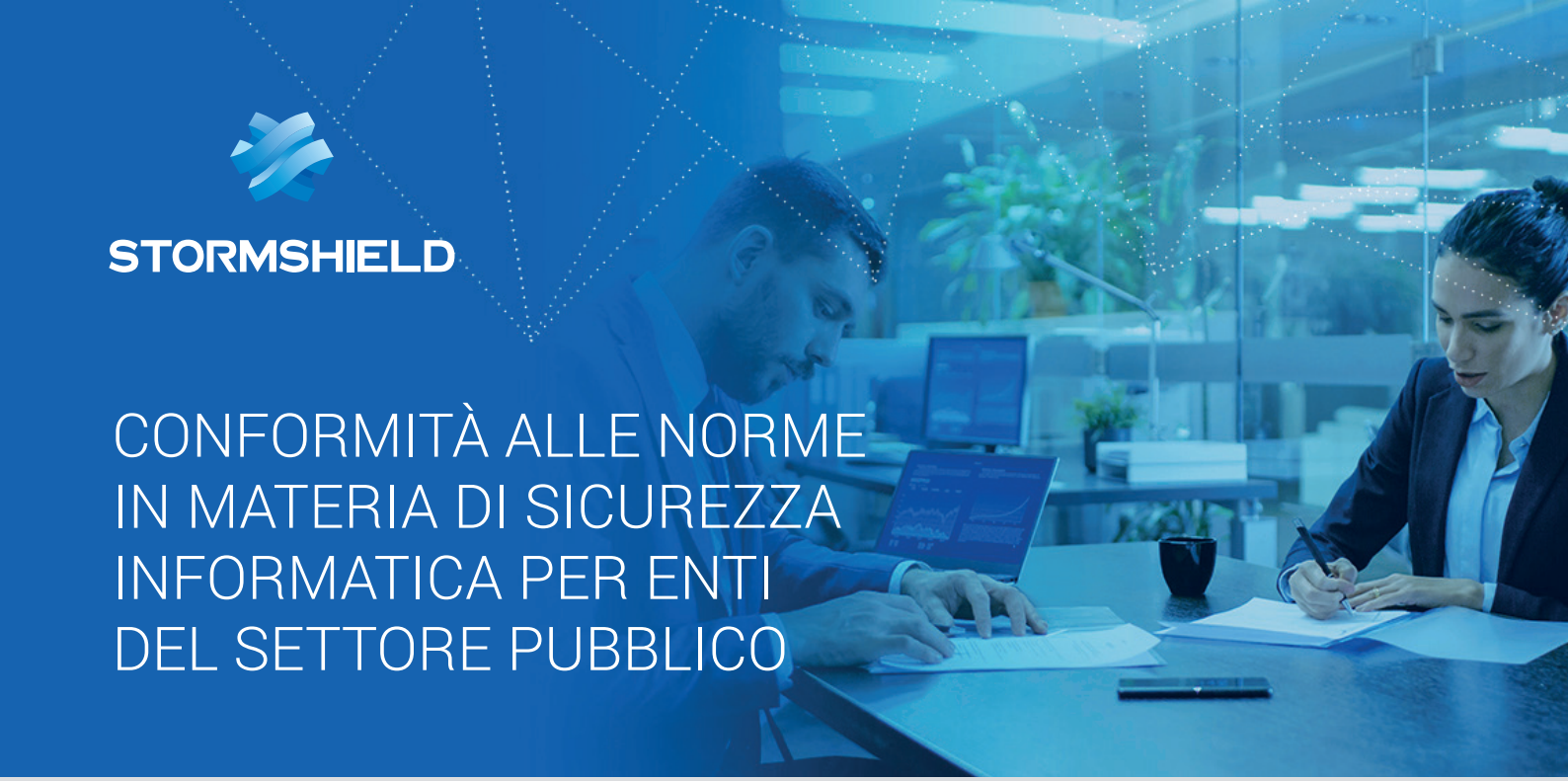


CONFORMITÀ ALLE NORME IN MATERIA DI SICUREZZA INFORMATICA PER ENTI DEL SETTORE PUBBLICO

Le popolazioni si aspettano che gli organismi pubblici mettano a disposizione informazioni online in modo semplice, affidabile e tempestivo.
Eppure, le amministrazioni pubbliche (inclusi i comuni, le agenzie governative e i ministeri) sono spesso oggetto di attacchi informatici. Gli enti pubblici devono dunque far fronte all'esigenza di soddisfare le attese degli utenti, assicurando al tempo stesso la continuità del servizio e la sicurezza dei sistemi informativi.

