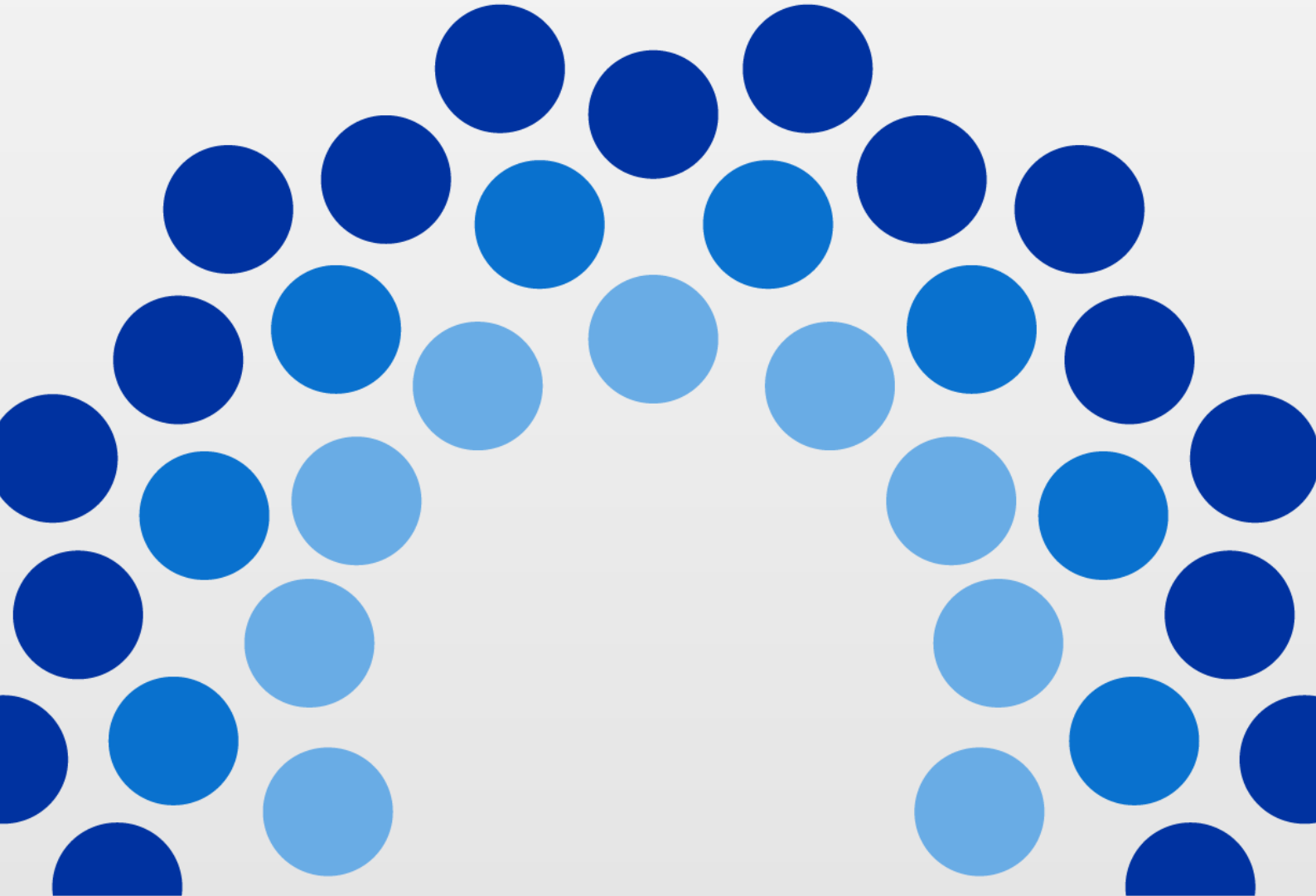
Sistema di Gestione della Sicurezza delle Informazioni di InfoCamere

Sintesi di politiche, processi e misure di sicurezza delle informazioni



Versione	2	Data Versione:	10 / 02 / 2022
Descrizione modifiche	Adeguamento delle politiche, dei processi e delle misure di sicurezza delle informazioni		
Motivazioni	Necessità di aggiornare le informazioni per le terze parti		
Struttura emittente:	Information Security Governance		

InfoCamere - Società Consortile di Informatica delle Camere di Commercio Italiane per Azioni

Capitale Sociale € 17.670.000 i.v.
Registro Imprese Roma, REA RM 804877
Codice Fiscale e Partita Iva 02313821007
Codice LEI 815600EAD78C57FCE690

Sede Legale
Via G.B. Morgagni 13 - 00161 Roma
T.+39 06 442851

Sede Operativa e Amministrativa
Corso Stati Uniti 14 - 35127 Padova
T +39 049 8288111
PEC: protocollo@pec.infocamere.it
www.infocamere.it

Precedenti emissioni

Versione	1.1	Data Versione:	19 / 11 / 2018
Descrizione modifiche	Seconda emissione		
Motivazioni	Correzione di un riferimento normativo		
Struttura emittente :	Sicurezza delle Informazioni e Privacy		

Indice

1 Introduzione al documento

1.1 Scopo e campo di applicazione del documento

Il documento ha lo scopo di informare i soggetti esterni interessati in merito ai contenuti delle politiche di sicurezza delle informazioni di InfoCamere, corredate da cenni su processi e particolari misure di sicurezza adottate.
Il documento è rivolto principalmente

- ai clienti e agli utenti dei servizi erogati da InfoCamere, in modo che possano conoscere quanto posto in atto da InfoCamere per garantire la sicurezza dei servizi erogati;
- ai fornitori di InfoCamere affinché garantiscano, a loro volta, un livello di sicurezza analogo nei servizi forniti.

I clienti e gli utenti dei servizi erogati da InfoCamere comprendono le Camere di Commercio, imprese, cittadini, Pubblica Amministrazione, Associazioni di Categoria, Ordini professionali, Operatori dell'informazione commerciale.
InfoCamere gestisce una rete informatica che collega le Camere di Commercio e due data center presso le sedi di Padova e Milano. InfoCamere progetta, sviluppa ed eroga servizi informatici, tra cui il Registro delle imprese telematico.

InfoCamere si è dotata di un Sistema di Gestione della Sicurezza delle Informazioni certificato secondo lo standard ISO/IEC 27001

Le principali informazioni relative ad InfoCamere sono disponibili sul sito www.infocamere.it.

