazione

Dati visite mediche

Prescrizioni per idoneità

Allegati alle visite

Formazione

Conservazione per un periodo dall'evento

Conservazione dopo la cessazione del rapporto

SQuadra - Segnalazioni

D.Lgs. 24/23 – Protezione segnalanti (whistleblower)

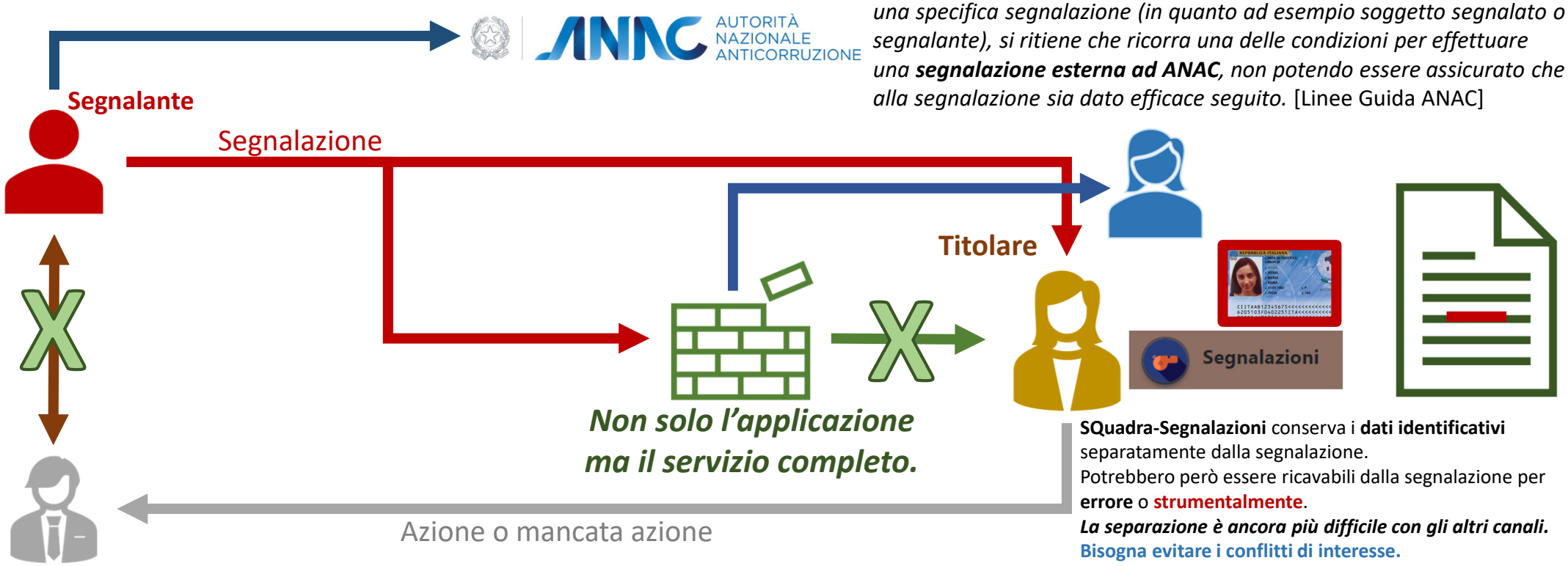
Comunicazioni ordinarie

DECRETO LEGISLATIVO 10 marzo 2023, n. 24 riguarda la **protezione** delle persone che segnalano violazioni da qualunque «**danno**» contribuendo all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per l'ente e, di riflesso, per l'interesse pubblico collettivo.

È opportuno che chiunque venga a conoscenza di violazioni lo segnali direttamente nell'ambito lavorativo.

Protezione da segnalazioni «strumentali»

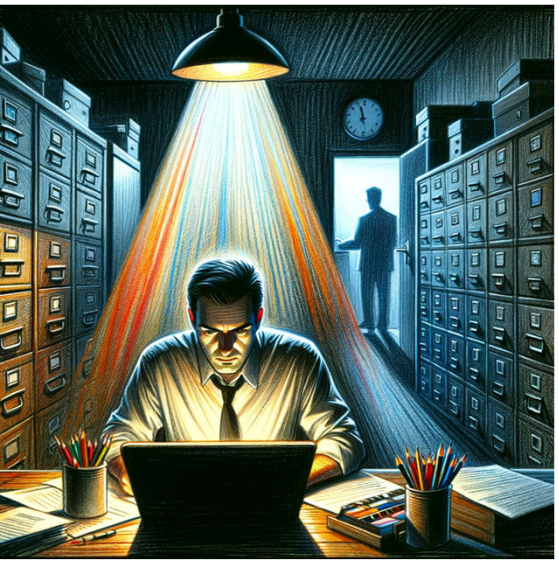
*Laddove **il gestore** versi in un'ipotesi di **conflitto di interessi** rispetto ad una specifica segnalazione (in quanto ad esempio soggetto segnalato o segnalante), si ritiene che ricorra una delle condizioni per effettuare una **segnalazione esterna ad ANAC**, non potendo essere assicurato che alla segnalazione sia dato efficace seguito.* [Linee Guida ANAC]



SQuadra-Segnalazioni conserva i **dati identificativi** separatamente dalla segnalazione.
Potrebbero però essere ricavabili dalla segnalazione per **errore** o **strumentalmente**.
La separazione è ancora più difficile con gli altri canali.
Bisogna evitare i conflitti di interesse.

*La persona deve solo **dimostrare** di aver **effettuato una segnalazione** e di aver **subito un danno**.*
*Salvo prova contraria, **il danno si presume derivato dalla segnalazione**.*

Canali interni



Scritto informatico

Scritto cartaceo

Orale

Incontro diretto

Scritto informatico

Ingresso al canale

Canale interno per le segnalazioni *(ai sensi del D.Lgs. 24/23)*

Questo canale permette a **chiunque di comunicare con l'Ente** sulla base della *Politica per la gestione delle segnalazioni* consultabile dal bottone "Politica" presente in basso.
ATTENZIONE: Questo canale non deve essere utilizzato per emergenze! *In caso di pericolo immediato bisogna contattare le autorità competenti.*

Nuova segnalazione

Identificativo

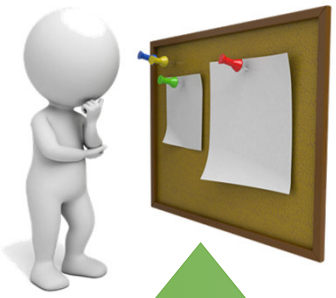
Password

Password o Codice dimenticati?