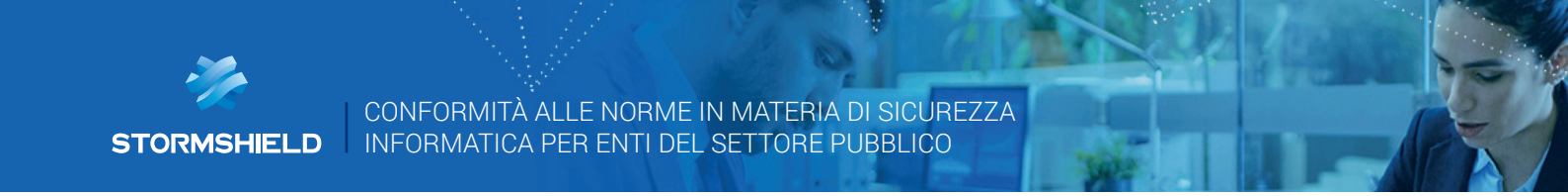
> NORMATIVE EUROPEE: CONFORMITÀ OBBLIGATORIA

> 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 pubblico 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.

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".

> **NORMATIVE EUROPEE: CONFORMITÀ OBBLIGATORIA**

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.

EU Restricted

La classificazione di sicurezza "EU Restricted" si applica a informazioni a carattere sensibile la cui divulgazione non autorizzata, alterazione o mancata disponibilità avrebbe conseguenze avverse agli interessi dell'UE o degli stati membri. Nei casi in cui informazioni con classificazione "EU Restricted" debbano essere trasmesse al di fuori di un'area fisica sicura, la classificazione richiede che i dati siano crittografati a mezzo di soluzioni certificate.

Stormshield Network Security e Stormshield Data Security hanno ricevuto la certificazione "EU Restricted". Possono pertanto essere utilizzate in contesti sensibili per la crittografia di informazioni con la classificazione "EU Restricted" garantendone la trasmissione sicura.

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 pubblico 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.

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

Riferimenti generali di sicurezza (Référentiel Général de Sécurité, RGS)

Il "Référentiel Général de Sécurité (RGS)" si applica ai sistemi informativi implementati dalle autorità amministrative nell'ambito dei rapporti intrattenuti con altri enti pubblici o con i rispettivi utenti. Le autorità amministrative hanno altresì l'obbligo di garantire la sicurezza degli scambi elettronici. I Riferimenti propongono una metodologia e una serie di regole e best practice destinate alle amministrazioni pubbliche, in cui la protezione dei dati assume un'importanza significativa. La soluzione Stormshield Data Security mette a disposizione funzioni di crittografia dei dati per rispondere alle esigenze di qualificazione dei prodotti di sicurezza e dei provider di servizi fiduciari. Stormshield offre inoltre ulteriori linee di prodotti che intendono aiutare gli enti pubblici a conformarsi ai requisiti normativi, incrementando al tempo stesso la resilienza delle infrastrutture.

Politica di sicurezza dei sistemi informativi dello Stato (PSSIE)

La PSSIE si applica a tutti i sistemi informativi degli organi amministrativi dello Stato francese (ministeri, enti pubblici sotto tutela di un ministero, servizi decentrati dello Stato e autorità amministrative indipendenti). Questa politica racchiude principi fondamentali come la scelta di elementi affidabili per la realizzazione dei sistemi informativi, la governance della sicurezza e la sensibilizzazione degli operatori. Tra questi principi, la circolare sottolinea la necessità, per gli organi amministrativi dello Stato, di ricorrere a prodotti e servizi qualificati dall'ANSSI.

Stormshield propone una gamma di prodotti qualificati dall'ANSSI e pertanto conformi al principio fondamentale della PSSIE, che consiste nell'adozione di prodotti affidabili. Si tratta di prodotti che possono dunque essere installati nell'ambito dei sistemi informativi degli organi amministrativi dello Stato, per mettere in sicurezza la rete, proteggere i dati sensibili e rafforzare la protezione delle postazioni di lavoro.

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)

A mezzo dello standard BSI 200-2 "IT-Grundschutz-Methodik", il BSI ha identificato una serie di misure di sicurezza minime implementabili dai governi locali al fine di assicurare un livello di protezione adeguato.

