MISURE ORGANIZZATIVE E TECNICHE POSTE IN ESSERE DAL TITOLARE DEL TRATTAMENTO

SINTESI IL510.02.04_GESTIONE DEL RISCHIO DATA PROTECTION E PIA

EDIZIONE	REDATTO	VISTATO	MODIFICHE	DATA
02	Gruppo Lavoro Data Protection	Comitato Data Protection	Aggiornamento Misure	02/11/2020
01	Gruppo Lavoro Data Protection	Comitato Data Protection	Aggiornamento Misure	20/04/2020
00	Gruppo Lavoro Data Protection	Comitato Data Protection	-	20/09/2019

Sommario

SCOPO

Il quadro giuridico europeo in materia di protezione dei dati personali è stato profondamente rinnovato dal Regolamento (UE) 2016/679 (Regolamento Generale sulla Protezione dei dati – GDPR), entrato in vigore il 24 maggio 2016 e applicabile a partire dalla data del 25 magio 2018.

Il Gruppo Policlinico, consapevole della portata innovativa del Regolamento, al fine di rafforzare ulteriormente le misure tecniche ed organizzative adottate a protezione dei dati personali trattati nell'ambito dell'attività d'impresa, all'indomani dell'entrata in vigore del Regolamento si è attivato per adeguarsi al cambiamento in corso, avviando un percorso di compliance normativa al nuovo quadro normativo in materia di data protection.

Il presente documento si pone l'obiettivo di:

- rappresentare sinteticamente le modalità di Gestione del Rischio in materia di Data Protection;
- riportare le misure di carattere organizzativo e tecnico adottate da Policlinico al fine di contenere i rischi relativi alla Data Protection;

CAMPO DI APPLICAZIONE

La presente procedura si applica alle seguenti società/organizzazioni, afferenti il Policlinico di Monza S.p.a.

- Policlinico di Monza - Monza;
- Istituto Clinico Universitario di Verano Brianza;
- Policlinico di Monza – Poliambulatori "Nievo" e "Via Modigliani";
- Policlinico di Monza – Poliambulatori "Reggio Calabria" e "Bovalino";
- Clinica San Gaudenzio di Novara;
- Clinica Santa Rita di Vercelli;
- Città di Alessandria;
- Clinica Salus di Alessandria;
- Clinica Eporediese di Ivrea;
- Clinica La Vialarda di Biella;
- U.O. di Ortopedia presso Ospedale della S.M. Misericordia di Albenga;
- Clinica Pinna Pintor di Torino;
- Doc Service – Novara;

La presente, inoltre, si riferisce a tutto il personale e ai collaboratori (liberi professionisti o altra tipologia contrattuale), di ogni ordine e grado in riferimento alle mansioni ed attribuzioni definite dall'organizzazione di propria appartenenza.

Policlinico di Monza S.p.a., nell'ambito della Gestione del Rischio in materia di Data Protection, ha posto in essere le seguenti misure di sicurezza:

1 - POLITICA PER LA SICUREZZA

L'Organizzazione ha adottato apposite Politiche in materia di Sicurezza dei dati. All'interno di tale documento è riportato non solo il modello organizzativo adottato, ma anche le misure di carattere tecnico ed organizzativo poste in essere al fine di dare adempimento alle disposizioni del regolamento, rispettare i principi e i diritti in capo agli interessati, garantire un adeguato livello di rischio per le attività di trattamento poste in essere dall'organizzazione. Le Politiche vengono aggiornate con cadenza semestrale ovvero in caso di modifiche alle attività di trattamento in essere.

2 - ORGANIZZAZIONE PER LA SICUREZZA

E' adottato un Modello Organizzativo Data Protection, approvato dal CDA che prevede la presenza di ruoli differenti con ripartizione delle responsabilità e mansioni (come da apposita Job Description).
Le figure nominate dal Titolare prevedendo compiti differenti, sintetizzabili come segue:

- **Data Manager**: Attuazione e Gestione: le figure coinvolte in queste attività danno attuazione alle decisioni aziendali e hanno cura di effettuare i trattamenti nel rispetto delle politiche/linee guida definite dal Titolare in stretto coordinamento con gli altri ruoli deputati alla Governance.
- **Referenti Data Protection**: Governo e Sorveglianza: I ruoli coinvolti in questa attività determinano il sistema di Governance applicabile ai trattamenti effettuati dall'Azienda e definiscono le linee guida e le decisioni strategiche in materia di Data Protection.
- **DPO di Gruppo**: è stato nominato un DPO di Gruppo, conformemente all'articolo 37 del Regolamento UE;
- Tutti i soggetti che trattano dati per conto del Titolare sono istruiti in tal senso e formalmente **autorizzati** per le attività di trattamento dati svolti.
- I soggetti esterni che trattano dati per conto del Titolare sono stati nominati **Responsabili al Trattamento ex art. 28** del Regolamento, rispondendo ai requisiti richiesti dal Regolamento.
- E' stato istituito un **Comitato Data Protection** di Gruppo, che si riunisce almeno semestralmente, con l'intento di verificare lo stato di compliance alle disposizioni del Regolamento.

3 - SICUREZZA DELLE RISORSE UMANE

Chiunque avvii un rapporto lavorativo/di collaborazione con il Titolare che prevede il trattamento di dati personali viene autorizzato con apposita nomina d'incarico, nell'ambito della quale viene istruito in relazione alle mansioni e comportamenti da tenere in sede dell'attività erogata.
In fase di avvio dell'attività di collaborazione viene inoltre fornito apposito Vademecum e Regolamento Data Protection.
E' previsto infine un corso di formazione obbligatorio in avvio di rapporto di lavoro, che tratta specificatamente argomenti di Protezione dati Personali ed contenuti del regolamento UE 2016/679.
E' calendarizzata annualmente formazione specifica in materia di Data Protection, destinata ai dipendenti/Collaboratori della Clinica.
E' presente apposita procedura in caso di modifica delle mansioni e cessazione del rapporto di lavoro.

4 - GESTIONE DEI BENI

E' presente apposito Inventario contenente tutti gli asset in uso presso l'organizzazione. La responsabilità della gestione dell'inventario è in capo all'Ufficio Manutenzione della Clinica.

Sono state definite e condivise con il personale apposite regole volte alla corretta restituzione da parte dei collaboratori degli asset aziendali forniti per scopi lavorativi.
E' presente apposita procedura volta al corretto trasporto e dimissione degli asset e alla corretta gestione dei supporti removibili.

5 - CONTROLLO DEGLI ACCESSI

All'interno della Clinica viene tenuto apposito Registro, contenente tutti i soggetti autorizzati al Trattamento.
Nel suddetto registro vengono segnalati in i soggetti autorizzati al trattamento (dipendenti, liberi professionisti e altri collaboratori) e i relativi trattamenti (contenuti nel registro dei trattamenti dell'organizzazione) per i quali hanno ricevuto apposita autorizzazione.
Tale strumento permette anche la corretta gestione delle utenze di directory di rete, applicative, e di altri strumenti, garantendo cosi la limitazione dell'accesso a determinate directory al personale, in base alla mansione svolta.
E' presente apposita procedura di log-in sicuro (utente + password) e apposita procedura condivisa con il personale relativa alla sicurezza delle credenziali di accesso (Password policy).

6 - CRITTOGRAFIA

Apposite politiche in relazione all'utilizzo della crittografia sono adottate per quanto concerne la trasmissione informatica di documentazione contenente dati particolari.
I dispositivi portatili di nuova introduzione sono protetti da crittografia (pc, usb, hard-disk).

7 - SICUREZZA FISICA E AMBIENTALE

L'accesso ai locali contenenti informazioni è delimitato al solo personale autorizzato e sono poste in essere specifiche misure di sicurezza fisica di accesso a tali aree (aree dove sono ubicati documenti sanitari, dispositivi elettromedicali, pc, ecc…); in particolare l'accesso ai locali CED e agli Archivi è consentito solo a personale autorizzato, le chiavi per l'accesso sono custodite da apposito soggetto autorizzato ed è necessaria firma per il ritiro e la consegna.
Sono inoltre condivise con il personale operante presso la Clinica apposite politiche di gestione della postazione di lavoro (Clear Desk e Clear Screen) .
E' presente un servizio di manutenzione interno alla Clinica che garantisce la corretta manutenzione delle apparecchiature, come da normativa cogente applicabile.
Sono garantiti gli standard di sicurezza dei luoghi e degli ambienti di lavoro come da normativa cogente applicabile e da requisiti di autorizzazione ed accreditamento (Antincendio, Sicurezza elettrica, sismica, ecc…).
Presso la sala server sono presenti:

- Sistema di monitoraggio temperatura presente in tutte le sale;
- Sistema di rilevamento incendio presente in tutte le sale server.
- Estintori CO2 presenti in tutte le sale server.
- Sistema di raffreddamento mediante condizionatori dedicati

8 - SICUREZZA DELL'OPERATIVITA'

Le procedure sono condivise con il personale ed i collaboratori mediante il Sistema Gestione Qualità ISO 9001:2015 in apposita cartella accessibile da tutti i pc.
I cambiamenti vengono autorizzati dal Titolare. Il comitato e il DPO forniscono consulenza in materia di protezione dei dati quando interpellati, in ottica "privacy by design".
La sicurezza logica viene garantita mediante i seguenti controlli:

- Anti-Malware avanzato comportamentale
- Antispam
- Backup delle informazioni
- Raccolta di log degli eventi Active Directory e Server
- Restrizioni Installazione del software sui sistemi di produzione e Client
- Gestione delle vulnerabilità tecniche (Patch Management)
- Desktop Management

9 - SICUREZZA DELLE COMUNICAZIONI

La rete privata è protetta dal Firewall ICSA Lab Certified Kerio control Firewall attivo su Client Gestito Tramite Policies + Configurazione Firewall Locale ad-hoc su tutti i server.
In fase di implementazione un Cluster Watchguard Total Security Firewall con le seguenti funzionalità:

- Intrusion Prevention;
- Reputation-Based Threat Prevention;
- URL Filtering;
- Application Control;
- Gateway Anti Virus;
- Network Discovery;
- APT Blocker;
- DNS Watch

La navigazione internet è abilitata a livello utente con profili di navigazione differenziati per categoria di utenti.
Sono poste in essere apposite politiche in relazione alle modalità di utilizzo della e-mail, per le comunicazioni, in particolare per quanto concerne i trasferimenti di categorie particolari di dati.

10 - ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI

Congiuntamente con il DPO e il Comitato Data Protection, vengono stabiliti e verificati i requisiti inerenti l'ambito data protection che il sistema deve garantire già dalla fase di progettazione (privacy-by-design quando si stabiliscono i requisiti), mediante la Valutazione d'Impatto e l'analisi del Rischio in materia Data Protection.

11 - RELAZIONI CON I FORNITORI

I rapporti con i soggetti fornitori che trattano dati per conto dell'Organizzazione sono normati mediante la nomina degli stessi quali responsabili oppure con-titolari oppure titolari autonomi del trattamento. Tale nomina avviene mediante apposito DPA a firma del Titolare e controfirmato dal fornitore in questione.

12 - GESTIONE DEGLI INCIDENTI

l'Organizzazione ha adottato apposite modalità di gestione del Data Breach, traendo spunto dalla procedura proposta dal WP 29, e contenute nella procedura.
la Procedura prevede i ruoli per il personale: a chi segnalare l'incidente, chi lo tratta e come gestire il data breach.
Le modalità di valutazione della gravità dell'incidente sono adottate partendo dalle linee guida del WP29 e di ENISA.
La procedura prevede inoltre la compilazione del Registro Data Breach e l'analisi delle cause profonde che hanno portato all'evento avverso in materia di Data Protection.

13 - CONTINUITA' OPERATIVA

Presente sistema di backup in grado di ripristinare l'intera infrastruttura server a seguito di guasto.
L'attuale sistema di backup esegue tale attività nelle ore notturne, ed in caso di guasto viene ripristinato lo stato del giorno precedente. Gli applicativi contenenti categorie particolari di dati prevedono il ripristino del DB allo stato di 30 minuti prima del guasto.
La nuova infrastruttura in fase di implementazione è costituita da un cluster Nutanix primario accoppiato con un cluster di disaster recovery. Il backup dell'intera infrastruttura avviene in maniera continua secondo una schedulazione differenziata per categoria di server. Per i server ERP il backup con replica su sito di DR avviene ogni 2 ore.

14 - CONFORMITA' ALLE PRESCRIZIONI

Il DPO di Gruppo ed il Comitato svolgono audit presso l'organizzazione partendo da apposito modello di verbale, almeno con cadenza annuale.
E' previsto apposito verbale di audit, che viene fornito all'organizzazione dopo aver proceduto allo svolgimento dello stesso.
Sono presenti indicatori di risultato aventi ad oggetto l'ambito privacy (customer satisfaction) volti a garantire un monitoraggio continuo.

