Codice A1000A
D.D. 11 ottobre 2021, n. 555
Audit Privacy 2021- Attuazione del piano triennale 2019-2020 - DGR n. 1-387 del 18 ottobre 2019, ''Regolamento Ue 2016/679 D.lgs. 196/2003. Approvazione Piano Triennale di Audit Privacy 2019-2021''.

ATTO DD 555/A1000A/2021 DEL 11/10/2021

DETERMINAZIONE DIRIGENZIALE
A1000A - DIREZIONE DELLA GIUNTA REGIONALE

OGGETTO: Audit Privacy 2021- Attuazione del piano triennale 2019-2020 - DGR n. 1-387 del 18 ottobre 2019, "Regolamento Ue 2016/679 D.lgs. 196/2003. Approvazione Piano Triennale di Audit Privacy 2019-2021".

La Regione Piemonte, con DGR n. 1-387 del 18 ottobre 2019, ha approvato il Piano triennale di Audit Privacy 2019-2021. Detto piano individua talune azioni volte a rafforzare il "sistema privacy" della Giunta regionale nell'ambito dell'"AUDIT SULLA CONFORMITA' ALLA NORMATIVA PRIVACY (GDPR 2016/679)", quali:
1) Rappresentazione dell'organigramma "sistema privacy", che evidenzia le figure previste dal Regolamento europeo;
2) Mappatura e aggiornamento dei trattamenti, da parte dei referenti privacy come da DGR n. 1-192del 9 agosto 2019, con validazione da parte dei Delegati;
3) Valutazione di impatto per tutti i trattamenti per cui è obbligatorio per legge effettuarla in ambito regionale, da parte dei referenti privacy, previa validazione da parte dei Delegati, come da DGR n. 1-192 del 9 agosto 2019;
4) Verifica della valutazione di impatto dei trattamenti ad alto rischio effettuata dalle strutture regionali, su un campione selezionato;
5) Audit di conformità, dell'adeguamento alla normativa GDPR, sugli atti di nomina a responsabile esterno del trattamento, su un campione selezionato;
4) Audit sull'adeguamento delle misure di sicurezza e applicazione della normativa GDPR nei confronti dei responsabili esterni del trattamento, su un campione selezionato;
5) Audit sulla sicurezza informatica delle misure adottate dalla Direzione Segretariato in quanto responsabile dei sistemi informativi;
6) Diffusione della cultura dell'Audit privacy;
7) Interventi urgenti di Audit privacy.
L'Audit privacy si inserisce nella policy di Audit che la Regione ha avviato a partire dal 2012 istituendo, con D.G.R. n. 31-4009 dell'11 giugno 2012, il Settore "Audit Interno" ed è diretta alla verifica di conformità dell'azione dell'amministrazione regionale alla vigente disciplina sul trattamento dei dati personali con particolare riferimento ai processi, agli strumenti ed alle modalità che assicurano la riservatezza, integrità e disponibilità dei dati e dei trattamenti.
Il presupposto giuridico dell'Audit privacy è rinvenibile nei Considerando del Regolamento UE 2016/679 (GDPR), dal 74 al 79, i quali, in particolare, stabiliscono che:

- *il titolare deve mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche* (cit. Considerando 74).
- *La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento (78)* .