Legge sul governo elettronico (EGovG)

La legge sul governo elettronico (governo federale e governi delle province) si applica principalmente alle attività amministrative delle autorità federali. Nelle circostanze in cui l'esecuzione di un'attività amministrativa presupponga il pagamento di tasse o commissioni, il paragrafo 4 dell'EGovG (governo federale) stipula che le autorità statali debbano consentire il pagamento o saldo delle medesime tramite la partecipazione ad almeno una procedura di pagamento caratterizzata da sufficienti misure di protezione, come solitamente avviene nelle transazioni commerciali elettroniche. In riferimento alle autorità statali che conservano dati elettronici, il paragrafo 6 dell'EGovG (governo federale) introduce l'obbligo di predisporre misure di sicurezza adeguate a livello tecnico e organizzativo (in conformità allo stato dell'arte) al fine di garantire l'osservanza dei principi che regolano la corretta archiviazione delle informazioni. Gli enti pubblici sono infine tenuti a osservare i principi applicabili alla corretta conservazione di documenti, introducendo misure tecniche e organizzative adeguate e conformi allo stato dell'arte.

Legge federale sulla protezione dei dati (BDSG)

I dati che rivelano la razza o l'origine etnica di individui, le opinioni politiche, le credenze religiose o filosofiche o l'appartenenza di questi ultimi ad associazioni sindacali, nonché il trattamento di informazioni generiche, dati biometrici per l'identificazione univoca di persone fisiche o dati concernenti la vita o l'orientamento sessuale di persone fisiche sono considerate categorie di dati speciali ai sensi dell'Art. 9 del GDPR. Il trattamento di tali informazioni 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 durante il trattamento dei dati.

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

Leggi in materia di protezione dei dati applicabili agli stati federali (ad es. Renania Settentrionale-Vestfalia: DSG NRW)

Il DSG NRW introduce una serie di norme complementari per l'implementazione del Regolamento generale sulla protezione dei dati (GDPR). Ad esempio, il paragrafo 58 del DSG NRW specifica i requisiti per la sicurezza delle attività di trattamento dei dati, con il fine specifico di garantire quanto segue:

- la riservatezza, integrità, disponibilità e resilienza su base permanente dei sistemi e servizi associati al trattamento dei dati; e
- la possibilità di ripristinare rapidamente la disponibilità e l'accesso ai dati personali nel caso di eventi imprevisti a livello fisico o tecnico.

Legge De-Mail

La legge De-Mail è entrata in vigore in Germania in data 3 maggio 2011 e rappresenta lo standard adoperato dall'amministrazione federale. La normativa stabilisce che la trasmissione dei messaggi debba avvenire esclusivamente per mezzo di canali crittografati e che i contenuti degli stessi debbano essere archiviati in forma crittografata. Ai sensi del paragrafo 1 (I) della legge De-Mail, i servizi "De-Mail" sono servizi eseguiti su piattaforme di comunicazione elettronica che servono a garantire il completamento di transazioni commerciali sicure, riservate e verificabili.

Per soddisfare i requisiti applicabili allo scambio di comunicazioni elettroniche in modo sicuro, Stormshield Data Security offre una soluzione end-to-end di protezione delle e-mail. Questa soluzione mette a disposizione una serie di funzioni finalizzate a garantire la sicurezza, riservatezza e autenticità degli scambi per tutti gli utenti di internet.

Legge di esecuzione del regolamento eIDAS e Legge in materia di servizi fiduciari (VDG)

In data 29 marzo 2017, il Governo federale ha approvato la Legge di esecuzione del regolamento eIDAS per consentire l'implementazione del Regolamento UE eIDAS ((UE) 910/2014). La Legge di esecuzione del regolamento eIDAS ha introdotto la cosiddetta Legge in materia di servizi fiduciari (VDG). Il più noto servizio fiduciario è rappresentato dalla "firma digitale". Il paragrafo 13 del VDG affronta indirettamente il tema della sicurezza informatica. Ai sensi della norma, il provider qualificato di servizi fiduciari è tenuto a informare soggetti specifici circa le misure necessarie per contribuire alla sicurezza dei servizi fiduciari qualificati offerti e all'utilizzo affidabile degli stessi.

