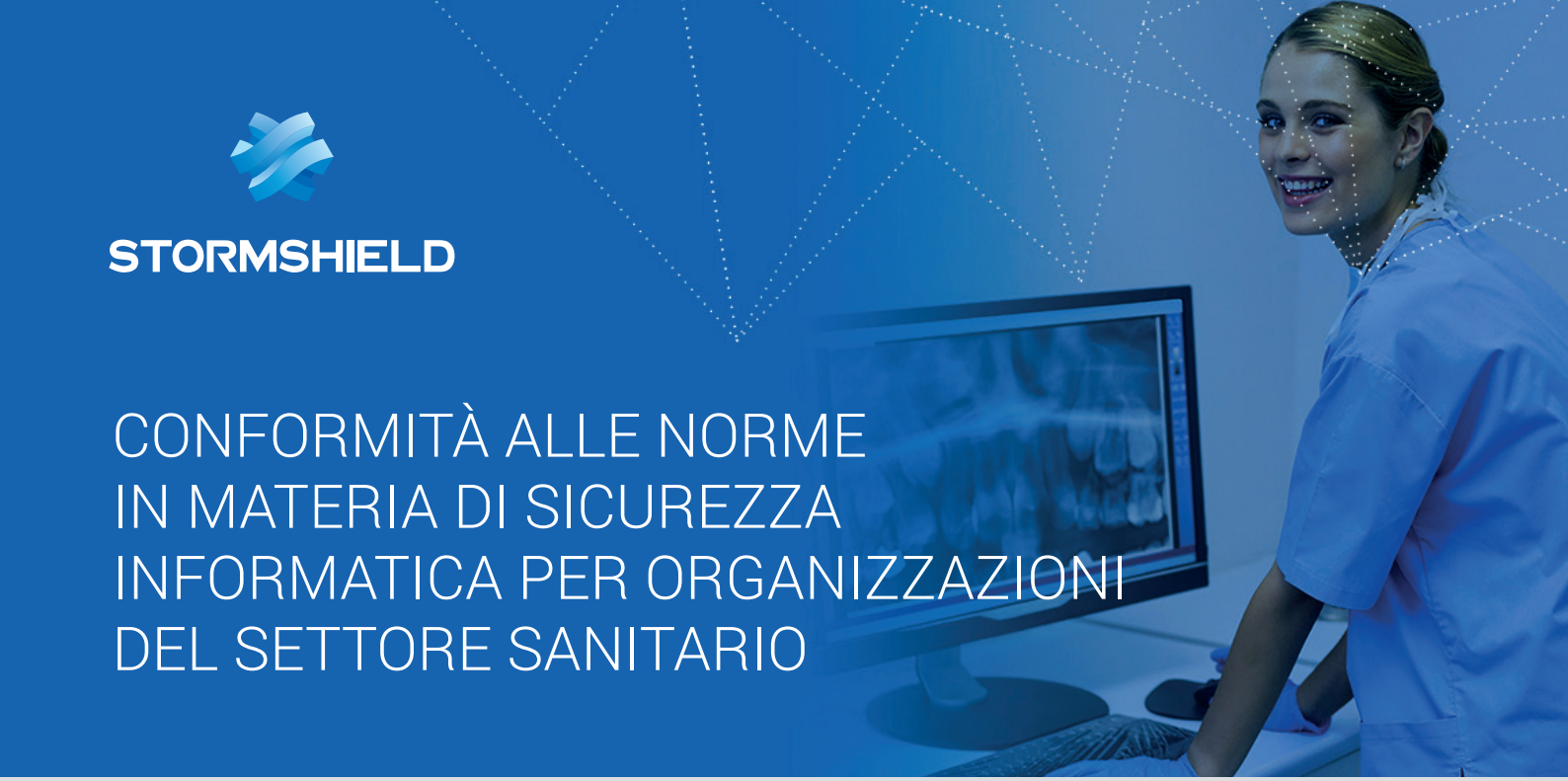
STORMSHIELD



CONFORMITÀ ALLE NORME IN MATERIA DI SICUREZZA INFORMATICA PER ORGANIZZAZIONI DEL SETTORE SANITARIO

Nel settore sanitario, in cui la disponibilità dei servizi ricopre un'importanza critica, gli attacchi informatici possono realmente trasformarsi in una questione di vita o di morte. Inoltre, i fornitori di servizi sanitari devono far fronte all'obbligo giuridico di tutelare i dati dei pazienti. Tale requisito si applica anche al contesto odierno, in cui i sistemi sanitari si affidano in misura sempre maggiore a dati trasmessi mediante dispositivi mobili ma che devono pur sempre essere difesi da potenziali intrusioni.