1.2 Livello di riservatezza

	Livello	Ambito di diffusione consentito
X	Pubblico	Il documento può essere diffuso all'esterno dell'azienda.
	Uso interno	Il documento può essere diffuso solo all'interno dell'azienda. Le terze parti a cui viene comunicato, hanno l'obbligo di non diffusione.
	Riservato	Il documento **non può essere diffuso** all'interno dell'azienda. La sua visibilità è limitata ad un gruppo ristretto di persone. L'indicazione "Riservato" DEVE essere riportata anche nel Piè-di-pagina del documento.

1.3 Termini e definizioni

In questa sezione si riportano termini e definizioni particolari e specifici del documento.

Termine	Descrizione
Asset	Qualunque bene o informazione importante per il business aziendale
Cloud computing	Paradigma per abilitare l'accesso alla rete ad un pool scalabile ed elastico di risorse fisiche o virtuali condivisibili, con *provisioning* self-service e modalità di amministrazione concordata, che consiste in un modello flessibile per la fornitura di servizi ICT che consente un accesso più facile a risorse configurabili e condivise (rete fisica, risorse di *storage* e di processo, servizi e applicazioni per l'utente finale) attraverso tecnologie basate su Internet
Credenziali	Informazioni e strumenti utilizzati per richiedere il diritto di accedere ad una risorsa informatica. Esempi: userid/password, Certificati digitali, smartcard, token ...
Disponibilità	Proprietà dell'informazione di essere accessibile e utilizzabile quando necessaria.

Termine	Descrizione
	InfoCamere considera come “Disponibilità” l'accessibilità di dati, documenti elettronici e identità digitali per le camere di commercio, pubblica amministrazione e terzi.
Integrità	Proprietà dell’informazione di essere completa e esatta. InfoCamere considera come “Integrità” l’esatta rispondenza dei dati, documenti elettronici e identità digitali a quanto affidatole da camere di commercio, pubblica amministrazione e terzi.
Key Management	Gestione delle Chiavi - Regole di gestione delle chiavi in ambito crittografico, comprese la generazione, custodia, gestione dei dati di input ed output, conservazione, distruzione.
Minaccia (threat)	Causa potenziale di incidente, che può risultare in un danno per un sistema o un’organizzazione.
N.d.A.	Non-disclosure Agreement
PDCA	Plan Do Check Act – Modello di gestione ciclico
Riservatezza	Proprietà dell’informazione di essere nota solo a chi ne ha il diritto InfoCamere considera come “Riservatezza” la capacità di rendere accessibili dati, documenti elettronici e identità digitali esclusivamente a chi è autorizzato da camere di commercio, pubblica amministrazione e terzi, in conformità a leggi, regolamenti e contratti.
SGSI – ISMS	Acronimi per: - Sistema di Gestione della Sicurezza delle Informazioni (italiano) - Information Security Management System (inglese)
S.O.	Direzione, Struttura Organizzativa o Unità Operativa
SoA	Statement of Applicability – Dichiarazione di applicabilità dei controlli previsti dallo standard ISO 27001
Vulnerabilità (vulnerability)	Debolezza di un asset o gruppo di asset che può essere sfruttata da un attaccante.

2 Obblighi di rispetto delle Politiche

Le Politiche di Sicurezza costituiscono gli indirizzi della Direzione per il supporto della sicurezza delle informazioni in InfoCamere, il loro rispetto è obbligatorio per tutto il personale InfoCamere e viene idoneamente contrattualizzato con le terze parti pertinenti (chiunque acceda alle informazioni di InfoCamere a qualunque titolo).

2.1 Politica Generale di Sicurezza

In accordo con i requisiti di business, con le leggi e con i regolamenti pertinenti ad InfoCamere, viene definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti un insieme di politiche per la sicurezza delle informazioni.

- Viene contrattualmente previsto un impegno al rispetto delle Politiche di Sicurezza da parte dei clienti, fornitori e “terze parti”.
- Vengono definiti e rivisti periodicamente i requisiti per i *Non disclosure Agreement* [N.d.A.] e viene richiesto, in ogni contratto che comporti l'accesso da parte di 'terze parti' ad informazioni significative per il business, un modello di 'N.d.A.' per le terze parti, che prevede l'impegno a non divulgare informazioni riservate dell'Organizzazione.

Le politiche per la sicurezza delle informazioni devono essere riesaminate ad intervalli pianificati o nel caso in cui si siano verificati cambiamenti significativi nella legislazione applicabile, nella tecnologia utilizzata e in occasione di significative modifiche organizzative, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.

3 Organizzazione della Sicurezza delle Informazioni

InfoCamere intraprende l'attuazione e controlla l'esercizio della sicurezza delle informazioni all'interno dell'organizzazione.
Le responsabilità relative alla sicurezza delle informazioni vengono completamente definite e assegnate.
I compiti e le aree di responsabilità in conflitto tra loro sono separati per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset dell'organizzazione.

Vengono mantenuti appropriati contatti con le autorità pertinenti, inclusi gli organismi pubblici e privati nazionali ed internazionali che promuovono la sicurezza delle informazioni e le autorità di pubblica sicurezza.

Vengono mantenuti adeguati contatti con gruppi di interesse specialistico nell'ambito della sicurezza delle informazioni, con i “security forum” e le associazioni professionali, al fine di:

- migliorare la conoscenza aziendale sulle “*best-practices*” e mantenere l'aggiornamento in tema di sicurezza delle informazioni;
- assicurarsi che la comprensione delle tematiche di sicurezza delle informazioni in azienda sia aggiornata e completa;
- ricevere tempestivamente informazioni (*alert*, avvisi, patch da applicare) in merito a vulnerabilità, possibili attacchi e contromisure da applicare.

La sicurezza delle informazioni è indirizzata nell'ambito della gestione dei progetti, a prescindere dal tipo di progetto.

- I nuovi servizi informatici vengono valutati dal punto di vista della sicurezza delle informazioni dalle funzioni di sicurezza sin dalle prime fasi di sviluppo.
- I progetti di sviluppo software InfoCamere contengono specifici requisiti di conformità e sicurezza.
- Il rispetto dei requisiti di sicurezza nel software viene periodicamente verificato

4 Sicurezza delle Risorse Umane

InfoCamere adotta tutte le misure necessarie al fine di assicurare che il personale e i collaboratori siano a conoscenza delle loro responsabilità per la sicurezza delle informazioni e vi adempiano.