Controllo segnalazione

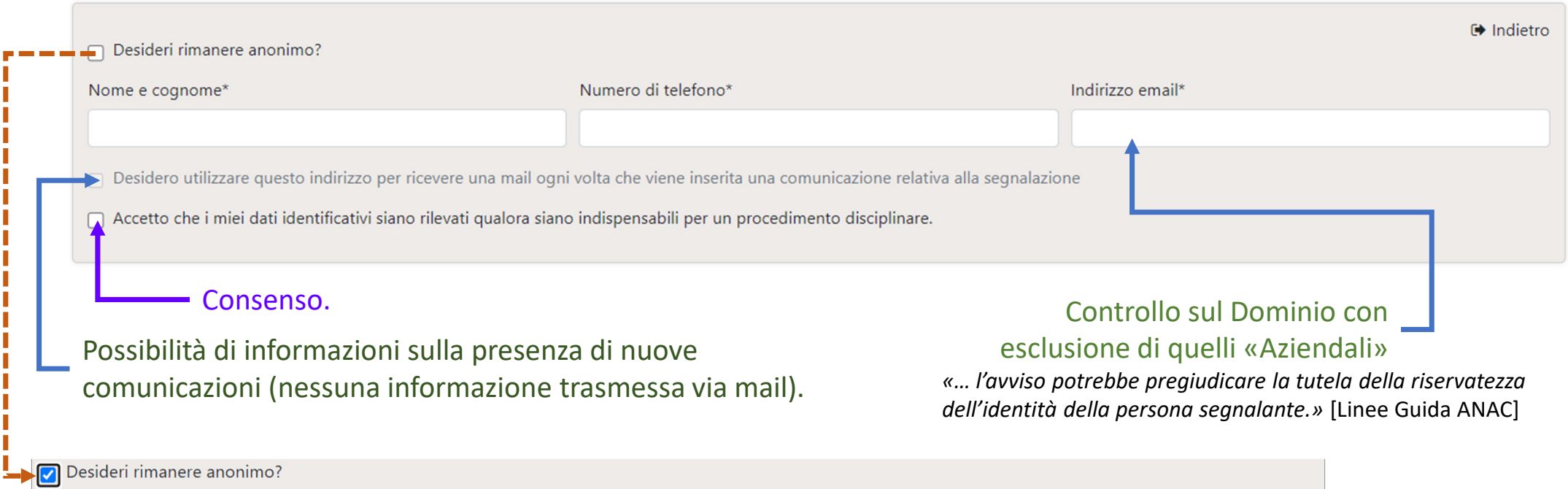
Istruzioni | Informativa privacy | Politica

Modalità per effettuare le Segnalazioni



Politica per le segnalazioni e procedura aziendale

Nuova Segnalazione - Segnalante

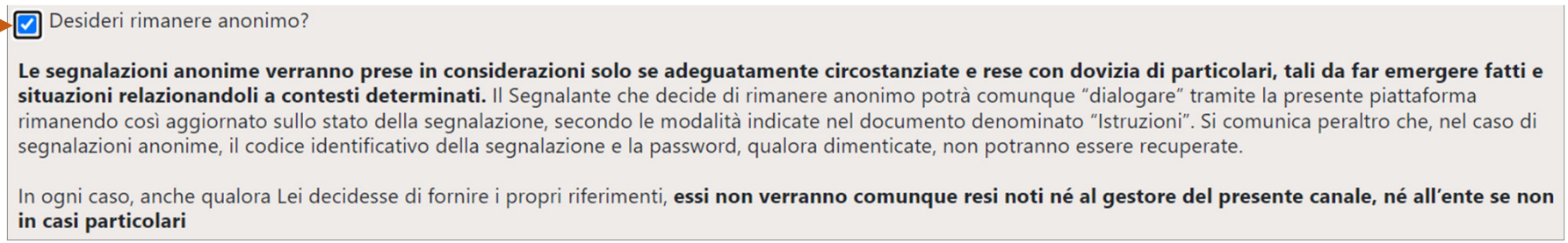


Consenso.

Possibilità di informazioni sulla presenza di nuove comunicazioni (nessuna informazione trasmessa via mail).

Controllo sul Dominio con esclusione di quelli «Aziendali»

«… l'avviso potrebbe pregiudicare la tutela della riservatezza dell'identità della persona segnalante.» [Linee Guida ANAC]



Il consenso

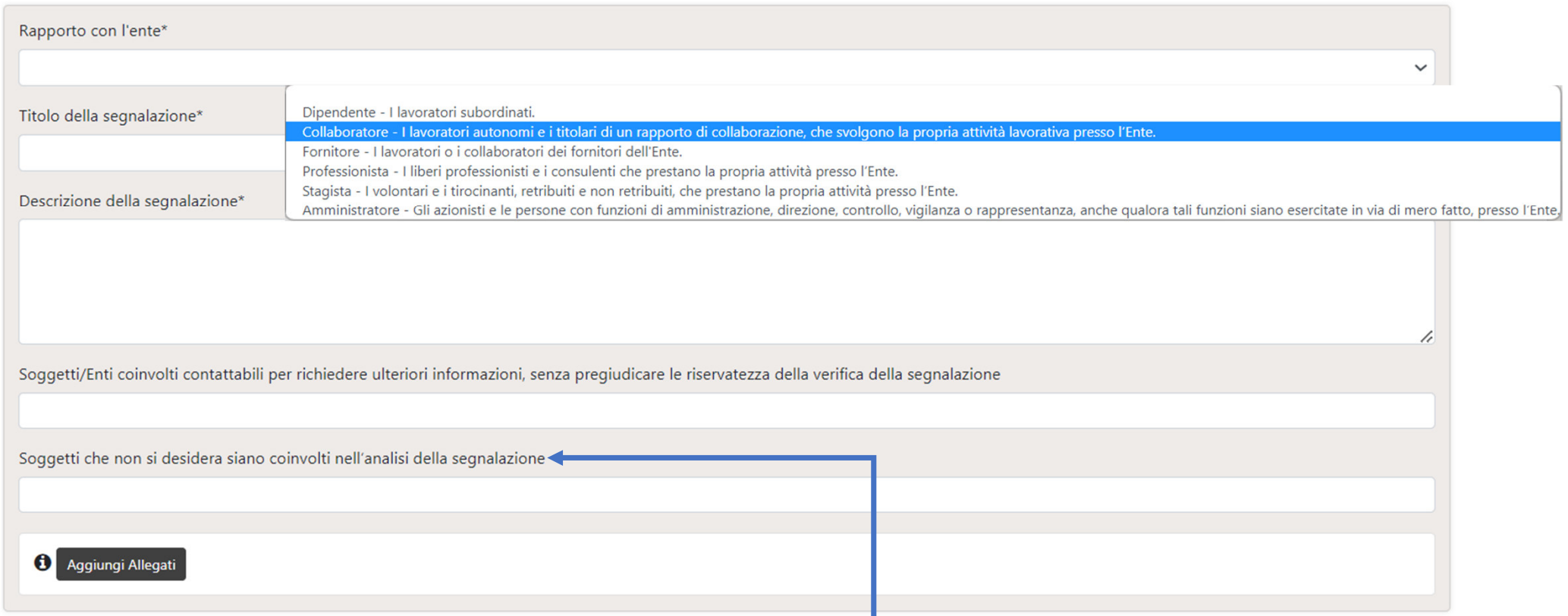
Il D.Lgsl 24/2023 prevede che "*Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del* ***consenso espresso della persona segnalante*** *alla rivelazione della propria identità*".

Bisogna però considerare, come indicato dalle "**Linee Guida sul consenso ai sensi del regolamento**" adottate dall'European Data Protection Board nel maggio 2020: "*lo* ***squilibrio di potere*** *che sussiste nel contesto dell'occupazione. Data la dipendenza risultante dal rapporto datore di lavoro/dipendente,* ***è improbabile che l'interessato sia in grado di negare al datore di lavoro il consenso*** *al trattamento dei dati senza temere o rischiare di subire ripercussioni negative come conseguenza del rifiuto*".