> NORMATIVE EUROPEE: CONFORMITÀ OBBLIGATORIA

> REQUISITI OPZIONALI DI CONFORMITÀ

> NORMATIVE LOCALI

> PER OGNI PROBLEMA C'È UNA SOLUZIONE STORMSHIELD

> LA CONFORMITÀ NON BASTA

> NORMATIVE EUROPEE: CONFORMITÀ OBBLIGATORIA

Le organizzazioni del settore sanitario hanno l'obbligo di ottemperare alle seguenti normative europee in materia di sicurezza informatica:

Regolamento generale sulla protezione dei dati (GDPR)

Il GDPR è un regolamento europeo introdotto con il fine di armonizzare le norme in materia di riservatezza in vigore nei Paesi europei, nonché per tutelare le informazioni personali dei cittadini e rivoluzionare l'approccio adottato dalle aziende sul fronte della riservatezza dei dati. Tale regolamento introduce nuove limitazioni e nuovi requisiti che i Responsabili dei Sistemi informativi, i CIO e CISO sono tenuti a osservare.

I requisiti includono, tra gli altri, il principio della "Data protection by default", secondo cui la tutela dei dati personali deve avvenire per impostazione predefinita nell'ambito di servizi e sistemi. I prodotti Stormshield aiutano le organizzazioni a conformarsi a tali requisiti incrementando la resilienza delle rispettive infrastrutture informatiche. Stormshield Data Security mette a disposizione anche funzioni di crittografia dei dati, che il GDPR identifica come una misura tecnica adeguata a garantire un livello di protezione commisurato al rischio.

Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS)

La Direttiva NIS, ovvero la prima normativa europea in materia di sicurezza informatica, intende incrementare il livello complessivo di protezione all'interno dell'Unione europea e dovrà essere recepita negli ordinamenti giuridici degli stati membri. Ai sensi della direttiva NIS, ogni Paese è tenuto a designare Operatori di Servizi Essenziali (OES) in settori quali energia, trasporti, acqua potabile, infrastrutture del mercato bancario e finanziario, sanità e infrastrutture digitali. Gli OES designati avranno l'obbligo di conformarsi ai requisiti della direttiva.

Stormshield mette a disposizione prodotti certificati e affidabili per consentire agli OES di implementare soluzioni di sicurezza informatica capaci di potenziare il livello di protezione dei sistemi informativi essenziali. Ad esempio, Stormshield Network Security è in grado di isolare le aree di rete, garantire la sicurezza degli accessi da remoto, consentire l'autenticazione degli utenti e gestire le vulnerabilità. Stormshield Endpoint Security (SES), lavorando congiuntamente a un prodotto antivirus (se presente), introduce una protezione efficace della postazione di lavoro contro minacce sofisticate. Inoltre, SES è in grado di migliorare la protezione dei sistemi operativi esistenti, consentire l'individuazione e la gestione di eventi imprevisti e proteggere da attacchi di tipo "bouncing".

> **NORMATIVE EUROPEE: CONFORMITÀ OBBLIGATORIA**

Payment Card Industry Data Security Standard (PCI-DSS)

Il PCI-DSS raggruppa una serie di norme di sicurezza delle informazioni applicabili alle aziende che raccolgono pagamenti mediante carte di credito emesse dalle principali società emittenti. L'osservanza di tali norme è obbligatoria per qualsiasi commerciante, istituzione finanziaria o altra persona giuridica che si fa carico dell'archiviazione, trattamento o trasmissione dei dati dei titolari di carte di pagamento. Le norme includono disposizioni in materia di sicurezza della rete, crittografia dei dati, gestione delle vulnerabilità e controllo efficace degli accessi.

I prodotti Stormshield permettono alle aziende di assicurare la conformità con molti dei principali requisiti PCI-DSS. Ad esempio, Stormshield Network Security (SNS) è in grado di isolare aree di rete e proteggere il traffico in uscita mediante crittografia, nonché gestire le vulnerabilità e l'autenticazione degli utenti. Stormshield Data Security consente di crittografare i dati dei titolari di carta per garantirne l'integrità e la riservatezza. Stormshield Endpoint Security (SES), lavorando congiuntamente a un prodotto antivirus, rafforza la protezione della postazione di lavoro contro minacce sofisticate. Inoltre, SES è in grado di migliorare la protezione dei sistemi operativi esistenti, consentire l'individuazione e la gestione di eventi imprevisti e proteggere da attacchi di tipo "bouncing".