15 - PRINCIPI, DIRITTI E DISPOSIZIONI GDPR

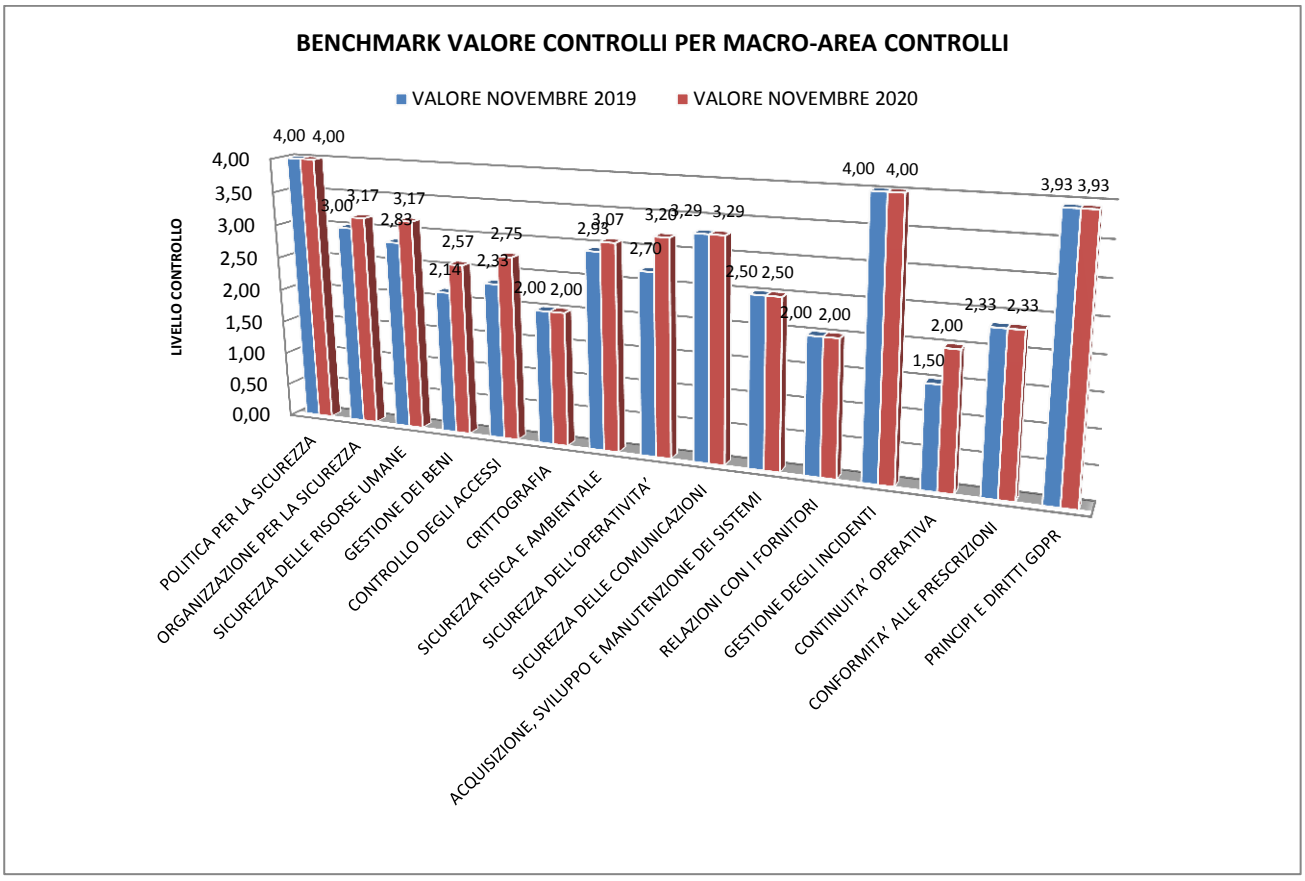
E' presente apposita procedura volta a dar seguito ad eventuali richieste di esercizio di diritto da parte dell'interessato (con contestuale aggiornamento del registro richieste interessati).
Viene fornita apposita informativa al paziente che afferisce alla Clinica, aggiornata alla luce delle disposizioni del regolamento. L'informativa è inoltre visionabile sul sito internet, posizionata ed affissa in tutte le aree prenotazione/accettazione.
E' presente apposito registro delle attività di trattamento, redatto ed aggiornato come da art. 30 del Regolamento.
Ai sensi dell'art. 32 sono poste in essere apposite modalità di gestione del rischio in ambito data protection, che prevede la valutazione d'impatto come da art. 35 del regolamento e da successivo provvedimento dell'Autorità Garante.
I tempi di conservazione della documentazione è definito dal Titolare sulla base del massimario di scarto Regione Lombardia.