> NORMATIVE LOCALI

ITALIA

Qualifiche di sicurezza (D.P.C.M. 22 luglio 2011)

Le qualifiche di sicurezza (ovvero "Abilitazione Preventiva, AP" e "Nulla Osta di Sicurezza Industriale, NOSI") permettono agli operatori economici la partecipazione a gare d'appalto o a procedure finalizzate all'affidamento di contratti classificati a livello "Riservato (R)" o superiore, più precisamente in riferimento alle gare d'appalto che prevedono il trattamento di informazioni classificate a livello Segretissimo (SS), Segreto (S), Riservatissimo (RR) o Riservato (R). Tali qualifiche impongono l'implementazione di misure specifiche da parte delle aziende, ivi comprese disposizioni di sicurezza fisiche e tecniche.

Legge 124/2007 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto), modificata e integrata dalla legge 133/2012

Il DIS (Dipartimento delle informazioni per la sicurezza), l'AISE (Agenzia informazioni e sicurezza esterna) e l'AISI (Agenzia informazioni e sicurezza interna) sono autorizzate a corrispondere con tutte le pubbliche amministrazioni e con i soggetti che erogano, in regime di autorizzazione, concessione o convenzione, servizi di pubblica utilità e chiedere ad essi la collaborazione necessaria per l'adempimento delle loro funzioni istituzionali. A tale fine possono in particolare stipulare convenzioni con i predetti soggetti (consultare l'art. 13 della legge per ulteriori dettagli).

D.P.C.M. 6 novembre 2015 (Disciplina della firma digitale dei documenti classificati)

Le disposizioni del regolamento si applicano a tutti i soggetti, pubblici e privati, in possesso delle previste abilitazioni di sicurezza per il trattamento di informazioni classificate. Il regolamento disciplina altresì le modalità di generazione, apposizione e verifica delle firme digitali nonché la validazione temporale di documenti informatici classificati.

Direttiva 1 agosto 2015 (Implementazione del quadro strategico nazionale per la sicurezza dello spazio cibernetico)

La Direttiva implementa le finalità illustrate nel Quadro strategico nazionale per la sicurezza dello spazio cibernetico, rendendo possibile il coordinamento tra i diversi soggetti pubblici e lo sviluppo di partenariati con tutti gli operatori non pubblici a cui è affidato il controllo di infrastrutture informatiche e telematiche da cui dipendono funzioni essenziali per il sistema-Paese. La Direttiva assegna all'Agenzia per l'Italia Digitale (AgID) il compito di rendere disponibili standard per le amministrazioni.

> 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. 17 febbraio 2017 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali - Decreto Gentiloni)

La Direttiva introduce gli organismi istituzionali incaricati della protezione cibernetica e della sicurezza informatica nazionali, disciplinando altresì gli obblighi e le responsabilità facenti carico a ciascun ente (CISR, CISR Tecnico, ruolo del DIS e linee guida applicabili, Nucleo per la sicurezza cibernetica e relative responsabilità). La Direttiva introduce inoltre misure applicabili agli "operatori di servizi essenziali" e ai fornitori di servizi di comunicazione.

D.P.C.M. 27 gennaio 2014 (Strategia nazionale per la sicurezza cibernetica - QSN)

La Strategia nazionale per la sicurezza cibernetica intende assicurare l'efficienza e l'interoperabilità delle risorse finalizzate alla difesa comune, al fine di incorporare nel processo di pianificazione della difesa in ambito NATO e nella dottrina militare un'efficace postura contro attacchi cibernetici.

Stormshield Network Security ha ricevuto la certificazione "UE-Riservato". Ciò significa che questi prodotti possono essere adoperati in contesti sensibili al fine di assicurare la trasmissione sicura di informazioni classificate, aiutando a garantire l'interoperabilità internazionale con le istituzioni UE.

> NORMATIVE LOCALI

ITALIA

Piano Triennale 2019-2021 dell'AgID per la Pubblica amministrazione

Il Piano stabilisce una serie di misure normative applicabili ai soggetti pubblici. Tali misure comprendono l'implementazione della piattaforma Infosec, un progetto pilota per la trasmissione automatizzata degli indicatori di compromissione (IoC), linee guida nazionali in materia di sicurezza informatica per i soggetti pubblici e l'obbligo di implementare le linee guida dell'AgID sulle misure di sicurezza.

Misure minime di sicurezza AgID (implementazione del D.P.C.M. del 1 agosto 2015)

Questa Direttiva intende implementare le misure dell'AgID finalizzate a contrastare le minacce alla sicurezza informatica e a fornire gli strumenti di protezione indispensabili per il settore della difesa in termini di controlli tecnici e organizzativi.