Direttiva relativa al riutilizzo dell'informazione del settore pubblico (PSI)

La Direttiva PSI introduce un quadro legislativo comune che incoraggia gli stati membri dell'UE a massimizzare il potenziale dell'informazione del settore pubblico rendendo possibile il riutilizzo della stessa. La PSI si applica a tutte le informazioni generate, raccolte o acquistate dagli enti pubblici. La Direttiva PSI, recepita nei vari ordinamenti giuridici nazionali, costituisce la base della politica di Open Data dell'Unione europea. Tutti gli enti che gestiscono informazioni a carattere pubblico o generano dati a partire da progetti di ricerca finanziati con fondi pubblici hanno l'obbligo di fornire l'accesso a tali informazioni, fatte salve limitazioni specifiche.

I prodotti Stormshield possono aiutare le organizzazioni a conformarsi ai requisiti della Direttiva PSI. In particolare, Stormshield Network Security (SNS) rende possibile la micro-segmentazione della rete per consentire l'isolamento dell'area di archiviazione dei dati pubblici. Inoltre, grazie alla gestione intuitiva delle politiche di protezione, SNS facilita l'identificazione delle aree di rete, la gestione degli accessi a livello di utente o di gruppo e l'introduzione di vincoli temporali.

Cybersecurity Act

Il regolamento europeo Cybersecurity Act rappresenta una riposta alla crescente minaccia di attacchi informatici, rafforzando le prerogative dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e dotandosi di un sistema europeo di certificazione in materia di cybersecurity. Questo sistema europeo di certificazione punta a rafforzare la sicurezza dei prodotti connessi, dei dispositivi dell'Internet delle cose e delle infrastrutture critiche tramite appositi certificati. Si tratta dunque di una certificazione di prodotti, processi e servizi che sarà valida in tutti gli Stati membri. I 3 livelli individuati ("di base", "sostanziale" ed "elevato") consentiranno agli utenti di stabilire il livello di affidabilità della sicurezza e garantiranno che gli elementi di sicurezza siano stati verificati in modo indipendente.

I prodotti Stormshield hanno già raggiunto il livello "Qualifica Standard" previsto in Francia dall'ANSSI (Agenzia nazionale per la sicurezza dei sistemi informativi). Sapendo che il livello "elevato" del sistema europeo corrisponde al livello "Qualifica Base" dell'ANSSI (che è inferiore al livello "Qualifica Standard"), i prodotti Stormshield sono dunque già conformi alle aspettative dell'ENISA in materia di cybersecurity.

Desideri saperne di più? Nessun problema!

> REQUISITI OPZIONALI DI CONFORMITÀ

Le organizzazioni del settore sanitario che desiderino migliorare i propri livelli di sicurezza informatica dovrebbero adeguarsi anche agli standard seguenti, sebbene la conformità a questi non rappresenti un requisito normativo.

Common Criteria / Evaluation Assurance Level (EAL3+, EAL4+ ecc.)

"Common Criteria for Information Technology Security Evaluation" è una norma internazionale (ISO/IEC 15408) per la certificazione della sicurezza informatica. Serve ad assicurare che il processo di definizione delle specifiche, implementazione e valutazione delle soluzioni per la sicurezza informatica sia condotto in modo rigoroso, standardizzato e ripetibile, nonché a un livello commisurato al contesto di applicazione previsto. Ai sensi della norma, il "livello di garanzia della valutazione" attribuito (EAL3+, EAL4+ ecc.) indica l'accuratezza dei test a cui è stato sottoposto il prodotto in esame (ad es. un firewall). Questa certificazione è riconosciuta in 30 Paesi del mondo in Europa, Nord America, Asia e Medio Oriente.

I prodotti Stormshield non sono solo certificati ai sensi delle norme "Common Criteria", ma hanno raggiunto il livello più alto di "Qualifica Standard" rilasciato dall'ente francese ANSSI (Agenzia Nazionale per la Sicurezza dei Sistemi Informativi). Per conseguire tale status, i prodotti devono:

- Ottenere una certificazione di alto livello in base a un obiettivo di sicurezza stabilito e validato dall'ANSSI;
- Superare ulteriori procedure di valutazione svolte dall'ANSSI, inclusa un'analisi del codice sorgente.