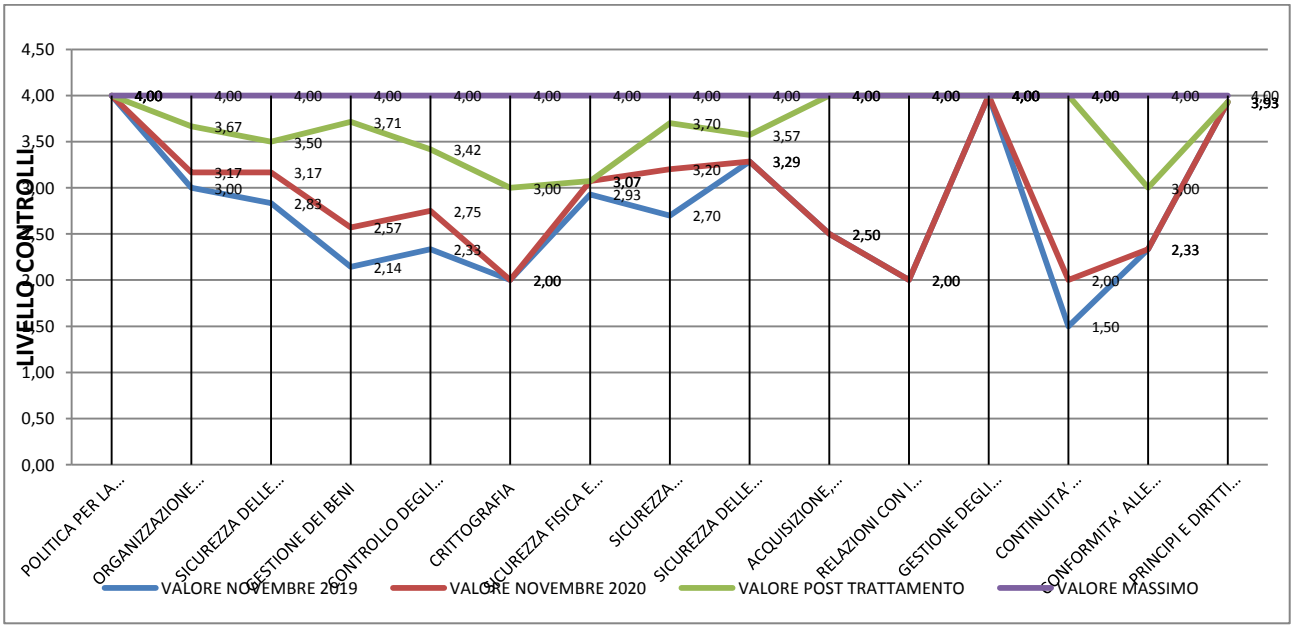
RAPPRESENTAZIONE GRAFICA ANDAMENTO PROGETTO DI COMPLIANCE AL REGOLAMENTO UE 2016/679