4.1 Prima dell'impiego

Le competenti funzioni si assicurano che nuovi dipendenti, collaboratori, personale a contratto o in genere destinato ad operare in azienda, siano adatti al ruolo che devono ricoprire e che abbiano compreso le loro responsabilità, al fine di ridurre il rischio di danneggiamenti o frodi.

Le funzioni aziendali competenti effettuano controlli per la verifica delle caratteristiche di idoneità su tutti i candidati all'impiego, in accordo con le leggi, con i regolamenti pertinenti e con l'etica. Tali controlli sono effettuati in proporzione alle esigenze di business, alla classificazione delle informazioni da accedere e ai rischi percepiti nell'impiego previsto.

Gli accordi contrattuali con il personale e con i collaboratori specificano le responsabilità loro e dell'organizzazione relativamente alla sicurezza delle informazioni.

4.2 Durante l'impiego

La direzione InfoCamere richiede a tutto il personale e ai collaboratori di applicare la sicurezza delle informazioni in conformità con le politiche e le procedure stabilite dall'organizzazione.

Tutto il personale InfoCamere e, qualora opportuno, i collaboratori esterni, ricevono un'adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività lavorativa.

InfoCamere prevede sanzioni nei confronti di chi commette una violazione delle regole previste nelle Politiche di sicurezza; le violazioni alle Politiche di Sicurezza sono sanzionate.

4.3 Al termine o in caso di variazioni dell'impiego

Le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o la variazione del rapporto di lavoro devono essere definiti, comunicati al personale o ai collaboratori e resi effettivi.

- Gli asset assegnati al personale devono essere restituiti in caso di cessazione del rapporto;
- Le autorizzazioni agli accessi devono essere rimosse in caso di termine del rapporto di impiego/collaborazione o modificati in caso di variazioni di appartenenza a strutture organizzative o incarico.

5 Gestione degli Asset

5.1 Responsabilità per gli asset

Le informazioni, gli altri asset associati ad informazioni e le strutture di elaborazione delle informazioni sono identificati; un inventario di questi asset viene pubblicato e mantenuto aggiornato, assieme agli strumenti tecnologici adottati a supporto e alle informazioni relative ai servizi di business ed agli asset tecnologici ad essi collegati.
Gli asset vengono censiti, catalogati e valutati in relazione alla loro importanza, quindi vengono assegnati ad un responsabile. Gli asset significativi vengono valutati, a intervalli pianificati, in base al valore, alle normative cui sono assoggettati, i requisiti di riservatezza, integrità e disponibilità, alla criticità per l'organizzazione.
L'utilizzo corretto degli asset assegnati al personale è specificamente regolamentato.

Le informazioni rilevanti sono classificate in modo da garantire che esse abbiano un adeguato livello di protezione. Sono previste linee guida per la classificazione delle informazioni, in dipendenza del loro valore, assoggettamento a normative specifiche, sensibilità e criticità per InfoCamere.

Si utilizza un appropriato sistema di 'etichettatura' e gestione delle informazioni in base alla loro classificazione.

5.2 Gestione dei supporti rimovibili

Sono sviluppate procedure per il trattamento dei supporti rimovibili e sono adottate idonee procedure per la dismissione dei supporti non più necessari in modalità sicure.

5.2.1 Trasporto dei supporti fisici

I supporti che contengono informazioni sono protetti da accessi non autorizzati, utilizzi impropri o manomissioni durante il trasporto.

6 Sistemi di sicurezza perimetrali

InfoCamere ha implementato nell'ambito dei propri DataCenter dei sistemi di sicurezza definiti "perimetrali", ovvero in uso per tutti i sistemi posti all'interno del DataCenter stesso, con particolare riferimento agli accessi da e per le reti internet; di seguito vengono descritti tali sistemi e la loro gestione.

7 Controllo degli accessi

InfoCamere limita l'accesso alle informazioni ed ai servizi di elaborazione delle informazioni secondo il criterio del "*need to access*" ovvero alle effettive e legittime necessità operative di ciascun soggetto.
InfoCamere emette specifiche Politiche in merito all'utilizzo delle workstation e dei dispositivi di elaborazione anche mobili individuali, dei servizi di posta e internet.
Inoltre InfoCamere pubblica una Politica di sicurezza sull'utilizzo e gestione delle credenziali di autenticazione nei sistemi informatici.

- Tutto il personale InfoCamere e le terze parti interessate vengono informati dell'esistenza di una Politica specifica per la gestione ed il controllo degli accessi logici alle risorse e vincolati, in dipendenza delle loro responsabilità o competenze, a rispettarne le prescrizioni.
- La strumentazione e le istruzioni per il controllo degli accessi vengono mantenute costantemente adeguate alle esigenze di business e di sicurezza degli accessi, anche in relazione alle evoluzioni organizzative e tecnologiche.

7.1.1 Gestione degli accessi alla rete ed ai servizi di rete

Agli utenti è consentito il solo accesso ai servizi ai quali sono stati specificatamente autorizzati.

- Vengono utilizzati appropriati metodi di autenticazione per controllare gli accessi al sistema da parte di utenti remoti;
- L'accesso fisico e logico alle "porte" di configurazione e diagnostica viene controllato;
- Separazione delle reti (sottoreti separate): gruppi (diversi) di servizi informatici, utenti e sistemi informativi sono separati nella rete;
- Per le reti condivise, specialmente quelle che si estendono oltre i confini dell'azienda, la capacità degli utenti di connettersi alla rete è limitata;
- Vengono implementati controllo relativi al *routing* per assicurarsi che le connessioni dei computer e i flussi di informazioni non violino la politica di controllo accessi delle applicazioni di business.

7.2 Gestione degli accessi degli utenti

7.2.1 Registrazione e de-registrazione degli utenti

InfoCamere prevede e attua una procedura formale per la registrazione e de-registrazione degli utenti, per garantire e revocare l'accesso a tutte le informazioni ed i servizi del sistema informatico.

InfoCamere prevede e attua un processo formale per l'assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi da essa erogati all'utenza.