Notare che la "Qualifica Standard" rappresenta un prerequisito per il rilascio delle denominazioni "NATO-Riservato" o "UE-Riservato" richieste per la gestione di informazioni classificate.

Elenco delle raccomandazioni dell'ENISA

L'agenzia europea ENISA ha pubblicato un elenco di raccomandazioni sulla sicurezza informatica nell'ambito dei contratti pubblici ospedalieri, per servizi, prodotti o infrastrutture. Un documento destinato a responsabili informatici dei centri ospedalieri.

I prodotti Stormshield sono qualificati e certificati ai massimi livelli europei: sinonimo di affidabilità e solidità. Permettono agli Operatori dei servizi essenziali (OSE) di distribuire soluzioni di sicurezza in grado di migliorare il livello di protezione dei Sistemi informatici essenziali (SIE). A titolo di esempio, Stormshield Network Security permette la segmentazione delle reti, la protezione degli accessi da remoto, l'autenticazione degli utenti e la gestione delle vulnerabilità. Distribuendo una soluzione qualificata e certificata ai massimi livelli europei, usufruirete di un prodotto la cui solidità è stata comprovata durante il processo di certificazione.

Desideri saperne di più? Nessun problema!

> REQUISITI OPZIONALI DI CONFORMITÀ

Le organizzazioni del settore sanitario che desiderino migliorare i propri livelli di sicurezza informatica dovrebbero adeguarsi anche agli standard seguenti, sebbene la conformità a questi non rappresenti un requisito normativo.

Standard ISO/IEC 27000 Tecnologie dell'informazione - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni

La serie ISO/IEC 27000 è una famiglia di norme in materia di sicurezza delle informazioni che fornisce un framework globalmente riconosciuto per una gestione efficace della sicurezza delle risorse informative. Caratterizzata da un ambito di applicazione deliberatamente ampio, questa serie di norme si applica ad aziende di qualsiasi dimensione e settore.

Il Sistema di gestione della sicurezza delle informazioni (ISMS) fornisce un approccio sistematico alla protezione di infrastrutture sensibili. In considerazione del carattere dinamico del rischio e delle misure di protezione richieste, l'ISMS incorpora feedback e miglioramenti costanti per reagire ai cambiamenti che interessano le minacce, le vulnerabilità o l'impatto di eventi imprevisti.

I prodotti Stormshield sono ideati per garantire la protezione delle infrastrutture sensibili. Il formato di log standard permette alle aziende di centralizzare tutte le informazioni, favorendo l'identificazione di trend e potenziali vulnerabilità. L'interfaccia grafica estremamente intuitiva facilita inoltre l'implementazione di miglioramenti da parte degli utenti.

> NORMATIVE LOCALI

REGNO UNITO

Data Protection Act 2018 (Legge sulla protezione dei dati)

Con un ambito di applicazione simile a quello del GDPR, il Data Protection Act è una norma specifica per il Regno Unito. La norma stabilisce che qualsiasi tipologia di dati personali dovrebbe essere soggetta a "un livello di protezione adeguato", definito sulla base del rischio potenziale associato ad accessi non autorizzati. Tale principio include misure di protezione tese a impedire l'elaborazione illecita o non autorizzata, la perdita accidentale, la distruzione o l'invalidazione delle informazioni.

I prodotti Stormshield aiutano le organizzazioni a conformarsi a tali requisiti incrementando la resilienza delle rispettive infrastrutture informatiche. Stormshield Data Security mette a disposizione anche funzioni di crittografia dei dati, che il GDPR identifica come una misura tecnica adeguata a garantire un livello di protezione commisurato al rischio.

> NORMATIVE LOCALI

FRANCIA

Codice della sanità pubblica - Articolo relativo ai soggetti che detengono dati sanitari

L'articolo L1111-8 del Codice della sanità pubblica stabilisce le condizioni di attività dei soggetti che detengono dati sanitari a carattere personale. Il Responsabile del trattamento e il relativo servizio di archiviazione hanno l'obbligo di garantire la protezione efficace dei dati sanitari detenuti.

Le soluzioni Stormshield aiutano a soddisfare i requisiti di conformità a carico delle strutture sanitarie grazie a un set completo di funzionalità. In particolare, Stormshield Data Security assicura la protezione dei dati con conformità garantita anche qualora i dati siano salvati all'interno di soluzioni Cloud, indipendetemente dalla posizione di archiviazione.