Per questi motivi viene **richiesto già in fase iniziale**, quando il **segnalante è totalmente libero**, la disponibilità del segnalante alla rilevazione della propria identità.

In ogni caso la **richiesta del consenso viene effettuata dal Gestore dei Canali** verso il quale il segnalante non ha rapporti e quindi il suo **eventuale consenso sarà libero.**

Nuova Segnalazione - Elementi



Possibilità di definire eventuali soggetti che non devono essere coinvolti nella gestione della segnalazione

Codice Univoco

Limite ai tentativi di ingressi giornalieri errati

Possibilità di definire un codice facilmente memorizzabile

Codice segnalazione*

Password*

Verifica password*

☐ *Ho memorizzato il **codice della segnalazione** e la password. Ho compreso che per la riservatezza non potrò recuperare il codice in altro modo. Ho scelto il **codice della segnalazione** senza nessun riferimento a dati personali* (qualora presenti il Gestore del canale sarà costretto ad **eliminare la segnalazione**) *

Premendo **INVIA SEGNALAZIONE** questa verrà gestita in modo sicuro. Ritornando sul canale ed inserendo il *codice* e la *password* potrà visualizzare la risposta o eventuali domande o inviare informazioni aggiuntive.

☐ **Acconsento** a che i miei dati personali possono essere trattati allo scopo di indagare e gestire la mia segnalazione in conformità con l'informativa sulla privacy che ho letto e accettato.*

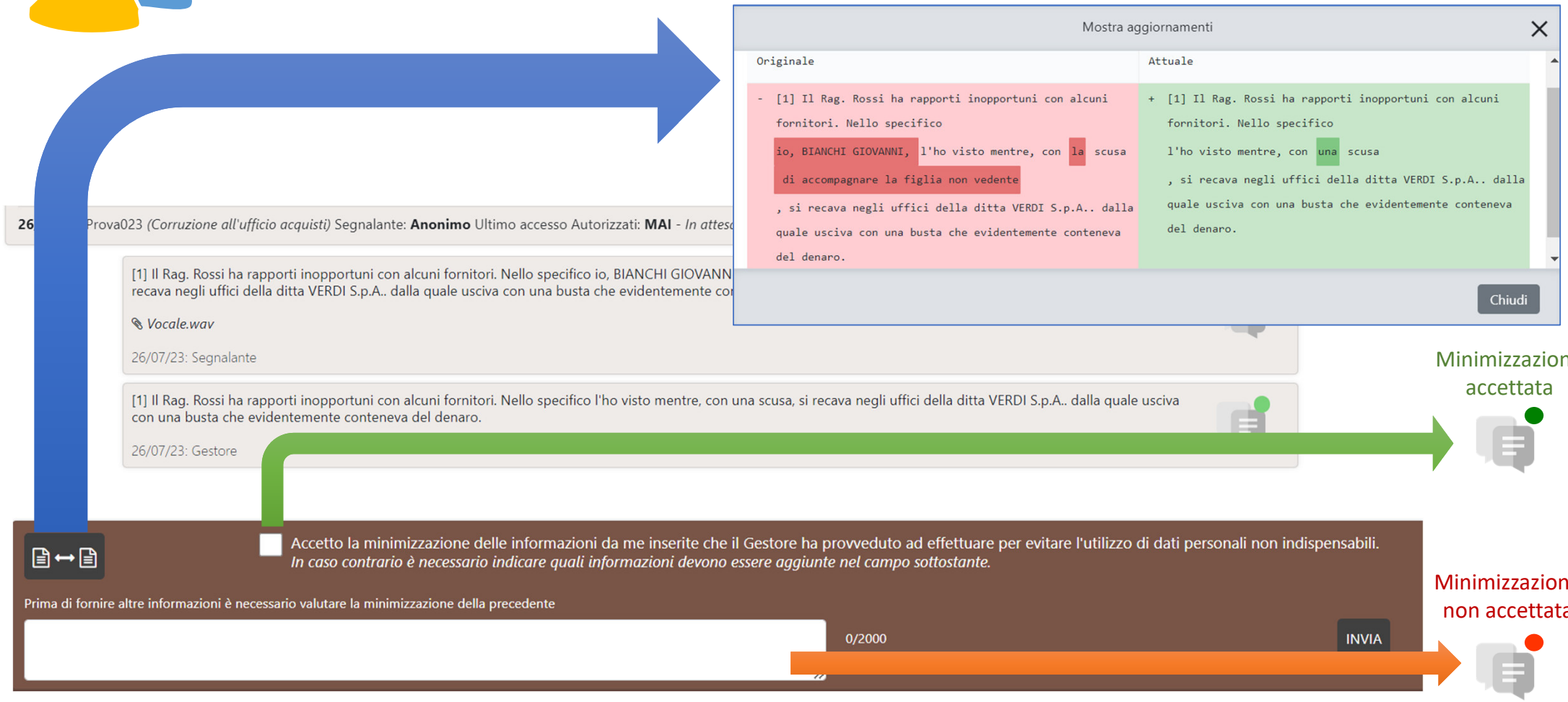
☐ Ho compreso che è opportuno **non inserire riferimenti alla mia identità** nella segnalazione ed eventualmente rimuoverli o oscurarli da eventuali allegati. È, inoltre, opportuno **limitare al massimo i riferimenti a dati personali di terzi** non necessari per la comprensione della segnalazione. Ho compreso che **rimarrò personalmente responsabile dell'eventuale contenuto diffamatorio delle comunicazioni**. *

Informativa Privacy

INVIA SEGNALAZIONE

Richiesta di minimizzare i dati.