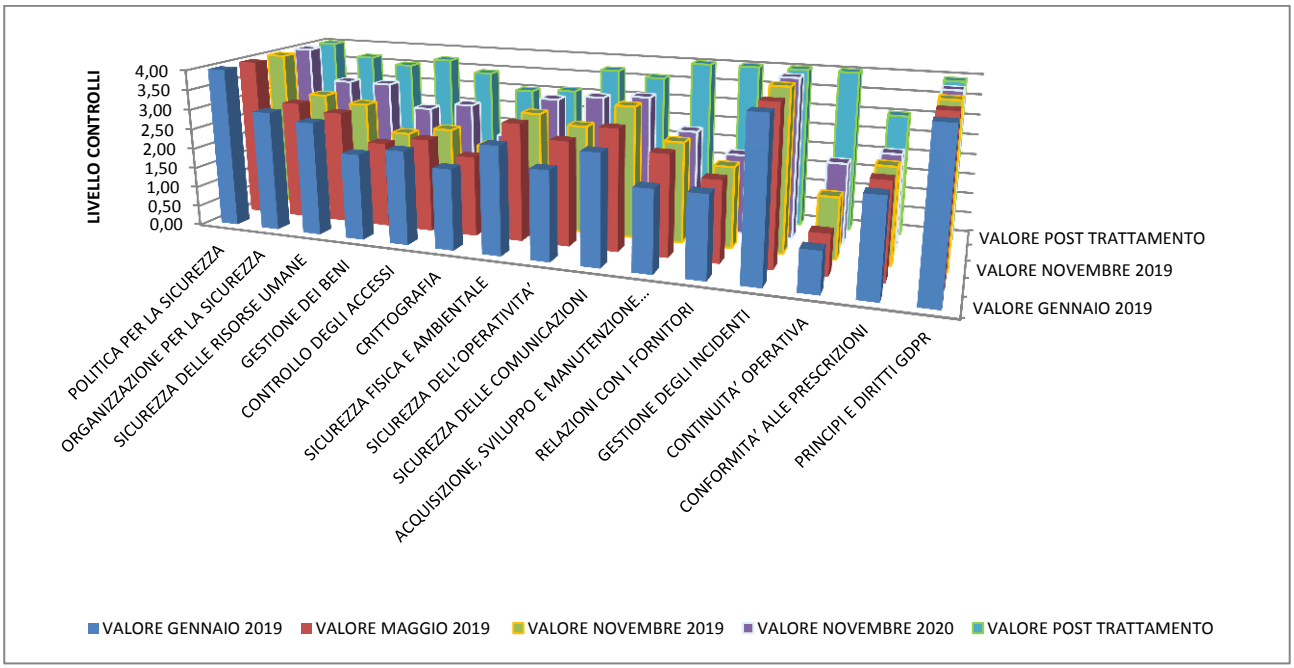
La presente sezione riporta lo stato dell'arte in merito all'andamento del progetto di compliance posto in essere a partire da Maggio 2018 da parte di Policlinico di Monza S.p.a.

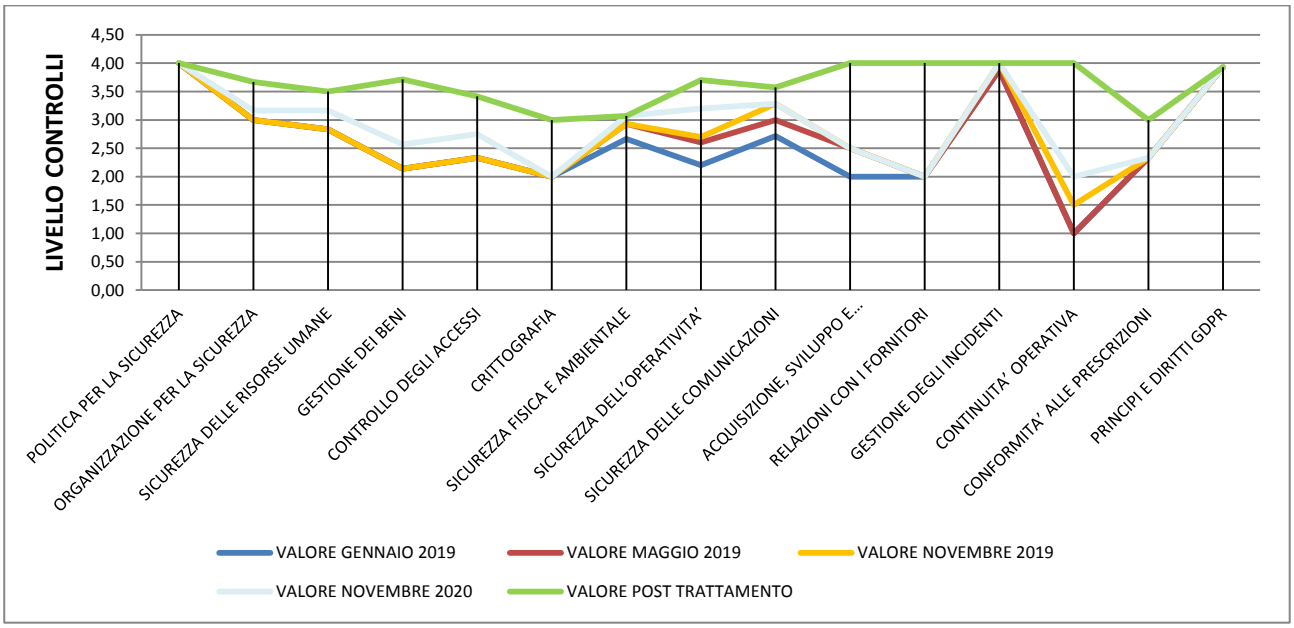
Dall'analisi dei grafici di seguito riportati, si evidenzia il continuo miglioramento in termini di sicurezza delle informazioni e dei dati trattati, grazie all'implementazione continua di misure di carattere tecnico ed organizzativo, come disposto dall'art. 32 del Regolamento UE 2016/679.