Nota interministeriale n. 901/SGDSN

La nota interministeriale n. 901 relativa alla tutela dei sistemi informativi a carattere sensibile si applica in particolar modo agli enti pubblici o privati soggetti alla normativa "PPST" sulla protezione del potenziale scientifico e tecnico della nazione che si fanno carico dell'utilizzo di sistemi informativi sensibili. I dati il cui trattamento è gestito mediante i suddetti sistemi informativi sensibili (come i brevetti da consegnare in aree con regimi restrittivi) devono inoltre essere contrassegnati dalla dicitura "Informazione riservata".

La soluzione Stormshield Data Security mette a disposizione funzioni di crittografia dei dati che permettono di impedire la compromissione di informazioni sensibili per tutelare l'immagine degli enti interessati. L'implementazione crittografica con certificazione EAL3+, qualificata da ANSSI e NATO, è adatta anche alla protezione dei dati di tipo "Riservato".

Ordinanza n. 2020-1407 del 18 novembre 2020 relativa agli incarichi delle agenzie regionali di salute

L'articolo 1 della presente ordinanza impone l'obbligo di segnalazione degli incidenti di carattere informatico alle autorità competenti dello Stato e all'Agenzia nazionale di sanità pubblica per tutte le strutture di salute, sanitarie e medico-sociali.

I registri di eventi proposti dalle soluzioni Stormshield, a titolo di eventi di sicurezza, fanno parte delle informazioni essenziali da trasmettere alle autorità competenti in caso di incidenti. L'evoluzione della soluzione Stormshield Endpoint Security risponde, nella fattispecie, a questa problematica quando l'attacco è sofisticato e quando tenta di aggirare i mezzi di protezione. Oltre a bloccare in maniera proattiva i tipi di attacchi più sofisticati, Stormshield Endpoint Security Evolution fornisce gli elementi di contestualizzazione necessari ad approfondire ulteriormente gli incidenti di sicurezza.

> NORMATIVE LOCALI

FRANCIA

Best practice ANSSI

L'Agenzia Nazionale per la Sicurezza dei Sistemi Informativi (ANSSI) riveste un ruolo chiave sul fronte della sicurezza informatica in Francia e si occupa inoltre di stilare periodicamente una serie di best practice. Non si tratta propriamente di "regolamenti", quanto piuttosto di linee guida finalizzate a supportare il processo decisionale per la selezione dei fornitori e delle soluzioni di sicurezza informatica, nonché per favorire l'implementazione delle medesime. Le best practice si concentrano su temi quali crittografia, sicurezza delle postazioni di lavoro e reti, proponendo risorse utili e approfondite.

La sezione "Sicurezza digitale delle comunità territoriali: l'essenziale della normativa" è una guida complementare al nostro e-book. Un documento sintetico, pratico e accessibile destinato alle parti interessate e ai dirigenti territoriali con la responsabilità di garantire l'applicazione e la conformità.

> NORMATIVE LOCALI

GERMANIA

Ufficio Federale per la Sicurezza Informatica (BSI)

Le norme BSI sono una componente fondamentale della metodologia IT-Grundschutz. Gli attuali standard BSI sono i seguenti:

- 200-1 (Requisiti generali per sistemi di gestione della sicurezza delle informazioni)
- 200-2 (Fondamenti per lo sviluppo di una gestione efficace della sicurezza delle informazioni)
- 200-3 (Tutte le operazioni associate ai rischi nell'implementazione delle misure di sicurezza informatica di base)

Legge sulla sicurezza informatica (IT-Sicherheitsgesetz) e Legge BSI (BSI-Gesetz)

La Legge sulla sicurezza informatica stabilisce che gli operatori del settore sanitario hanno l'obbligo di conformarsi a un livello minimo di protezione delle informazioni, segnalando eventuali interruzioni significative al BIS. In riferimento al concetto di "livello minimo di protezione", il paragrafo 8a del BSI-Gesetz è stato reso esecutivo mediante la Legge sulla sicurezza informatica, la quale definisce il "livello minimo" in termini astratti. In aggiunta, il 2016 ha visto l'introduzione del BSI-Kritisverordnung, il quale dettaglia i servizi critici che saranno tutelati ai sensi della Legge sulla sicurezza informatica. Tale ordinanza copre anche il settore sanitario.