Controllo minimizzazione

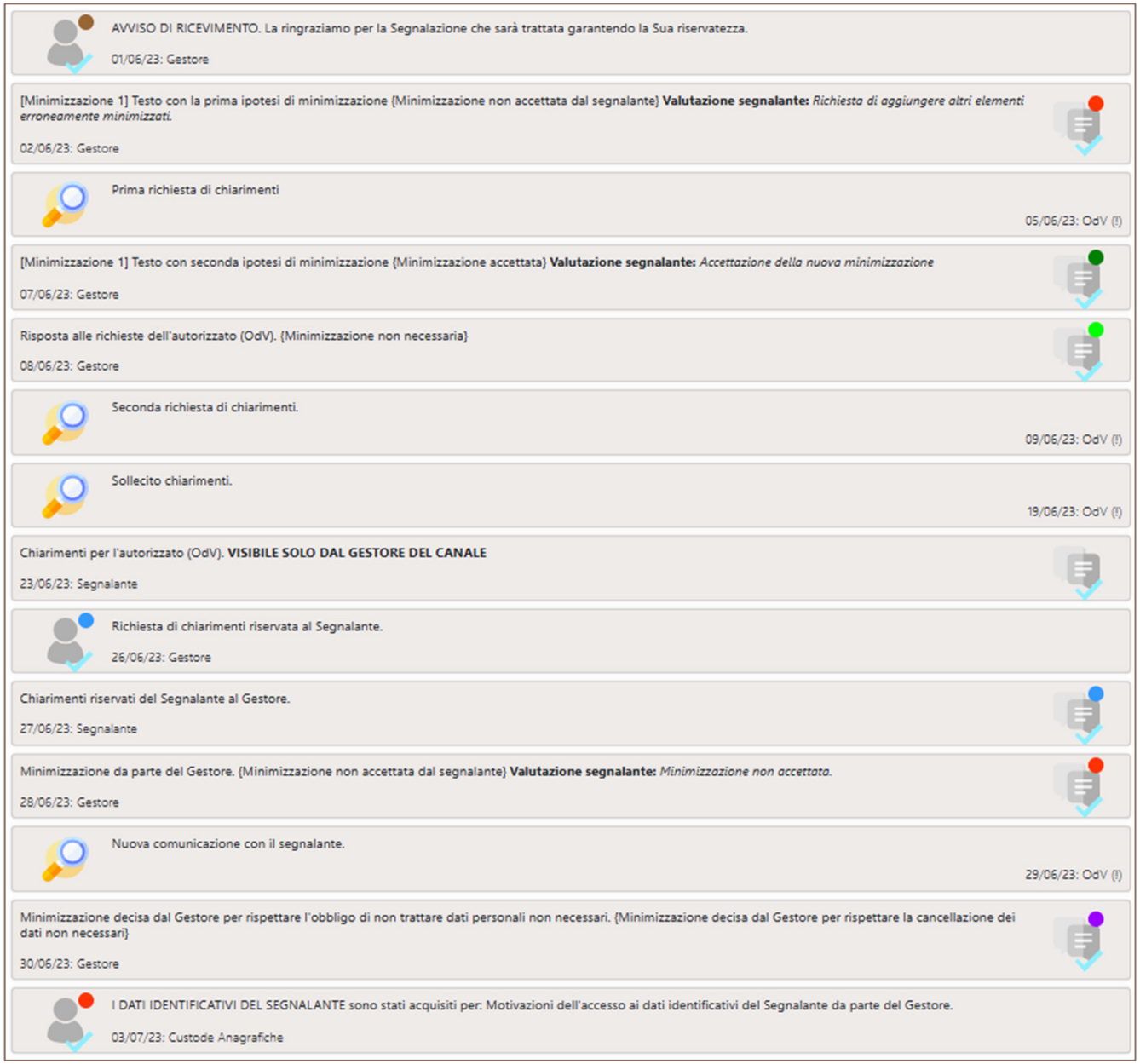


Minimizzazione accettata

Minimizzazione non accettata

Interlocuzione

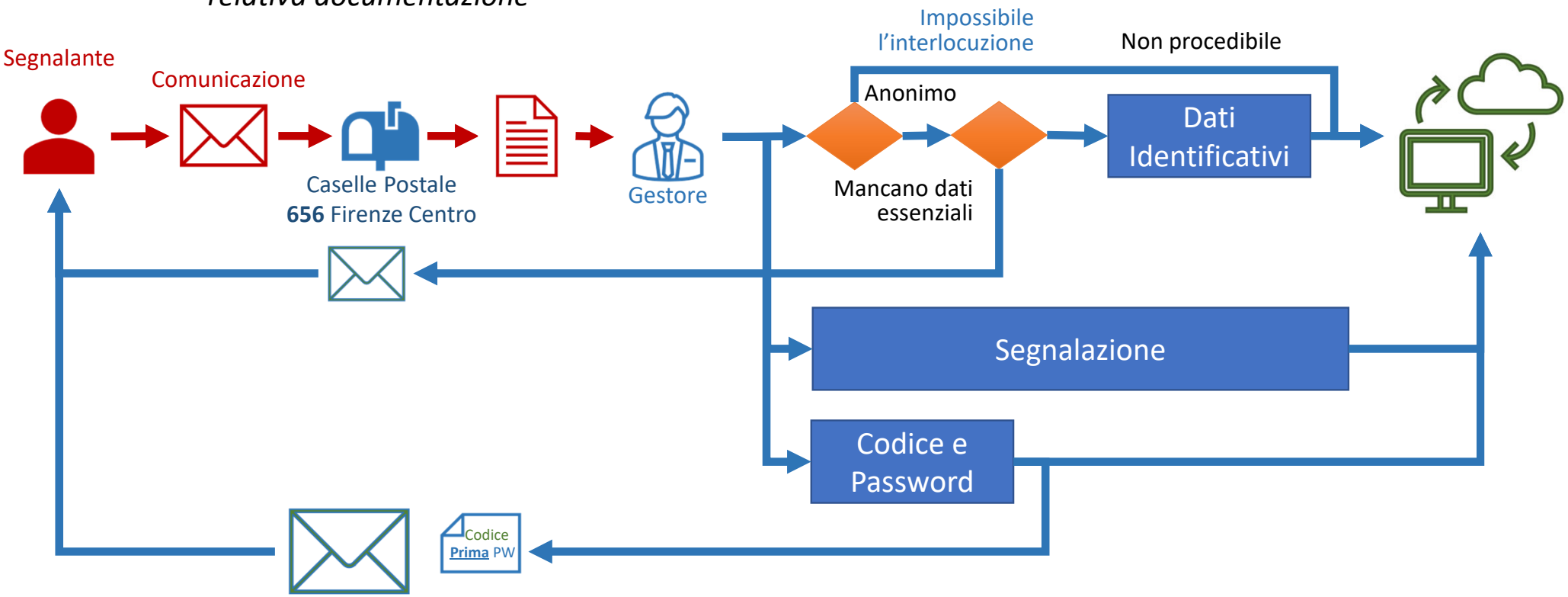
Icona	Significato
	Avviso di ricevimento della segnalazione.
	Comunicazione del Segnalante. **Visibile unicamente da Segnalante e dal Gestore.**
	Minimizzazione proposta dal Gestore.
	Minimizzazione non accettata dal Segnalante.
	Minimizzazione accettata dal Segnalante.
	Minimizzazione non necessaria.
	Minimizzazione decisa dal Gestore.
	Richieste di chiarimenti formulate dall'Istruttore/Addetto.
	Richiesta del Gestore riservata al solo Segnalante. **Visibile solo dal Segnalante e dal Gestore.**
	Risposta del Segnalante alla richiesta riservata del Gestore. **Visibile solo dal Segnalante, Gestore.**
	Informazione per il Segnalante che il Gestore ha avuto accesso ai dati identificativi.