In sintesi, quindi, i "Titolari dei dati", a mente della succitata disciplina, devono essere in grado di dimostrare la conformità delle attività di trattamento dell'Ente al Regolamento europeo. Nel contempo sono tenuti ad adottare le misure tecniche e organizzative adeguate a protezione dei dati personali che tengano conto della ripartizione delle responsabilità al loro interno e rispetto alle strutture esterne a cui sono affidate o con cui si condividono particolari attività.
L'Audit privacy, curata dal DPO con il supporto dei referenti privacy, individuati formalmente da ciascuna Direzione consente altresì, al Titolare, di individuare le aree di rischio su cui occorre agire attraverso misure adeguate per minimizzare i rischi.
L'Audit privacy 2020 ha avuto carattere ricognitivo e preliminare, volto a fotografare il rispetto degli adempimenti prescritti dal Regolamento europeo e dal Codice per la protezione dei dati, come modificato dal D.Lgs. 101/2018, sia a livello generale sia a livello delle singole Direzioni e articolazioni dell'Ente anche attraverso la mappatura dello stato delle misure adottate. La ricognizione ha riguardato l'attività documentale/provvedimentale nonché gli adempimenti organizzativi adottati successivamente all'entrata in vigore del GDPR, e, segnatamente:
a) la ricognizione dei provvedimenti e atti del Titolare;
b) la predisposizione di un questionario alle Direzioni;
c) la ricognizione dei sistemi informativi;
d) la ricognizione del sistema di videosorveglianza.
L'Audit 2020 si è concluso con una relazione generale e l'invio delle osservazioni alle singole Direzioni.

Il registro dei trattamenti

L'art. 30 del GDPR prevede, tra gli adempimenti principali in capo al Titolare, la tenuta del Registro delle attività di trattamento. Si tratta di un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare e dai responsabili del trattamento e costituisce nel contempo uno dei principali elementi di accountability in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno dell'Ente, indispensabile per ogni attività di valutazione o analisi del rischio e, dunque, preliminare rispetto a tali attività.
E' un importante strumento di censimento e analisi dei trattamenti effettuati dal Titolare e deve essere costantemente aggiornato in quanto il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.
Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento.
In particolare:
- Nel campo "**finalità del trattamento**" (*i dati personali sono raccolti per finalità determinate, esplicite e legittime*), occorre esplicare le finalità distinte per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini,...);
- Nel campo "**basi giuridiche che legittimano il trattamento**" occorre precisare la/le condizioni che legittimano il trattamento (es. adempimento di un obbligo legale del Titolare, consenso libero

e informato, esecuzione di un compito di interesse pubblico, esecuzione di un contratto di cui l'interessato è parte, salvaguardia degli interessi vitali dell'interessato, salvaguardia di un'altra persona fisica, trattamento necessario per il perseguimento di un legittimo interesse del Titolare (art. 6 GDPR);

- Nel campo "**riferimenti normativi e legittimi interessi", occorre indicare la base normativa del trattamento;**
- **Nel campo "origine dei dati", occorre indicare se i dati oggetto del trattamento sono stati raccolti presso l'interessato o comunicati da terzi;**
- **Nel campo "tipo di banca dati", occorre indicare se il trattamento avviene in forma cartacea o automatizzata;**
- Nel campo "**categorie di dati**", vanno specificate le tipologie di dati oggetto di trattamento (es. dati personali, dati particolari oppure reati e condanne penali);
- Nel campo "**categorie di interessati", occorre indicare q**ualsiasi persona fisica identificata o identificabile a cui si riferiscono i dati ;
- Nel campo **"titolari selezionati" occorrerà indicare la p**ersona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- Nel campo "r**esponsabili del trattamento", occorre indicare la p**ersona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- Nel campo "**trasferimenti e comunicazioni**", vanno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari a cui sono comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi); dovranno inoltre essere indicati gli eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- Nel campo "**misure di sicurezza**", sarà possibile selezionare le misure tecniche trasversali e le misure di sicurezza organizzative;
- Nel campo "**periodo di conservazione dei dati", occorre indicare i**l periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.