Stormshield mette a disposizione prodotti certificati e affidabili per l'implementazione di soluzioni di sicurezza informatica capaci di potenziare il livello di protezione dei sistemi. Ad esempio, Stormshield Network Security è in grado di isolare le aree di rete, garantire la sicurezza degli accessi da remoto, consentire l'autenticazione degli utenti e gestire le vulnerabilità. Stormshield Endpoint Security (SES), lavorando congiuntamente a un prodotto antivirus (se presente), introduce una protezione efficace della postazione di lavoro contro minacce sofisticate. Inoltre, SES è in grado di migliorare la protezione dei sistemi operativi esistenti, consentire l'individuazione e la gestione di eventi imprevisti e proteggere da attacchi di tipo "bouncing". Stormshield Data Security aiuta infine a prevenire le fughe di informazioni attraverso la cifratura di informazioni sensibili.

Legge federale sulla protezione dei dati (BDSG)

Il trattamento di dati sanitari richiede l'adozione di misure specifiche e adeguate al fine di salvaguardare gli interessi dei soggetti interessati, come sancito dal paragrafo 22 (2) del BDSG. Il paragrafo specifica altresì le misure a livello tecnico e organizzativo di cui sarà necessario farsi carico nel trattamento di dati sanitari.

I requisiti includono, tra gli altri, il principio della "Data protection by default", secondo cui la tutela dei dati personali deve avvenire per impostazione predefinita nell'ambito di servizi e sistemi. I prodotti Stormshield aiutano le organizzazioni a conformarsi a tali requisiti incrementando la resilienza delle rispettive infrastrutture informatiche. Stormshield Data Security mette a disposizione anche funzioni di crittografia dei dati, identificate come una misura tecnica adeguata per garantire un livello di protezione commisurato al rischio.

> NORMATIVE LOCALI

GERMANIA

Legge sulla salute digitale e il Libro quinto del Codice sociale

La Legge sulla salute digitale riguarda le comunicazioni elettroniche e le relative applicazioni nel settore sanitario. Contiene una roadmap concreta per la creazione di un'infrastruttura telematica protetta e l'introduzione di applicazioni sanitarie. La Legge sulla salute digitale modifica il Libro quinto del Codice sociale.

I prodotti Stormshield aiutano le organizzazioni a conformarsi ai requisiti della direttiva incrementando la resilienza delle rispettive infrastrutture informatiche. Stormshield Network Security offre caratteristiche di protezione innovative con gestione unificata delle minacce. Inoltre, Stormshield Endpoint Security provvede a migliorare il livello di sicurezza degli antivirus tradizionali neutralizzando le minacce avanzate. Stormshield Data Security aiuta infine a conformarsi ai requisiti in materia di protezione dei dati.

> NORMATIVE LOCALI

ITALIA

Decreto legislativo 18 maggio 2018, n. 65 (Attuazione della direttiva (UE) 2016/1148)

Il Decreto introduce misure tese a garantire la tutela dei dati personali a livello nazionale, ivi compresi: la costituzione del CSIRT (noto anche con la denominazione CIRT); gli obblighi a carico dei cosiddetti "operatori di servizi essenziali" e dei fornitori di servizi digitali relativamente alle procedure per rispondere alle violazioni di sicurezza; i principi di cooperazione internazionale su questioni attinenti alla sicurezza; e l'adozione di una strategia nazionale di sicurezza informatica.

Stormshield mette a disposizione prodotti certificati e affidabili per consentire agli OES di implementare soluzioni di sicurezza informatica capaci di potenziare il livello di protezione dei sistemi informativi essenziali. Ad esempio, Stormshield Network Security è in grado di isolare le aree di rete, garantire la sicurezza degli accessi da remoto, consentire l'autenticazione degli utenti e gestire le vulnerabilità. Stormshield Endpoint Security (SES), lavorando congiuntamente a un prodotto antivirus (se presente), introduce una protezione efficace della postazione di lavoro contro minacce sofisticate. Inoltre, SES è in grado di migliorare la protezione dei sistemi operativi esistenti, consentire l'individuazione e la gestione di eventi imprevisti e proteggere da attacchi sofisticati.