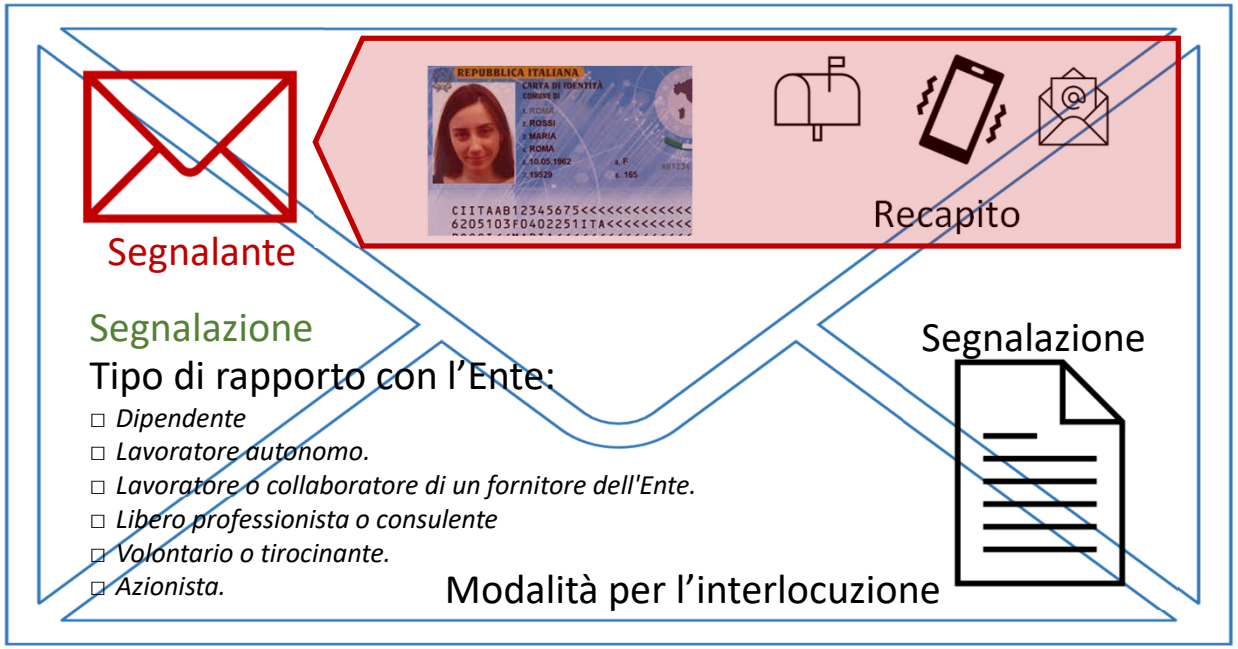
Scritto cartaceo

Forma scritta (non informatica)

Linee Guida ANAC: *[Gli Enti] sono tenuti a registrare le segnalazioni anonime ricevute e conservare la relativa documentazione*

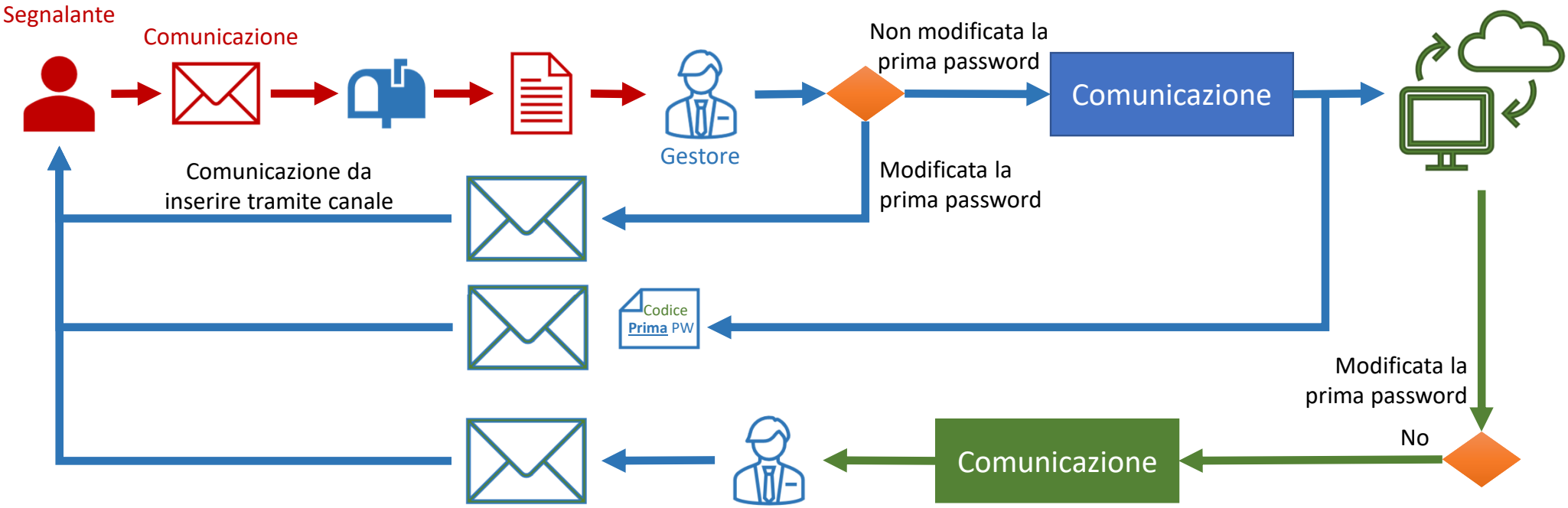


Plico per comunicazione scritta



«quando si utilizzino canali e tecniche tradizionali, occorre indicare gli strumenti previsti per garantire la riservatezza richiesta dalla normativa» [Garante privacy]

Interlocuzione scritta (non informatica)



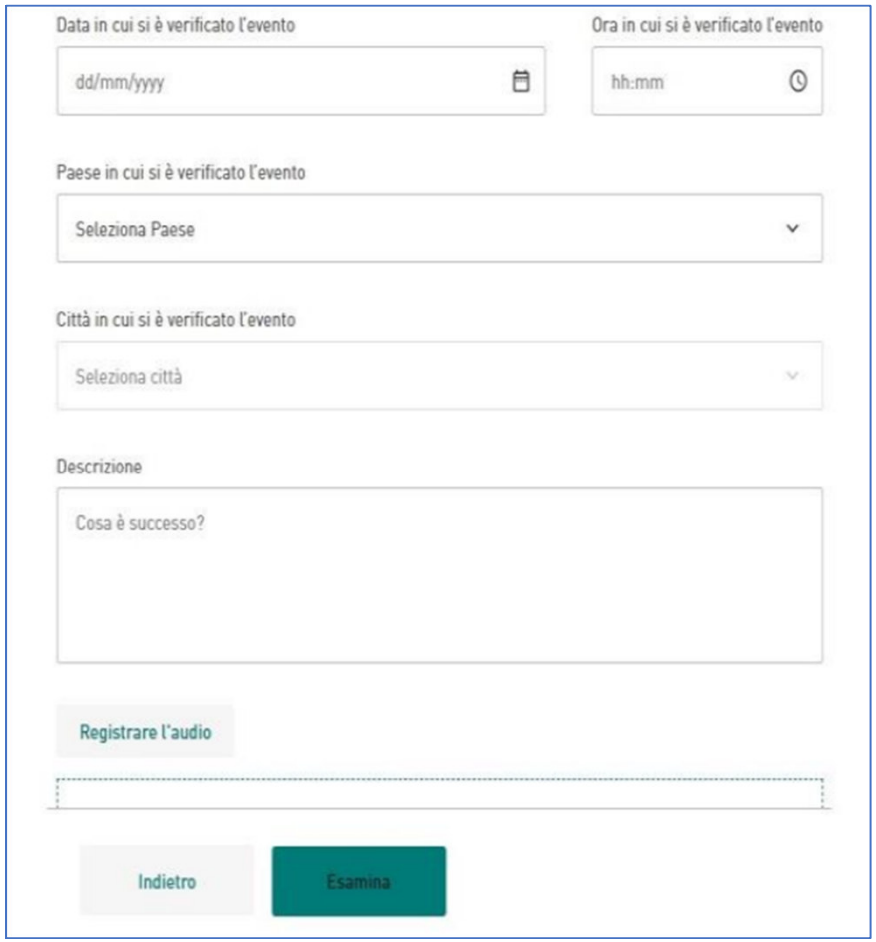
Orale

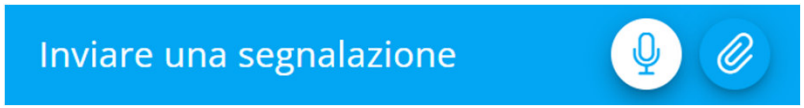
Forma orale

Le segnalazioni interne in forma orale sono effettuate attraverso linee telefoniche o sistemi di messaggistica vocale [Art. 4.3]