La Regione Piemonte, avvalendosi del CSI Piemonte, si è dotata di un applicativo web denominato "Data protection manager (DPM)" che consente sia il popolamento del registro dei trattamenti, sia la gestione delle valutazioni d'impatto. Il registro dei trattamenti, allo stato attuale, è composto da 701 trattamenti, suddivisi per Direzione i cui trattamenti sono stati validati dalle relative Direzioni.
L'Audit 2021 consiste nella verifica a campione di un numero pari a 20 trattamenti estratti con metodo casuale dal registro.
Gli elenchi dei trattamenti sono stati estratti mediante una generazione di un foglio Excel dell'applicativo Microsoft Excel DATI/STATISTICHE/CAMPIONAMENTO, impostando come dimensione del campionamento i numeri da 1 a 20, completo di tutti i 701 trattamenti inseriti dalle Direzioni nel Registro dei trattamenti (DPM) (vedi Verbale estrazione campione di trattamenti da sottoporre a controllo del 12 luglio 2021 – Allegato A).
Il controllo dei trattamenti prevede una verifica della completezza della compilazione dei campi previsti dal DPM con particolare riferimento ai seguenti adempimenti:

- **finalità del trattamento;**
- **basi giuridiche che legittimano il trattamento;**
- r**iferimenti normativi e legittimi interessi;**
- **origine dei dati;**
- **tipo di banca dati;**
- **categorie di dati;**
- **categorie di interessati;**
- **titolari selezionati;**

- **responsabili del trattamento;**
- **trasferimenti e comunicazioni;**
- **misure di sicurezza;**
- **periodo di conservazione dei dati;**
- **una verifica sulla correttezza della compilazione.**

Nel caso di trattamento che possa comportare *"un rischio elevato per i diritti e le libertà delle persone"***, (ad esempio, quando si prevede di avviare un trattamento mediante** *"utilizzo di nuove tecnologie, avuto riguardo alla natura, all'oggetto, al contesto e alle finalità del trattamento")* **la verifica concerne, ai sensi dell'articolo 35 primo comma del GDPR, la previa valutazione dell'impatto dei trattamenti.**

Sui trattamenti estratti saranno effettuati controlli di Audit esterno su eventuali responsabili del trattamento ex art. 28 GDPR.

IL DIRETTORE

Richiamati i seguenti riferimenti normativi:

- Regolamento UE 2016/679;
- Deliberazione Giunta Regionale 18/05/2018 , n. 1 - 6847;
- Deliberazione Giunta Regionale 28/09/2018 , n. 1 - 7574;
- Deliberazione Giunta Regionale 18/10/2019 , n. 1 - 387;
- Deliberazione Giunta Regionale 09/08/2019 , n. 1 - 192;
- Deliberazione Giunta Regionale 27/08/2020, n. 19 - 1177;

determina

determina

di approvare, nell'ambito delle attività di Audit privacy per l'anno 2021, in attuazione del piano triennale Audit Privacy 2019-2020 di cui alla DGR n. 1-387 del 18 ottobre 2019, la sopra descritta modalità di esecuzione – Audit registro dei trattamenti - e nel contempo di approvare i seguenti Allegati, parte integrante della presente determinazione:

- Allegato A - Verbale estrazione campione di trattamenti da sottoporre a controllo;
- Allegato B - Check-list di controllo dei trattamenti;
- Allegato C - Check-list di controllo responsabili esterni ex art. 28 GDPR;
- Allegato D – Elenco trattamenti estratti.

IL DIRETTORE (A1000A - DIREZIONE DELLA GIUNTA REGIONALE)
Firmato digitalmente da Paolo Frascisco

Allegato

ALLEGATO A

VERBALE

DI ESTRAZIONE DELL'ELENCO DEI TRATTAMENTI ESTRATTI DAL REGISTRO DEI TRATTAMENTI (DPM) RELATIVO ALL'AUDIT PRIVACY 2021.

Il 12 luglio 2021, alle ore 14.00 si è tenuta la prima seduta di estrazione dei trattamenti del Registro dei trattamenti (DPM), presso la sede di piazza Castello 165, Torino piano 3A.

Sono presenti la dott.ssa Annamaria Cucurachi funzionaria in staff della Direzione della Giunta regionale, nonché la dott.ssa Elisa Valesio funzionaria in staff della Direzione della Giunta regionale.

Gli elenchi dei trattamenti sono stati estratti mediante una generazione di un foglio Excel completo di tutti i 701 trattamenti inseriti dalle Direzioni nel Registro dei trattamenti (DPM).