I prodotti Stormshield aiutano le organizzazioni del settore pubblico a conformarsi a tali requisiti incrementando la resilienza delle rispettive infrastrutture informatiche. All'ottemperanza ai requisiti normativi contribuisce anche Stormshield Network Vulnerabilty Manager, una soluzione integrata a livello di rete all'interno dei prodotti Stormshield Network Security che facilita la gestione delle vulnerabilità. Inoltre, Stormshield Endpoint Security provvede a migliorare il livello di sicurezza degli antivirus tradizionali neutralizzando le minacce avanzate, mentre Stormshield Data Security, il quale ha ottenuto la certificazione "UE-Riservato", aiuta a garantire la conformità ai requisiti in materia di tutela dei dati.

D.P.C.M. 3 dicembre 2013 (Regole tecniche in materia di sistema di conservazione)

Il D.P.C.M. Introduce requisiti applicabili ai sistemi di conservazione di documenti (ivi compresi i documenti amministrativi e metadati associati) e dossier elettronici, introducendo altresì regole sull'integrità, affidabilità e disponibilità per i suddetti documenti e requisiti applicabili alla componente funzionale della gestione di sistemi di conservazione.

> NORMATIVE LOCALI

SPAGNA

Codice di sicurezza informatica

Il Codice mette a disposizione degli avvocati uno strumento in cui è possibile individuare le norme più recenti direttamente applicabili al tema della sicurezza informatica, facilitando le attività di studio e analisi necessarie per fornire a persone giuridiche, istituzioni e cittadini un livello di protezione adeguato nell'ambito di uno Stato di diritto sociale e democratico.

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. 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.

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

In generale, il programma si applica a siti e registri elettronici e ai sistemi informativi accessibili elettronicamente dai cittadini (per l'esercizio di diritti, l'adempimento di doveri, la raccolta di informazioni e la verifica dello stato di procedure amministrative).

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.

> NORMATIVE LOCALI

SPAGNA

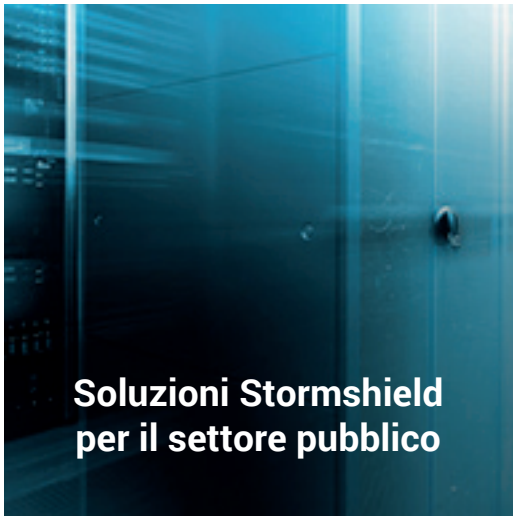
Legge PIC (Protezione delle infrastrutture critiche)

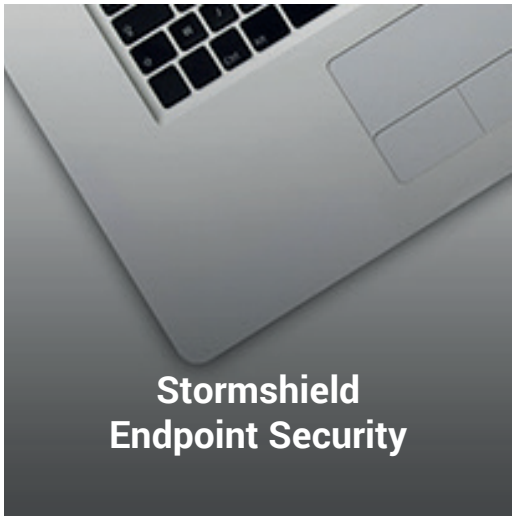
La Legge sulla protezione delle infrastrutture critiche (Ley PIC 8/2011) è integrata dal decreto reale 704/2011. La norma persegue principalmente i due obiettivi seguenti: classificare le infrastrutture responsabili dell'erogazione di servizi essenziali alla società, e ideare un piano di misure di prevenzione e protezione efficaci contro potenziali minacce alle suddette infrastrutture, sia dal punto di vista della sicurezza fisica che in termini di protezione delle tecnologie dell'informazione e della comunicazione.

Stormshield mette a disposizione prodotti certificati e affidabili per consentire alle infrastrutture critiche 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".

> PER OGNI PROBLEMA C'È UNA SOLUZIONE STORMSHIELD.

Prodotti e soluzioni Stormshield per il settore pubblico





> 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.