[Linee guida ANAC] … il legislatore ha introdotto nuove e ***ulteriori modalità*** *di presentazione della segnalazione,* ***non solo*** *per iscritto o* ***tramite piattaforma dedicata*** *ma anche oralmente, ad esempio mediante* ***linea telefonica gratuita*** *o, in alternativa, con* ***altro sistema di messaggistica vocale.***

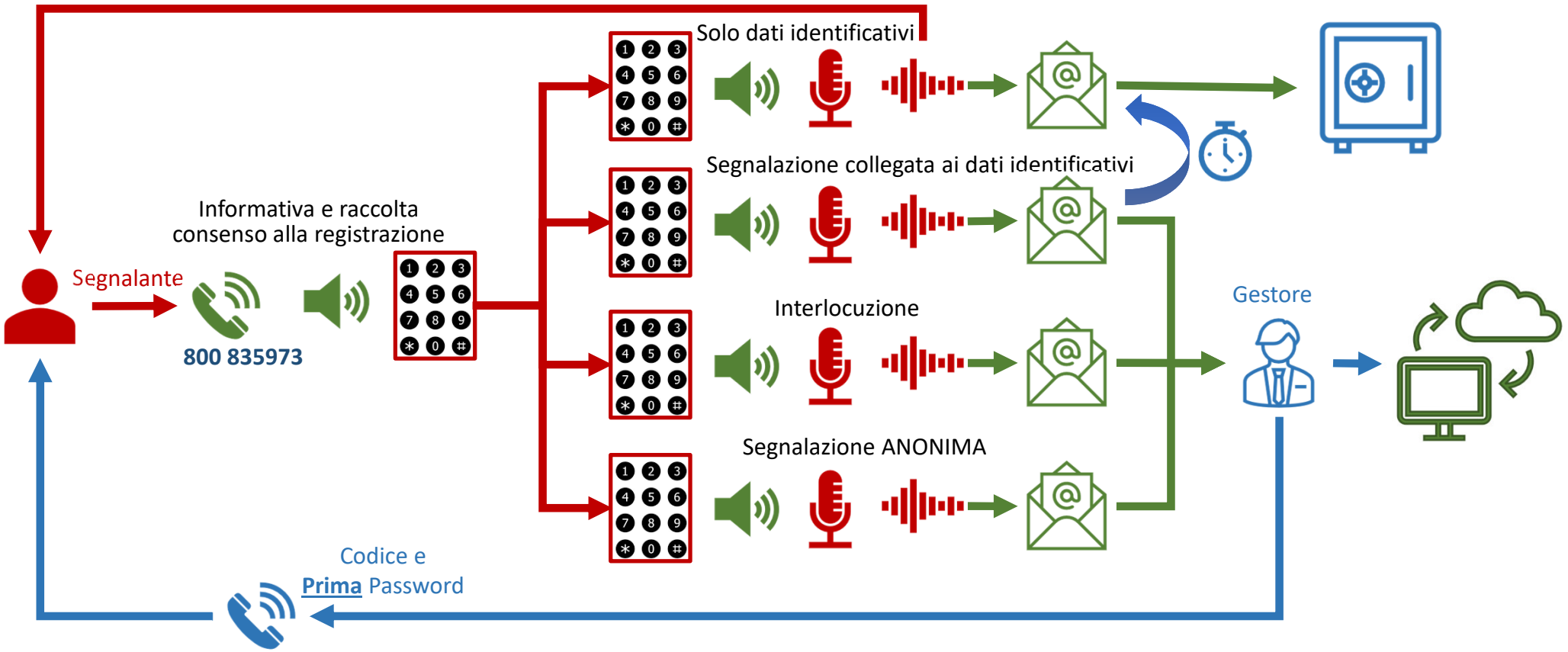
Lo scopo delle segnalazioni orali è permetterle a chi non ha possibilità di accesso al canale informatico.
Inserire un vocale all'interno del canale informatico o come allegato (dopo aver riempito tutti gli altri campi) non è una **ulteriore modalità**.