- L'utilizzo delle password e, in genere, delle credenziali utente è controllato con un processo di gestione formale, anche automatizzato, fin ove possibile.
- I responsabili rivedono i diritti di accesso degli utenti ad intervalli regolari, utilizzando un processo formalizzato.

7.2.2 Accesso ai sistemi operativi

- L'accesso ai sistemi operativi è controllato da procedure di log-on.
- Tutti gli Utenti devono avere un identificatore unico (user ID) per il solo uso personale, e un'idonea tecnica di identificazione è utilizzata per assicurare l'asserita identità di un utente.
- I codici di identificatore unico, una volta utilizzati, non possono essere riassegnati a persone diverse, neppure a distanza di tempo.
- Sono attivi sistemi per assicurare un'adeguata qualità delle password.

7.2.3 Controllo degli accessi alle applicazioni ed alle informazioni

- L'accesso alle informazioni ed alle funzionalità dei sistemi applicativi da parte degli utenti e del personale di supporto viene limitato in base al principio di necessità.
- I sistemi critici per il business e la sicurezza delle informazioni devono disporre di ambienti e sistemi di elaborazione dedicati (isolati).

7.2.4 Elaborazioni su mobile e telelavoro

1. Vengono adottate misure di sicurezza adeguate a difesa dai rischi di utilizzo del 'mobile computing' e relative modalità di trasmissione e comunicazione.
2. Vengono adottate misure di sicurezza adeguate a difesa dai rischi inerenti le attività di Telelavoro.

7.2.5 Gestione dei diritti di accesso privilegiato

L'allocazione e l'utilizzo delle utenze e dei privilegi amministrativi è ristretto e controllato.

7.3 Responsabilità dell'utente

L'assegnazione di informazioni segrete di autenticazione è controllata attraverso un processo di gestione formale.
I responsabili degli asset o i responsabili dei rischi riesaminano a intervalli regolari i diritti di accesso degli utenti.
I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni vengono rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione.

7.3.1 Utilizzo delle informazioni segrete di autenticazione

Tutto il personale e le terze parti interessate:

- segue le politiche di sicurezza specifiche relative alle password e all'utilizzo di informazioni segrete di autenticazione in particolare non divulgando le proprie credenziali.
- Si assicura che le apparecchiature anche se non presidiate abbiano un'adeguata protezione al fine di proteggere le informazioni segrete, anche di autenticazione (possibilità di alterazione non autorizzata delle credenziali).

7.4 Limitazione dell'accesso alle informazioni

L'accesso a informazioni e funzioni di sistemi applicativi deve essere limitato secondo le politiche di controllo degli accessi:

1) Procedure di log-on sicure

Quando richiesto dalle politiche di controllo degli accessi, l'accesso a sistemi e applicazioni è controllato da procedure di log-on sicure.

2) Sistema di gestione delle password

I sistemi di gestione delle password sono interattivi e assicurano password di qualità.

3) Uso di programmi dì utilità privilegiati

L'uso di programmi di utilità che potrebbero essere in grado di aggirare i controlli applicativi e di sistema viene limitato ed è strettamente controllato.

4) Controllo degli accessi al codice sorgente dei programmi

Gli accessi al codice sorgente dei programmi sono limitati alle effettive necessità operative e consentiti ai soli utenti autorizzati.

8 Crittografia

A fine di assicurare un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni InfoCamere prevede l'utilizzo di idonei controlli crittografici.

Ove valutato necessario, con idonea analisi dei rischi incombenti sugli asset, sono attuati controlli crittografici per la protezione delle informazioni dalle minacce di violazione della riservatezza e dell'integrità dei dati, anche ai fini di "non ripudio" della autenticità degli stessi.

- Si considera la robustezza dell'algoritmo di crittografia in funzione della criticità dei dati.
- Gli algoritmi di crittografia e la lunghezza delle chiavi vengono valutati periodicamente in relazione alla normativa, alle raccomandazioni internazionali ed in relazione al livello di protezione richiesto. In particolare gli algoritmi deprecati vengono sostituiti con algoritmi ritenuti validi a livello internazionale.
- La crittografia è valutata come mezzo di protezione delle informazioni memorizzate su dispositivi removibili o apparati mobili di elaborazione.Si valutano inoltre i rischi di impossibilità di "ispezione" di dati cifrati per identificare eventuali malware.
- La trasmissione di informazioni critiche viene protetta attraverso la crittografia.

Sono previste, da parte delle funzioni responsabili degli asset protetti da controlli crittografici, idonee tecniche di protezione e viene stabilita la durata delle chiavi crittografiche attraverso il loro intero ciclo di vita.

- Sono definiti i metodi di gestione della generazione delle chiavi e delle procedure da adottare in caso di danneggiamento o perdita delle chiavi di decifratura, identificando i responsabili.

9 Sicurezza Fisica e Ambientale

InfoCamere intende assicurare gli asset rilevanti per il business e la sicurezza delle informazioni contro ogni rischio di danneggiamento, furto, perdita di riservatezza, eventi calamitosi naturali o atti dolosi. InfoCamere predispone idonee misure di controllo degli accessi fisici e regole di accesso per il personale e prevede la sicurezza nella gestione degli apparati acquisiti a salvaguardia della erogazione dei servizi tecnologici quali generatori di emergenza, impianti antincendi, anti-allagamento ed anti-intrusione, i quali richiedono un controllo periodico della collocazione e dello stato di efficienza dei beni in generale, degli impianti, delle macchine e delle attrezzature presenti, oltre che la pianificazione degli interventi di manutenzione degli impianti, dei macchinari, delle attrezzature e dei beni in generale e l'alienazione dei beni inutilizzabili in quanto obsoleti e/o non più riparabili.

InfoCamere, tramite apposita procedura, definisce il sistema delle autorizzazioni e le modalità operative per la gestione degli accessi e della permanenza nelle sedi di InfoCamere durante e al difuori del normale orario di servizio.
Sono disciplinati gli accessi da parte di:

- Dipendenti di InfoCamere;
- personale delle Società/Enti esterni nell'ambito dell'esecuzione di un contratto stipulato con InfoCamere;
- Visitatori-Ospiti occasionali;
- Ospiti abituali.