La prima colonna (A) è stata numerata da 1 a 701.

Ai fini dell'estrazione del campione di atti da sottoporre a controllo si è utilizzata la funzione dell'applicativo Microsoft Excel DATI/STATISTICHE/CAMPIONAMENTO con metodo casuale, impostando come dimensione del campionamento i numeri da 1 a 20.

Dato il permanere della situazione di Emergenza legata all'epidemia da Covid-19 si è deciso di effettuare un Audit a distanza, senza il coinvolgimento delle Direzioni in presenza.

Tutto ciò premesso e considerato, si riportano gli esiti delle estrazioni effettuate e il metodo utilizzato per l'elenco allegato.

Trattamenti

L'elenco comprende n. 701 trattamenti inseriti nell'applicativo DPM al 21 luglio 2021. In esito all'operazione automatica di campionamento, sopra descritta, sono stati estratti n. 20 trattamenti con i numeri indicati in calce all'elenco (v. Allegato C) e automaticamente collocati in ordine crescente, come di seguito riportato: N. 36; N. 43; N. 69; N. 120; N. 148; N. 151; N. 153; N. 187; N. 244; N. 264; N. 266; N. 283; N. 330; N. 494; N. 511; N. 526; N. 582; N. 605; N. 637; N. 671.

La seduta si è chiusa alle ore 14.57.

Le funzionarie:

dott.ssa Annamaria Cucurachi;

dott.ssa Elisa Valesio (verbalizzante).

ALLEGATO B

Checklist Audit 2021. Registro dei Trattamenti DPM.

Il Regolamento UE 2016/679 (di seguito GDPR), all'articolo 30, individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento. L'articolo 35 del GDPR prevede i casi in cui è d'obbligo effettuare la valutazione d'impatto.

Compilazione del trattamento in DPM

DESCRIZIONE TRATTAMENTO

DOMANDE	SI	NO	NON APPLICABILE	NOTE
1) Sono individuate le finalità del trattamento?				
2) E' individuata la base giuridica che legittima il trattamento?				
3) Sono indicati i riferimenti normativi e legittimi interessi?				
4) E' indicata l'origine dei dati?				
5) E' indicato il tipo di banca dati?				
6) Sono indicate le categorie di dati oggetto del trattamento?				
7) Sono indicate le categorie di interessati oggetto del trattamento?				
8) E' indicato il Titolare del trattamento?				
9) E' indicato, se previsto, un responsabile del trattamento ex articolo 28 del GDPR?				
10) E' un trattamento comunicato ad altri Titolari?				
11) E' un trattamento che comporta trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale?				
12) Le misure di sicurezza sono indicate?				
13) E' indicato il periodo di conservazione dei dati?				
14) E' un trattamento che prevede *"un rischio elevato per i diritti e le libertà delle persone"?*				

15) Se la risposta al quesito 14 è SI, la valutazione d'impatto di cui all'articolo 35 del GDPR è stata effettuata?				
16) La valutazione d'impatto è completa?				

Eventuali osservazioni/criticità.

ALLEGATO C

Titolare del Trattamento:	
Data Compilazione:	

Registro	CHECK	SI	NO	N/A	NOTE
Registro Titolare:	Esiste il registro delle attività eseguite come Titolare?				
Registro Responsabile:	Esiste il registro delle attività di trattamento svolte-per conto del Titolare in qualità di Responsabile?				
Aggiornamento Registri	I registri sono periodicamente aggiornati?				

Ruoli e Responsabilità	CHECK	SI	NO	N/A	NOTE
Soggetti Designati al Trattamento:	Esiste un organigramma/funzionigramma, o elenco, che identificano i soggetti designati al trattamento?				
Designazione Autorizzati:	Le figure autorizzate al trattamento dei dati sono formalmente nominate tramite lettere di incarico, nomine o altri documenti, che identificano ruolo, responsabilità e obblighi delle figure con riferimento ai trattamenti gestiti nonchè sono identificati i privilegi di accesso a specifici asset/archivi assegnati?				