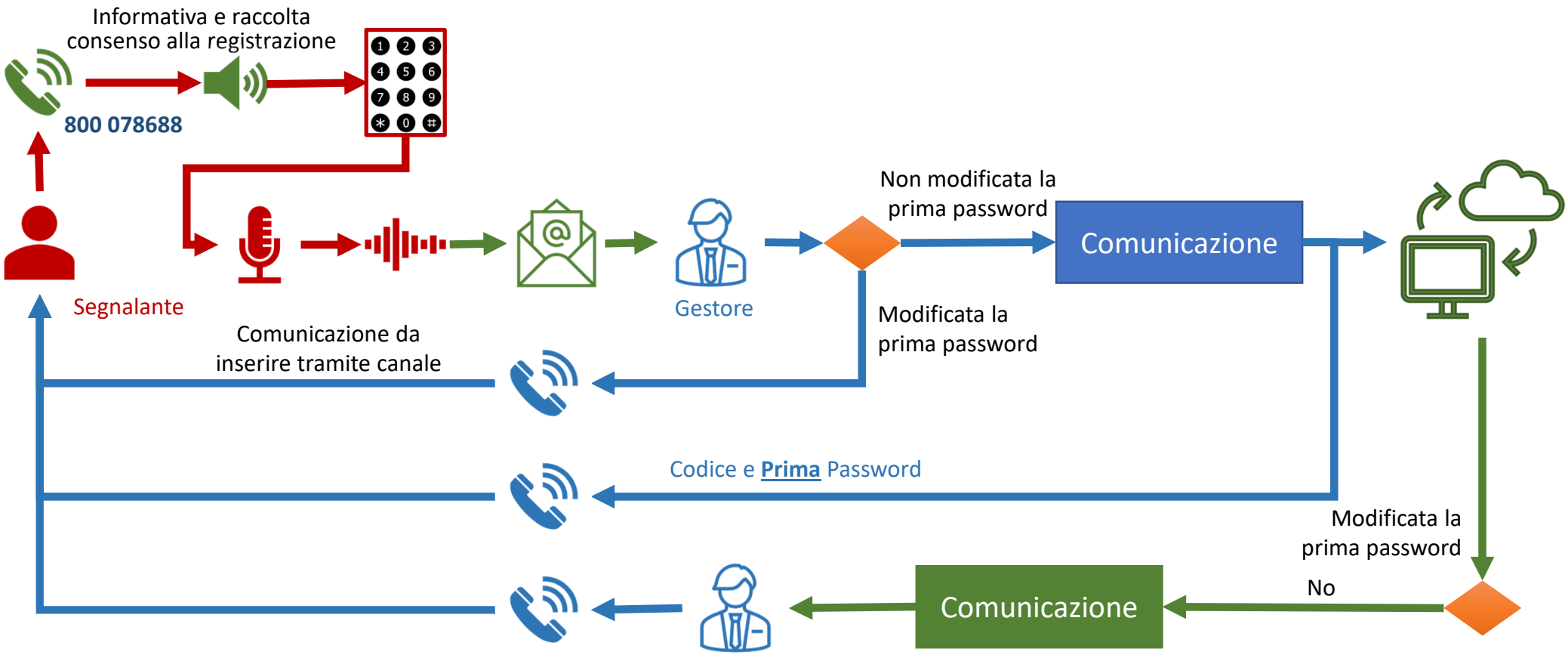


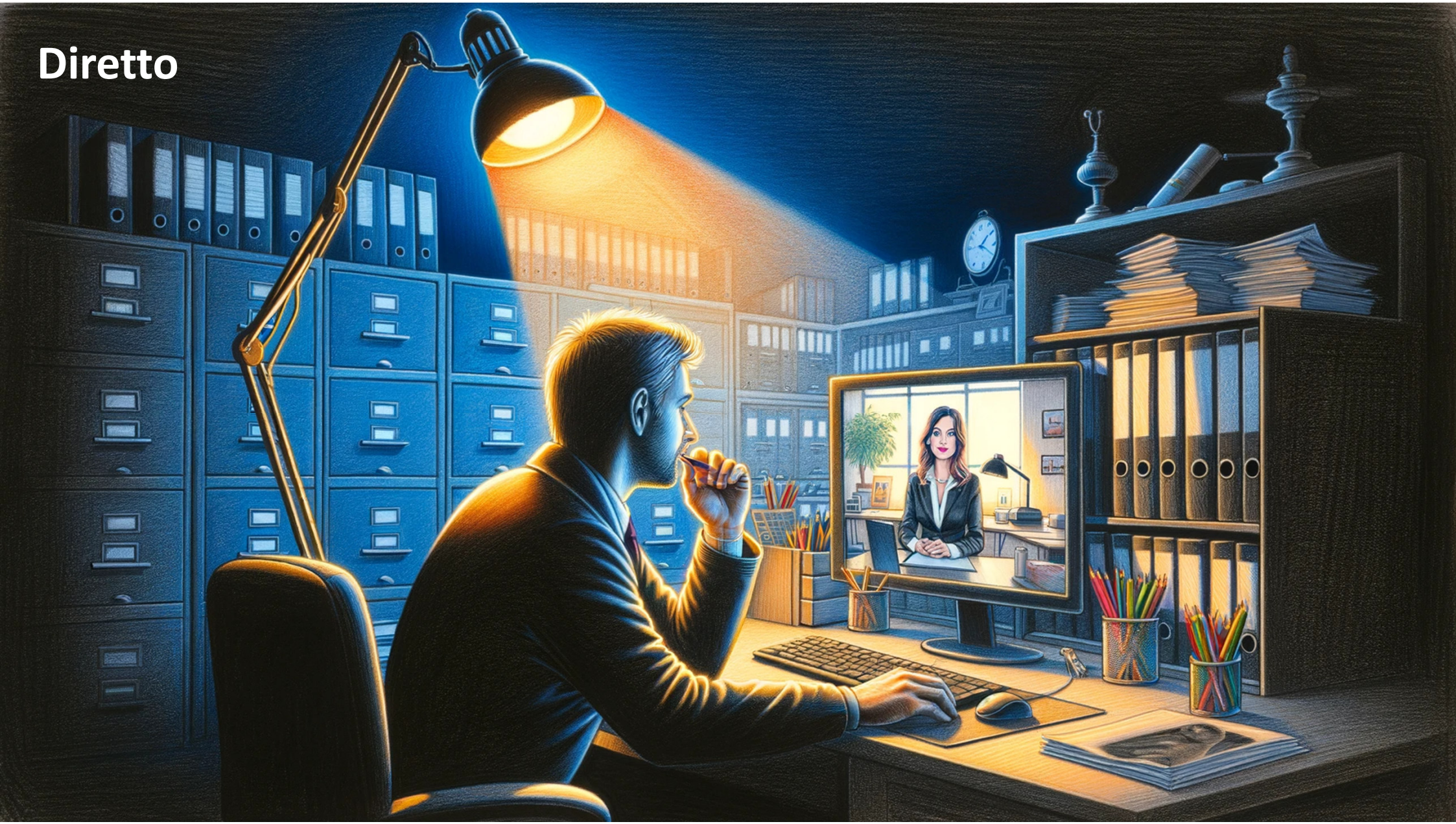
Forma orale

Linee Guida ANAC: … *segnalare oralmente mediante linea telefonica* ***gratuita*** …