D.P.C.M. 178 del 2015 (Fascicolo Sanitario Elettronico - FSE)

Il Fascicolo Sanitario Elettronico l'insieme di dati e documenti digitali di tipo sanitario e socio-sanitario generati dagli eventi clinici dei pazienti, che si propone principalmente di agevolare l'assistenza al paziente e facilitare l'integrazione delle diverse competenze professionali in termini di sanità e assistenza. La conformità alla norma (anche dal punto di vista della sicurezza) si basa sui principi del GPDR e sulle disposizioni del Garante relative all'FSE.

I prodotti Stormshield aiutano le organizzazioni sanitarie a conformarsi a tali requisiti incrementando la resilienza delle rispettive infrastrutture informatiche. Stormshield Data Security mette a disposizione anche funzioni di crittografia dei dati, identificate come una misura tecnica adeguata per garantire un livello di protezione commisurato al rischio.

> NORMATIVE LOCALI

SPAGNA

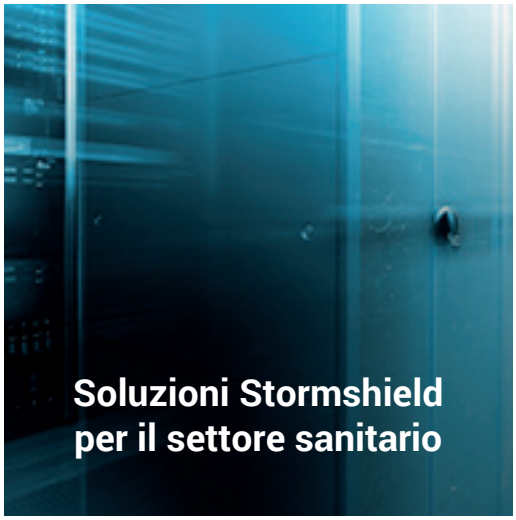
Programma di sicurezza nazionale, Decreto reale 3/2010 dell'8 gennaio

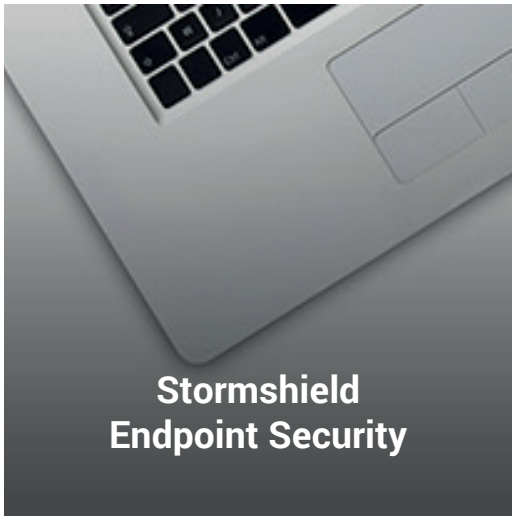
Le aziende ospedaliere identificate come "personalità giuridiche pubbliche", ovvero collegate all'Amministrazione Generale dello Stato, alle Comunità autonome o agli Organi amministrativi locali (o dipendenti da questi ultimi) sono tenute a conformarsi pienamente ai requisiti di tale programma per le attività non regolate dal diritto privato.

I prodotti Stormshield aiutano le organizzazioni a conformarsi ai suddetti requisiti incrementando la resilienza delle rispettive infrastrutture informatiche. Stormshield Network Security offre caratteristiche di protezione innovative con gestione unificata delle minacce. I nostri prodotti SNS rappresentano la sola gamma europea qualificata come "Productos Cualificados" e l'unica gamma di firewall qualificata come "Productos Aprobados" dal Centro criptologico nazionale spagnolo (CCN). Inoltre, Stormshield Endpoint Security provvede a migliorare il livello di sicurezza degli antivirus tradizionali neutralizzando le minacce avanzate. Stormshield Data Security mette infine a disposizione funzioni di crittografia dei dati, identificate come una misura tecnica adeguata per garantire un livello di protezione commisurato al rischio.

> PER OGNI PROBLEMA C'È UNA SOLUZIONE STORMSHIELD.

Prodotti e soluzioni Stormshield per il settore sanitario





> LA CONFORMITÀ NON BASTA

L'elevatissimo numero di norme e regolamenti è diventato un problema realmente difficile da gestire per le organizzazioni. La presente guida è stata creata per orientarsi tra le diverse normative applicabili ai vari settori industriali.
Ma la conformità non è tutto. Le aziende devono soprattutto imparare a individuare e gestire efficacemente i rischi a cui sono esposte se intendono realmente garantire la sicurezza delle informazioni.