La procedura comprende:

- gli accessi a tutti i luoghi ed agli apparati inerenti alla sicurezza;
- le modalità di concessione e revoca delle autorizzazioni di accesso;
- le modalità di registrazione degli accessi;
- i controlli previsti.

9.1 Aree sicure

9.1.1 Perimetro di sicurezza fisica

Vengono definiti e utilizzati dei perimetri di sicurezza per proteggere le aree che contengono informazioni critiche e le strutture di elaborazione delle informazioni.

- Sono previsti controlli per assicurare che solo le persone autorizzate possano avere accesso all'interno del perimetro aziendale.
- I locali che contengono apparecchiature informatiche critiche per il business, soggette a specifiche normative, o archivi informatici contenenti dati sensibili, sono ad accesso ulteriormente controllato; le persone non specificamente autorizzate non possano accedervi.
- Sono previste misure di protezione fisica contro danneggiamenti esterni quali fuoco, acqua, terremoti, esplosioni, disordini, ed altri fenomeni disastrosi naturali o causati dall'uomo.

È progettata e applicata la sicurezza fisica agli uffici, ai locali e agli impianti. È prevista una apposita documentazione di Processo in tal senso.

È progettata e applicata un'adeguata protezione fisica da calamità naturali, attacchi malevoli o accidenti.

9.1.2 Lavoro in aree sicure

Sono progettate e attuate procedure per lavorare nelle aree sicure.

I punti di accesso, come le aree dì carico e scarico e altri punti attraverso i quali persone non autorizzate potrebbero accedere ai locali, devono essere controllati e, se possibile, isolati dalle strutture di elaborazione delle informazioni per evitare accessi non autorizzati.

9.2 Apparecchiature

InfoCamere attua specifiche procedure per prevenire la perdita, il danneggiamento, il furto o la compromissione di asset e l'interruzione delle attività operative dell'organizzazione. Le apparecchiature sono collocate in locali idoneamente predisposti al fine di proteggerle dai rischi derivanti dalle minacce e dai pericoli ambientali, oltre che dai rischi di accesso non autorizzato. Sono protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi/dispositivi ausiliari. L'accesso alle risorse dell'azienda è soggetto a politiche che richiedono l'utilizzo di dispositivi e reti sicuri, anche quando il personale lavora in smart working, in telelavoro o in mobilità.

I cavi per l'energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informativi sono protetti da intercettazioni, interferenze o danneggiamenti.

Le apparecchiature vengono correttamente mantenute per assicurare la loro continua disponibilità e integrità.

9.3 Trasferimento degli asset fuori dalle sedi aziendali

Apparecchiature, informazioni o software non devono essere portati all'esterno del perimetro aziendale senza preventiva autorizzazione. Sono implicitamente autorizzati i trasferimenti dei dispositivi mobili in dotazione individuale da parte dell'assegnatario, salvo le disposizioni specifiche in contrario.

Sono previste misure di sicurezza per gli asset collocati o trasportati all'esterno delle sedi dell'organizzazione, considerando i diversi rischi derivanti dall'operare all'esterno dei locali dell'organizzazione stessa. (Ad esempio: non vengono lasciate incustodite le apparecchiature al di fuori dell'azienda).

InfoCamere prevede una Politica specifica di sicurezza in tal senso.

Tutte le apparecchiature contenenti supporti di memorizzazione sono controllate per assicurare che ogni dato critico o il software concesso in licenza sia rimosso o sovrascritto in modo sicuro prima della dismissione o del riutilizzo.

Vengono adottate le politiche di "scrivania pulita" per i documenti ed i supporti di memorizzazione rimovibili e di "schermo pulito" per i servizi di elaborazione delle informazioni.

- Le regole di 'scrivania pulita' sono essenziali per proteggere le informazioni su cartaceo e su *storage* removibile:
    - Sulle scrivanie non viene tenuta (al termine del lavoro) in modo da essere accessibile a terzi alcuna documentazione riservata su supporto cartaceo o su dispositivi di memorizzazione removibili (hard disk removibili, CD, DVD, chiavette usb).
- Le regole "*clear screen* / *clear desk*" (protezione e rimozione delle informazioni a video facilmente visibili-utilizzabili da terzi non autorizzati) sono essenziali per proteggere tutte le risorse di elaborazione delle informazioni sia in utilizzo individuale (schermi su computer / laptop / mobile e altri dispositivi), sia condiviso (console di sistemi di controllo, server, *appliance*…):
    - Non è lasciata accessibile la stazione di lavoro durante la propria assenza: viene bloccata, prevedendo lo sblocco con password, e viene attivato comunque uno *screensaver* automatico protetto da password che pulisca la videata entro pochi minuti in caso di inutilizzo.
    - su *desktop* / *console*, durante lo svolgimento della propria attività, non devono essere facilmente visibili o accessibili informazioni riservate inutili per la corrente sessione di lavoro (ad esempio: lasciare aperto inutilmente un documento contenente informazioni sensibili, che possono essere inopportunamente lette da terzi alla ripresa anche regolare della sessione).

10 Sicurezza delle attività operative

InfoCamere intende prevenire la perdita, il danneggiamento, il furto o la compromissione di asset e l'interruzione delle attività operative dell'organizzazione. Sono Pubblicate Politiche specifiche in merito a:

- sicurezza dei sistemi di produzione;
- utilizzo e gestione dei Dispositivi mobili e stazioni di lavoro individuali;
- utilizzo e gestione dei log di Sicurezza ed AuditLog.

10.1 Procedure operative e responsabilità

InfoCamere intende assicurare che le attività operative nelle strutture di elaborazione delle informazioni siano conformi alle "*best-practices*" di sicurezza delle informazioni.
Vengono documentate e rese disponibili idonee procedure operative a tutti gli utenti che le necessitano.
I cambiamenti all'organizzazione, ai processi di business, alle strutture di elaborazione delle informazioni e ai sistemi che potrebbero influenzare la sicurezza delle informazioni sono controllati.
L'uso delle risorse è monitorato e messo a punto. Vengono effettuate proiezioni sui futuri requisiti di capacità per assicurare le prestazioni di sistema richieste.

10.1.1 Separazione degli ambienti di sviluppo, test e produzione

Gli ambienti di sviluppo, test e produzione vengono separati per ridurre il rischio di accesso o cambiamenti non autorizzati all'ambiente di produzione.