Amministratori di Sistema:	E' stato nominato l'amministratore di sistema (ove ne ricorrano i presupposti) ?				
Designazione Amministratori di Sistema:	Sono stati rispettati i termini previsti dal Provvedimento del Garante del 27.11.08 per le attività riconducibili all'Amministratore di Sistema?				
Identificazione dei **Responsabili** e dei sub-Responsabili:	Esiste un elenco di fornitori a cui sono stati affidati dati personali gestiti nella qualità di Titolare/Responsabile?				
Designazione del Fornitore quale Responsabile ai sensi delle norme Privacy	I fornitori a cui sono stati affidati i dati personali sono stati designati Responsabili (Sub-Responsabili) ai sensi del Regolamento europeo 679/2016 (GDPR) mediante atto scritto in cui vengono indicati i termini per la gestione dei dati personali (Data ProtecTion Agreement):				

Informative	CHECK	SI	NO	N/A	NOTE
Informativa rivolta ai clienti	E' presente e viene fornita ai clienti specifica informativa in cui vengono indicati i termini per il trattamento dei dati personali?				
Informativa rivolta ai dipendenti	E' presente e viene fornita ai dipendenti specifica informativa in cui vengono indicati i termini per il trattamento dei dati personali?				
Informativa rivolta ai visitatori del sito web	E' stata pubblicata sul sito web specifica informativa in cui vengono indicati i trattamenti connessi alla gestione del sito Internet?				
Informativa rivolta ai clienti	E' stata pubblicata l'informativa per la gestione dei cookies?				
Consensi	Le finalità indicate all'interno delle informative trovano corrispondenza con le finalità indicate all'interno del registro?				

Procedure ed Istruzioni	CHECK	SI	NO	N/A	NOTE
Diritti degli interessati	E' presente una procedura che disciplina le modalità con cui sono garantiti i diritti esercitati dagli interessati?				
Privacy by Design	E' presente una procedura che disciplina le modalità con cui vengono variati / implementati nuovi progetti (anche tecnologici) che prevedono l'impiego di dati personali?				
Nomina dei Responsabili	E' presente una procedura che disciplina le modalità di nomina di un fornitore come Responsabile / Sub-Responsabile del Trattamento dei Dati personali?				
Nomina soggetti Autorizzati	E' presente una procedura che disciplina le modalità di nomina dei soggetti Autorizzati?				
Violazione dei Dati (Data Breach)	E' presente una procedura per l'intercettazione e notifica al Garante di una violazione dei dati personali (Data Breach)				
Procedura controllo Sistema Privacy	E' presente Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento anche con attività di Audit (Art. 32, c.1, let. d GDPR)?				
Procedura Data Retention	E' presente una procedura che disciplina le modalità per conservazione e cancellazione dei dati personali?				
Cambio Mansione / Interruzione Rapporto	Esiste un processo strutturato e formalizzato che prevede la creazione, modifica e cancellazione degli utenti in caso di inizio, cambio o cessazione del rapporto di lavoro o delle mansioni e la rimozione delle utenze inattive o non più necessarie?				

Formazione	CHECK	SI	NO	N/A	NOTE
Attività Formative	Sono previste attività periodiche di formazione rivolte al personale dipendente?				

Applicazione attività Formative	Il materiale formativo tratta, oltre alla normativa GDPR in generale, anche la concreta implementazione degli adempimenti privacy e le modalità operative concrete da attuare dai dipendenti coinvolti nei vari trattamenti?				

Data Breach	CHECK	SI	NO	N/A	NOTE
Registro Data Breach	Esiste un registro dei data breach che preveda l'inserimento almeno delle seguenti informazioni: natura della violazione, interessati coinvolti, possibili conseguenze e nuove misure di sicurezza implementate?				
Gravità della Violazione	E' stata implementata una metodologia per determinare la gravità della violazione?				