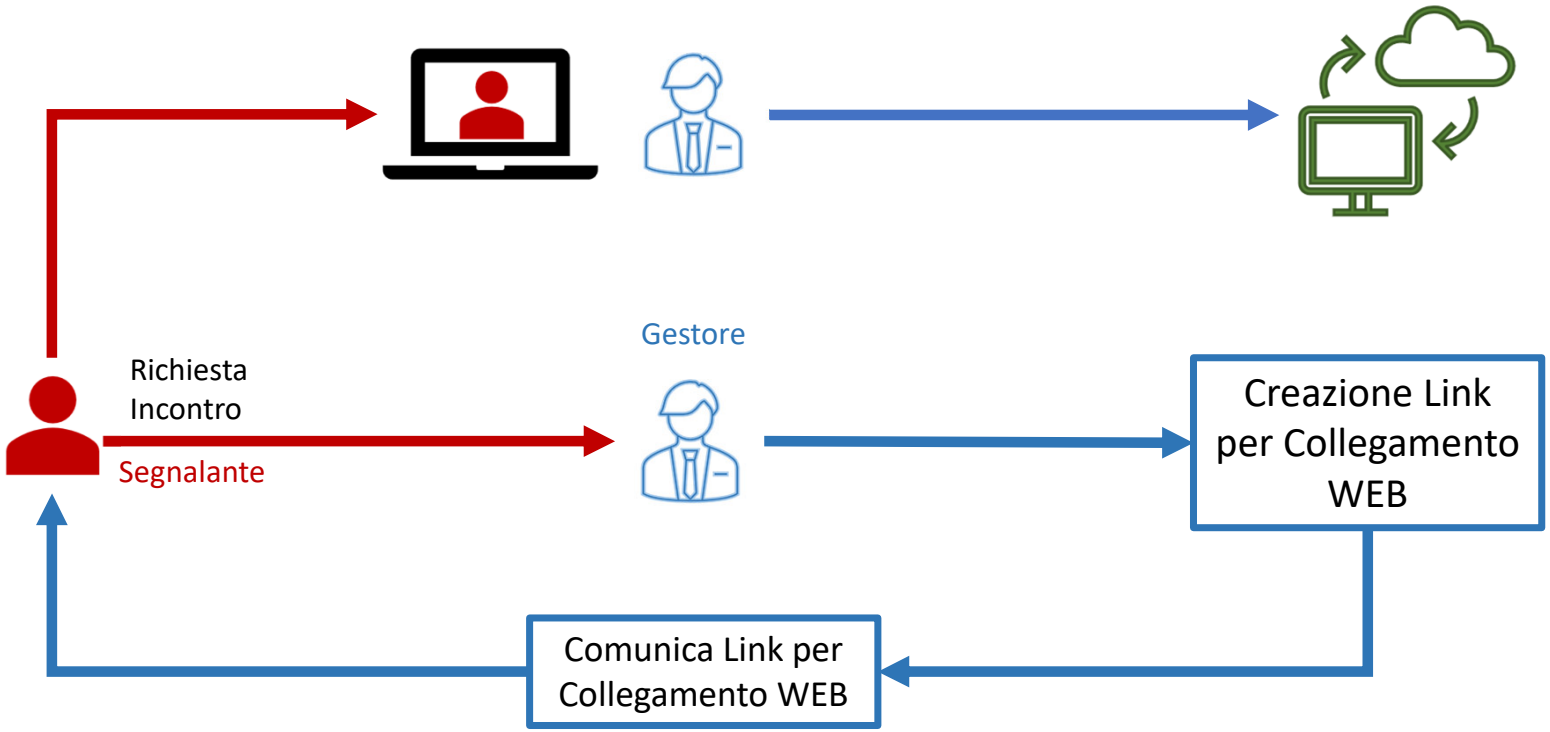


Interlocuzione in forma orale



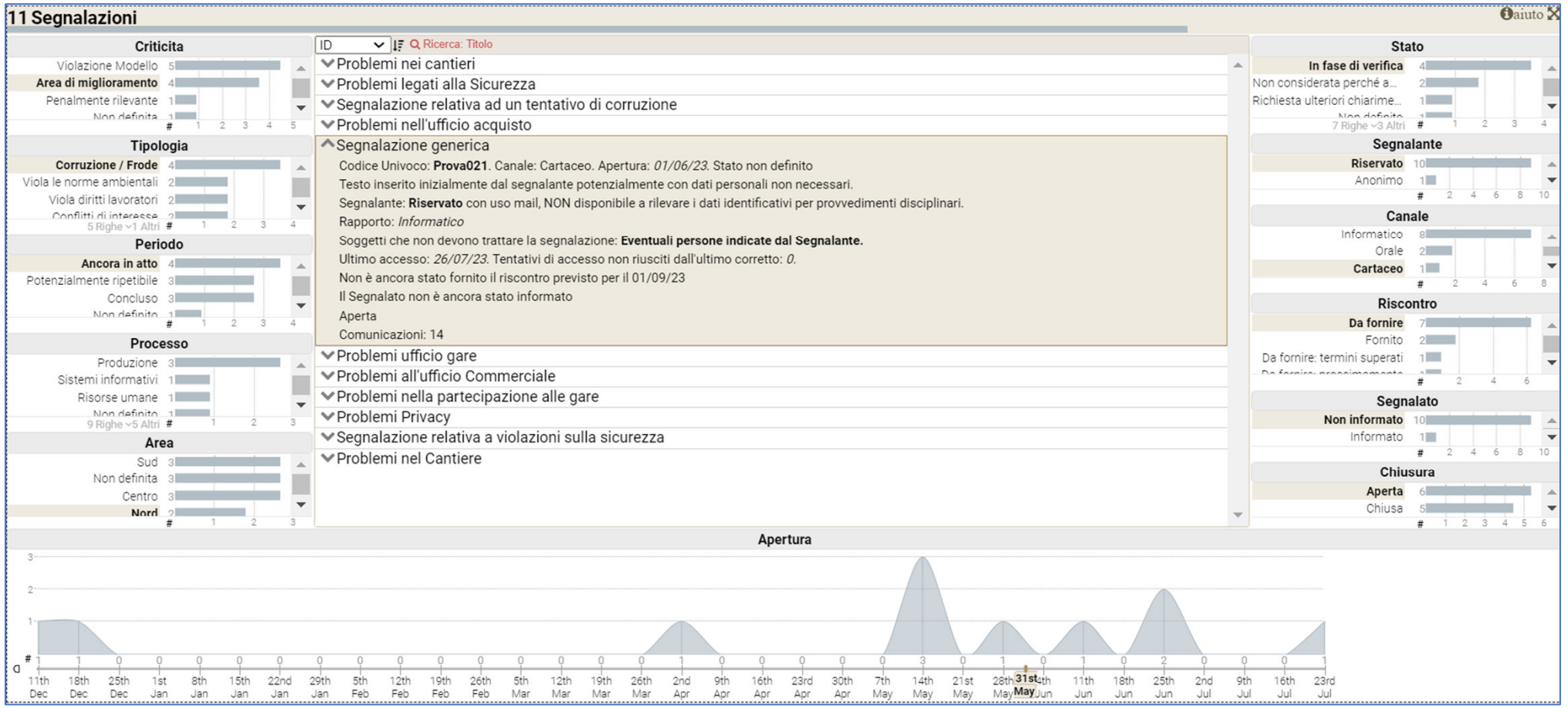

Diretto

Incontro diretto




Analisi

Analisi


11 Segnalazioni
aiuto
Criticita
Violazione Modello 5
Area di miglioramento 4
Penalmente rilevante 1
Non definita 1
Tipologia
Corruzione / Frode 4
Viola le norme ambientali 2
Viola diritti lavoratori 2
Conflitti di interesse 2
5 Righe 1 Altri
Periodo
Ancora in atto 4
Potenzialmente ripetibile 3
Concluso 3
Non definito 1
Processo
Produzione 3
Sistemi informativi 1
Risorse umane 1
Non definito 1
9 Righe 5 Altri
Area
Sud 3
Non definita 3
Centro 3
Nord 2
ID
Ricerca: Titolo
Problemi nei cantieri
Problemi legati alla Sicurezza
Segnalazione relativa ad un tentativo di corruzione
Problemi nell'ufficio acquisto
Segnalazione generica
Codice Univoco: Prova021. Canale: Cartaceo. Apertura: 01/06/23. Stato non definito
Testo inserito inizialmente dal segnalante potenzialmente con dati personali non necessari.
Segnalante: Riservato con uso mail, NON disponibile a rilevare i dati identificativi per provvedimenti disciplinari.
Rapporto: Informatico
Soggetti che non devono trattare la segnalazione: Eventuali persone indicate dal Segnalante.
Ultimo accesso: 26/07/23. Tentativi di accesso non riusciti dall'ultimo corretto: 0.
Non è ancora stato fornito il riscontro previsto per il 01/09/23
Il Segnalato non è ancora stato informato
Aperta
Comunicazioni: 14
Problemi ufficio gare
Problemi all'ufficio Commerciale
Problemi nella partecipazione alle gare
Problemi Privacy
Segnalazione relativa a violazioni sulla sicurezza
Problemi nel Cantiere
Stato
In fase di verifica 4
Non considerata perché a... 2
Richiesta ulteriori chiarime... 1
7 Righe 3 Altri
Segnalante
Riservato 10
Anonimo 1
Canale
Informatico 8
Orale 2
Cartaceo 1
Riscontro
Da fornire 7
Fornito 2
Da fornire: termini superati 1
Segnalato
Non informato 10
Informato 1
Chiusura
Aperta 6
Chiusa 5
Apertura
11th Dec
18th Dec
25th Dec
1st Jan
8th Jan
15th Jan
22nd Jan
29th Jan
5th Feb
12th Feb
19th Feb
26th Feb
5th Mar
12th Mar
19th Mar
26th Mar
2nd Apr
9th Apr
16th Apr
23rd Apr
30th Apr
7th May
14th May
21st May
28th May
31st May
4th Jun
11th Jun
18th Jun
25th Jun
2nd Jul
9th Jul
16th Jul
23rd Jul

Grazie per l’attenzione