10.2 Protezione dal malware

Le informazioni di proprietà InfoCamere o da essa gestite e le strutture preposte alla loro elaborazione sono protette contro il malware.
Sono previsti ed attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware.

- Deve essere formato e promosso un idoneo grado di consapevolezza degli utenti per prevenire le minacce e le vulnerabilità derivanti dal malware.

10.3 Backup

Sono effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata.

10.4 Raccolta di log e monitoraggio

Sono registrati gli eventi rilevanti e vengono generate evidenze.
La registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni viene effettuata, mantenuta e riesaminata periodicamente.
Le strutture per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati.

10.4.1 Log di amministratori e operatori

Le attività degli amministratori e degli operatori di sistema sono registrate tramite log, e questi sono protetti e riesaminati periodicamente.

10.5 Sincronizzazione degli orologi

Gli orologi di tutti i sistemi pertinenti che elaborano informazioni all'interno di un'organizzazione o di un dominio di sicurezza vengono sincronizzati rispetto a una singola sorgente temporale di riferimento.

10.6 Controllo del software di produzione

L'integrità dei sistemi di produzione è un requisito di sicurezza essenziale per InfoCamere.

10.6.1 Installazione del software sui sistemi di produzione

Sono attuate procedure per controllare l'installazione del software sui sistemi di produzione.

10.7 Gestione delle vulnerabilità tecniche

A fine di prevenire lo sfruttamento di vulnerabilità tecniche viene reso obbligatorio quanto segue:

- le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo sin dalle prime fasi dello sviluppo o introduzione di nuovi sistemi in azienda;
- l'esposizione a tali vulnerabilità deve essere valutata e appropriate misure devono essere intraprese per affrontare i rischi relativi.

Vengono stabilite e attuate regole per il governo dell'installazione del software da parte degli utenti.

10.8 Considerazioni sull'audit dei sistemi informativi

I requisiti e le pianificazioni delle attività di audit che prevedono una verifica dei sistemi di produzione sono attentamente valutati e concordati per minimizzare le interferenze con i processi di business.

11 Sicurezza delle comunicazioni

11.1 Gestione della sicurezza della rete

InfoCamere emette specifica Politica di Controllo accessi alla rete.
Le reti sono presidiate e controllate adeguatamente e costantemente contro i tentativi di intrusione, intercettazione e attacco, al fine di proteggere le informazioni nei sistemi e nelle applicazioni.
I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione dei servizi di rete sono identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o siano affidati all'esterno.
Nelle reti vengono segregati gruppi di servizi, di utenti e di sistemi informativi a seconda del livello di rischio incombente sui relativi asset. Gli ambienti di sviluppo e produzione sono separati, definendo idonee sottoreti tra loro isolate o ad interconnessione controllata.

11.2 Strumenti impiegati

11.2.1 Firewall

A protezione perimetrale dei server è presente un cluster firewall. Di tale strumento è possibile evidenziare due differenti livelli di gestione, rispettivamente, sistemistico ed amministrativo:
• gestione sistemistica del firewall: il firewall, come sistema software, è soggetto ad aggiornamento di versione. L'aggiornamento viene effettuato in base alle raccomandazioni del produttore, per mantenerlo continuativamente in piena efficienza;
• gestione amministrativa del firewall: per gestione amministrativa si intende l'implementazione delle regole che permettono o negano l'accesso ai sistemi posti a valle del firewall, o l'accesso alla rete internet a partire dai sistemi stessi. Le regole vengono implementate in base alle necessità applicative su richiesta del Cliente, dopo valutazione comune di aderenza alle policy generali e di eventuali rischi di sicurezza che tali regole possono comportare.

11.2.2 Intrusion Prevention System

Un'ulteriore sistema di protezione perimetrale dei web server fornito da InfoCamere sui sistemi consiste nel un sistema di *Intrusion Prevention*, di seguito denominato IPS.
Nello strumento di IPS si evidenziano due differenti livelli di gestione, uno sistemistico e l'altro amministrativo:
• gestione sistemistica dell'IPS: l'IPS, come sistema software, è soggetto ad aggiornamento di versione. L'aggiornamento viene effettuato in base alle raccomandazioni del produttore, al fine di mantenerlo sempre in piena efficienza;
• gestione amministrativa dell'IPS: per gestione amministrativa si intende l'implementazione delle regole di analisi del traffico che hanno lo scopo di identificare possibili tentativi di violazione dei sistemi. L'aggiornamento di tali regole viene effettuato quando (tipicamente più volte al mese) il Fornitore ne rilascia un nuovo set. Gli aggiornamenti di regole vengono applicati automaticamente secondo le configurazioni raccomandate dal Fornitore, ed eventualmente intervenendo manualmente se dovessero emergere falsi positivi che bloccano le funzionalità applicative.

11.2.3 Sistema anti-DDOS

InfoCamere ha realizzato un sistema di difesa da attacchi informatici di tipo DDoS (*Distributed Denial of Service*) in grado di individuare e bloccare il traffico anomalo prima che questo arrivi alla connessione Internet del Cliente.
Per traffico anomalo si intende, in questo contesto, un flusso massiccio di richieste dolose provenienti da sorgenti distribuite e dirette verso uno dei servizi erogati, in grado di saturare la banda trasmissiva o la capacità elaborativa dei dispositivi di rete.
Una protezione efficace da attacchi di tipo DDoS richiede meccanismi di intercettazione del traffico doloso distribuiti nell'infrastruttura di rete del Fornitore di connettività (operatore TLC), in modo da poter intervenire il

più “a monte” possibile nei flussi che vanno dalle sorgenti degli attacchi ai loro obiettivi (che nel nostro caso sono posti all'interno dei datacenter InfoCamere).
In caso di allarme di questo tipo, segnalato dai sistemi di controllo di InfoCamere o da quelli dell'operatore TLC, il suddetto meccanismo DDoS prevede il dirottamento da parte dell'operatore stesso del traffico anomalo verso un sistema di “pulizia” del traffico, in grado di inoltrare ad InfoCamere il solo traffico “pulito”. Per evitare falsi allarmi, il processo di dirottamento non sarà attivato in modo automatico ma solo su richiesta esplicita di InfoCamere.