Le misure riportate nei grafici sono raggruppate per macro-aree come da paragrafi precedenti.


BENCHMARK VALORE CONTROLLI PER MACRO-AREA CONTROLLI
VALORE NOVEMBRE 2019
VALORE NOVEMBRE 2020
LIVELLO CONTROLLO
4,00 4,00
3,00 3,17
2,83 3,17
2,57 2,75
2,14 2,33
2,00 2,00
2,93 3,07
2,70 3,20
3,29 3,29
2,50 2,50
2,00 2,00
4,00 4,00
1,50 2,00
2,33 2,33
3,93 3,93
POLITICA PER LA SICUREZZA
ORGANIZZAZIONE PER LA SICUREZZA
SICUREZZA DELLE RISORSE UMANE
GESTIONE DEI BENI
CONTROLLO DEGLI ACCESSI
CRITTOGRAFIA
SICUREZZA FISICA E AMBIENTALE
SICUREZZA DELL'OPERATIVITA'
SICUREZZA DELLE COMUNICAZIONI
ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI
RELAZIONI CON I FORNITORI
GESTIONE DEGLI INCIDENTI
CONTINUITA' OPERATIVA
CONFORMITA' ALLE PRESCRIZIONI
PRINCIPI E DIRITTI GDPR


LIVELLO CONTROLLI
VALORE NOVEMBRE 2019
VALORE NOVEMBRE 2020
VALORE POST TRATTAMENTO
VALORE MASSIMO


LIVELLO CONTROLLI
4,00
3,50
3,00
2,50
2,00
1,50
1,00
0,50
0,00
POLITICA PER LA SICUREZZA
ORGANIZZAZIONE PER LA SICUREZZA
SICUREZZA DELLE RISORSE UMANE
GESTIONE DEI BENI
CONTROLLO DEGLI ACCESSI
CRITTOGRAFIA
SICUREZZA FISICA E AMBIENTALE
SICUREZZA DELL'OPERATIVITA'
SICUREZZA DELLE COMUNICAZIONI
ACQUISIZIONE, SVILUPPO E MANUTENZIONE...
RELAZIONI CON I FORNITORI
GESTIONE DEGLI INCIDENTI
CONTINUITA' OPERATIVA
CONFORMITA' ALLE PRESCRIZIONI
PRINCIPI E DIRITTI GDPR
VALORE POST TRATTAMENTO
VALORE NOVEMBRE 2019
VALORE GENNAIO 2019
VALORE GENNAIO 2019
VALORE MAGGIO 2019
VALORE NOVEMBRE 2019
VALORE NOVEMBRE 2020
VALORE POST TRATTAMENTO


LIVELLO CONTROLLI
4,50
4,00
3,50
3,00
2,50
2,00
1,50
1,00
0,50
0,00
POLITICA PER LA SICUREZZA
ORGANIZZAZIONE PER LA SICUREZZA
SICUREZZA DELLE RISORSE UMANE
GESTIONE DEI BENI
CONTROLLO DEGLI ACCESSI
CRITTOGRAFIA
SICUREZZA FISICA E AMBIENTALE
SICUREZZA DELL'OPERATIVITA'
SICUREZZA DELLE COMUNICAZIONI
ACQUISIZIONE, SVILUPPO E...
RELAZIONI CON I FORNITORI
GESTIONE DEGLI INCIDENTI
CONTINUITA' OPERATIVA
CONFORMITA' ALLE PRESCRIZIONI
PRINCIPI E DIRITTI GDPR
VALORE GENNAIO 2019
VALORE MAGGIO 2019
VALORE NOVEMBRE 2019
VALORE NOVEMBRE 2020
VALORE POST TRATTAMENTO