Valutazione dei Rischi / DPIA	CHECK	SI	NO	N/A	NOTE
Valutazione dei rischi	E' stata eseguita, per tutti i trattamenti sia come Titolare che Responsabile, una Valutazione dei rischi per i diritti e le libertà degli interessati che considerino le minacce e i potenziali impatti per gli Interessati?				
Trattamento ad Alto Rischio	Sono stati identificati i trattamenti che possono presentare rischi elevati per gli interessati ai sensi del WP248 nonchè dell'allegato 1 del provvedimento n. 467 del 11-10-2018?				
Esecuzione del DPIA	Per i trattamenti ad alto rischio sono stati eseguiti i DPIA per determinare se il rischio residuo degli interessati è ritenuto accettabile?				

MIsure di Sicurezza	CHECK	SI	NO	N/A	NOTE

Back-up	Sono effettuate periodicamente copie di back-up dei dati al fine di garantire la continuità operativa?				
Archiviazione Backup	Tutti i supporti di back-up e di archiviazione sono conservati in aree di memorizzazione sicure e controllate a livello ambientale?				
Censimento Asset	E' stata effettuata la mappatura delle banche dati e degli archivi -cartacei e non- relativi ai trattamenti svolti?				
Formazione Security IT	Sono previste le modalità di aggiornamento e di formazione dei dipendenti dell'area IT e degli utenti dei sistemi informatici con riferimento alle misure tecniche di sicurezza?				
Privilegi di Accesso	L'accesso ai sistemi contenenti dati personali avviene attraverso codice ID e password univoci per ciascun utente?				
Password	Le password sono cambiate periodicamente ed è richiesta una lunghezza minima (almeno 8 caratteri o la lunghezza massima consentita dal sistema) e devono contenere almeno 2 tipologie diverse di caratteri (es. numeri, lettere, caratteri speciali, maiuscoli)?				
Verifica Privilegi	E' prevista la rivisitazione periodica dei diritti di accesso degli utenti ed è verificato l'allineamento tra ID/account attivi e utenti autorizzati?				
Limitazione degli accessi	Ove applicabile esistono autorizzazioni specifiche per diversi utenti o categorie, limitando l'accesso ai soli dati necessari allo svolgimento dell'attività? Sono limitati e controllati l'assegnazione e l'uso di diritti di accesso privilegiato?				
Cifratura	Esistono strumenti di cifratura dei dati statici su supporti di memorizzazione?				
Trasmissione sicura	Sono implementati protocolli crittografici in fase di trasferimento nelle comunicazioni e nelle transazione (es. certificati SSL/TSL)?				
Pseudonimizzazione	Sono implementate tecniche di pseudonimizzazione dei dati?				
AntiVirus	Le postazioni di lavoro sono costantemente protette e monitorate da programmi in grado di identificare e rimuovere software dannosi (es. antivirus, antispyware, etc) e prevenire intrusioni (es. firewall, etc.)?				

Aggiornamento AntiVirus	I programmi contro i software dannosi sono costantemente aggiornati?				
Software Non Autorizzati	E' vietata l'installazione di software non autorizzati ed esistono programmi in grado di identificare e rimuovere i software dai PC degli utenti?				
Penetration Test	Gli hardware/software acquistati/sviluppati sono sottoposti a test di vulnerabilità e penetration test?				
Registrazione dei Log	E' effettuata, mantenuta e riesaminata periodicamente la registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni?				
Attività di Collaudo	Sono eseguiti collaudi formali e test per assicurare funzionalità, conformità tecnica e requisiti di sicurezza in caso di acquisizione, sviluppo manutenzione dei sistemi IT, prima di rendere operativi i sistemi?				

Protezione perimetrale Strumenti di protezione della rete anche atti a prevenire intrusioni (es. firewall, etc.)

Network monitoring Strumenti per il monitoraggio del traffico rete

FIRMA _____