11.3 Trasferimento delle informazioni

Al fine di mantenere la sicurezza delle informazioni trasferite sia all'interno di InfoCamere che verso qualsiasi entità esterna è necessario quanto segue:

- InfoCamere prevede controlli a protezione del trasferimento delle informazioni, per tutte le tipologie di comunicazione.
- Devono essere formalizzati, in appositi accordi, i trasferimenti sicuri di informazioni di business tra l'organizzazione e le parti esterne.
- Le informazioni trasmesse attraverso messaggistica elettronica devono essere protette in modo appropriato in relazione al rischio ad esse relativo di intercettazione, alterazione, violazione di riservatezza.
- Sono previsti accordi di riservatezza o di non divulgazione (N.d.A.), in base alle necessità di proteggere le informazioni rilevanti per la sicurezza ed il business di InfoCamere nei contratti ed accordi con le terze parti.

12 Acquisizione, sviluppo e manutenzione dei sistemi

12.1 Requisiti di sicurezza dei sistemi informativi

InfoCamere intende assicurare che la sicurezza delle informazioni sia parte integrante di tutto il ciclo di vita dei sistemi informativi, inclusa la definizione dei requisiti specifici per i sistemi informativi che forniscono servizi, in particolare attraverso reti pubbliche: a tal scopo pubblica specifica Politica di sicurezza.
I requisiti relativi alla sicurezza delle informazioni sono incluse all'interno dei requisiti per i nuovi sistemi informativi o per l'aggiornamento di quelli esistenti.

12.2 Hardening

InfoCamere si è dotata di una Politica in materia di *hardening* dei Sistemi con l'obiettivo di definire le regole generali per il miglioramento e il mantenimento della massima efficienza dei Sistemi (server, dispositivi) gestiti da InfoCamere. Le indicazioni ivi contenute si applicano alle componenti di base (Sistema operativo), *Middleware* e strumenti/prodotti installati sui sistemi. Per quanto compatibili, le regole si applicano non solo ai server ma a tutti i sistemi in genere (inclusi dispositivi di rete, *appliance*) dotati di connessione in rete.
In alcuni casi possono essere necessari criteri più restrittivi di quelli esposti, specie in ambiti soggetti a requisiti normativi particolari.
Ciascuna struttura organizzativa tiene conto di queste indicazioni in fase di redazione delle istruzioni dettagliate di *hardening* per l'ambiente di propria competenza, indicando la corrispondenza tra le istruzioni e i requisiti indicati in questo documento.
Il rischio di danneggiamento di dati e sistemi informatici viene minimizzato da una corretta gestione di software di base, *middleware* e da un controllo sulla configurazione di tutti i dispositivi aziendali che intervengono nel trattamento di informazioni critiche.
L'*hardening* applicato al software di base e *middleware*, ovvero l'attività che consente il raggiungimento e mantenimento di un livello di sicurezza adeguato per i sistemi, è una componente indispensabile di questo processo.
Lo scopo della politica sull'accesso alla rete (Network Access Control) è quello di garantire la difesa dalle minacce informatiche degli asset InfoCamere o gestiti da InfoCamere e descrive regole di sicurezza specifiche per l'utilizzo e la gestione della rete da parte del personale InfoCamere e delle terze parti interessate.

Le informazioni trattate nei servizi applicativi sono protette al fine di prevenire trasmissioni incomplete, errori di instradamento, alterazione non autorizzata di messaggi, divulgazione non autorizzata, duplicazione non autorizzata di messaggi o attacchi.

12.3 Sicurezza nei processi di sviluppo e supporto

Le seguenti regole hanno il fine di assicurare che la sicurezza delle informazioni sia progettata e attuata all'interno del ciclo di sviluppo dei sistemi informativi.
Regole per lo sviluppo del software e dei sistemi che tengano conto dei rischi inerenti la sicurezza delle informazioni nelle fasi di sviluppo vengono stabilite e applicate al software sviluppato all'interno dell'organizzazione.
I cambiamenti apportati ai sistemi nel loro ciclo di vita sono tenuti sotto controllo attraverso l'utilizzo dì procedure formali di controllo dei cambiamenti.
Quando avvengono dei cambiamenti nelle piattaforme operative, le applicazioni critiche per il business sono riesaminate e sottoposte a test per assicurare che non ci siano impatti negativi sulle attività operative dell'organizzazione o sulla sua sicurezza.
La modifica dei pacchetti software viene disincentivata e limitata ai cambiamenti necessari; inoltre, tutti i cambiamenti devono essere strettamente controllati.

I requisiti per la progettazione e l'ingegnerizzazione di sistemi sicuri sono stabiliti, documentati, manutenuti e applicati ad ogni iniziativa di implementazione di un sistema informativo.
Sono definiti e protetti in modo appropriato gli ambienti di sviluppo dei sistemi e la loro integrazione, nell'intero ciclo di sviluppo.

Le strutture InfoCamere competenti supervisionano e monitorano l'attività di sviluppo dei sistemi affidata all'esterno.
Idonei test relativi alle funzionalità di sicurezza vengono effettuati durante lo sviluppo. Vengono stabiliti dei programmi di test e di accettazione dei sistemi ed i criteri ad essi relativi per i nuovi sistemi informativi, per gli aggiornamenti e per le nuove versioni.

Le regole elencate nelle politiche interne vengono tenute presenti fin dalle fasi di Disegno della Applicazione per poter trovare riscontro nei Requisiti imposti in fase di Specifiche, ed essere oggetto di Test prima del Rilascio delle Applicazioni realizzate in azienda o per l'azienda da terze parti.
Sempre più i Rischi connessi ad attacchi informatici tendono a sfruttare vulnerabilità presenti nelle applicazioni software. È necessario adottare idonee contromisure, che si applicano sin dalla fase di disegno e realizzazione del software.
Con riferimento ai rischi di seguito indicati, ed al fine di minimizzarli, il disegno e lo sviluppo delle applicazioni InfoCamere avvengono nel rispetto delle prescrizioni di sicurezza prestabilite e applicate al contesto di pertinenza.
Una storica top ten list dei rischi 'applicativi' (i più pericolosi e comuni errori nella scrittura di codice), aggiornata periodicamente nel sito OWASP, [TOP_10] può essere considerata la seguente:
***Parametri non controllati.** Le applicazioni usano le informazioni presenti nella richiesta HTTP per decidere come rispondere. Un attacco potrebbe avvenire modificando una qualsiasi parte della richiesta HTTP, l'URL, la querystring, gli headers, i cookies o i campi dei form.*
***Insufficiente Controllo degli accessi.** Il controllo degli accessi è una funzionalità di un'applicazione web che permette agli utenti l'accesso ad alcune risorse ma non ad altre: anche se presente può essere soggetto a debolezze.*
***Gestione insicura degli account e delle sessioni.** La gestione degli account e delle sessioni coinvolge una vasta gamma di processi, alcuni di basso livello, tipo l'autenticazione, la gestione degli utenti, la gestione delle sessioni attive, altri più evoluti, come le funzioni per il cambio di password e il recupero di password perdute. Le applicazioni web devono usare le sessioni per tenere traccia delle richieste di ogni utente, il protocollo HTTP non offre questa funzionalità e quindi ogni applicazione deve implementarla in qualche modo.*
***Cross Site Scripting (XSS).** Il cross-site scripting si verifica quando un'applicazione può essere usata per inviare codice maligno in esecuzione su un browser. Questo può avvenire in modo diretto o riflesso, un esempio potrebbe essere l'inserimento di codice javascript maligno all'interno di un messaggio di un forum, oppure sono potenziali vittime di XSS tutte le pagine che restituiscono direttamente una variabile ricevuta dall'utente. I problemi di sicurezza legati al XSS sono molto frequenti e difficili da identificare, però è importante eliminarli, perché il browser in caso di XSS concede allo script maligno i permessi del sito che lo ospita e questo potrebbe causare perdita di sicurezza e compromissione di dati sensibili.*
***Buffer Overflow.** Un buffer overflow compromette lo stack di esecuzione di un'applicazione e permette l'esecuzione di codice arbitrario sulla macchina vittima con i privilegi dell'applicazione. Anche se la tecnica è piuttosto complessa, esiste una vasta gamma di applicazioni sensibili a questi attacchi.*
***Iniezione di Comandi.** Gli attacchi di questo tipo agiscono inserendo codice all'interno dei parametri di chiamate a sistema e possono causare i più vari problemi. Ogni applicazione scritta in linguaggi interpretati, ogni applicazione che faccia uso di chiamate al sistema per l'esecuzione di programmi esterni, può essere soggetta a questo tipo di attacco. Oltre ai linguaggi di programmazione le iniezioni possono anche essere di codice SQL, che va ad alterare richieste a database; questo compromette ovviamente la sicurezza dei dati.*
***Problemi nella gestione degli Errori.** Una corretta gestione degli errori non espone informazioni sulla struttura interna dell'applicazione ad eventuali attacchi. Anche il semplice FileNotFound invece di un AccessDenied può essere un'informazione utile per un cracker, per non parlare degli stack trace dove vengono esposti parti di codice, nomi di files e cartelle.*
***Uso insicuro della crittografia.** Rischi connessi a problemi di questo tipo possono sorgere ogni qual volta un'applicazione ha bisogno di conservare informazioni sensibili. I punti principali in cui possono nascondersi degli errori sono: salvataggio insicuro di chiavi, certificati o password*

- *conservare in modo improprio dati segreti in memoria*
- *randomizzazione di bassa qualità*
- *algoritmi di bassa qualità*
- *mancata codifica dei dati veramente critici*
- *tentativo di inventare nuovi algoritmi di codifica*
- *errori nella procedura di recupero password perse*

***Amministrazione Remota insicura.** Diversi "application server" includono delle funzioni di amministrazione remota, spesso però a queste parti dell'applicazione non viene dedicata la particolare attenzione di cui*

avrebbero bisogno. Un accesso insicuro all'interfaccia di amministrazione può permettere a un intruso l'ingresso e la modifica di qualsiasi informazione o l'interruzione del servizio.
Configurazione del web server insicura. *La configurazione del web server e dell'application server giocano un ruolo fondamentale nella sicurezza di un'applicazione. Spesso amministratore di sistema e sviluppatore lavorano in due squadre diverse su due piani separati, i problemi connessi alla sicurezza spesso si trovano proprio in questo"spazio intermedio" di un sito, tra questi:*

- *programmi sul server non regolarmente aggiornati con patch di sicurezza*
- *server che permettono la lista delle directory o attacchi tipo path trasversale*
- *esempi o prove abbandonate sul server o backup non necessari visibili dall'esterno*
- *permessi errati su files e directory*
- *funzioni di debug amministrative accessibili*
- *messaggi di errore troppo informativi*
- *configurazione errata dei certificati SSL o della crittografia in generale*
- *uso di certificati auto-firmati o di default*

12.4 Dati di test

12.4.1 Protezione dei dati di test

I dati di test vengono scelti con attenzione, protetti e tenuti sotto controllo.

- InfoCamere valuta se proteggere con tecniche di "*data masking*" i dati riportati dall'ambiente di produzione in fase di test, attivando tali tecniche se i dati comportano significativi rischi di violazione di riservatezza.
- In ogni caso vengono riportati in test/sviluppo dall'ambiente di produzione solo i dati strettamente necessari per eseguire i test/collaudi.

13 Relazioni con i fornitori

13.1 Sicurezza delie informazioni nelle relazioni con i fornitori

InfoCamere intende assicurare la protezione degli asset dell'organizzazione accessibili da parte dei fornitori.

I requisiti di sicurezza delle informazioni per mitigare i rischi associati all'accesso agli asset dell'organizzazione da parte dei fornitori sono concordati con i fornitori stessi e documentati.

Tutti i requisiti relativi alla sicurezza delle informazioni sono stabiliti e concordati con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire informazioni e/o componenti dell'infrastruttura IT dell'organizzazione. Gli accordi con i fornitori includono i requisiti per affrontare i rischi relativi alla sicurezza delle informazioni e delle comunicazioni dei servizi e prodotti inclusi nella filiera di fornitura per l'ITC.

InfoCamere ricorre unicamente a fornitori che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, nominando questi ultimi, ove previsto, responsabili del trattamento dei dati personali, come prescritto dall'art. 28 del Regolamento (UE) 2016/679.

13.2 Gestione dell'erogazione dei servizi dei fornitori

InfoCamere verifica l'attuazione degli accordi con i fornitori per mantenere un livello concordato di sicurezza delle informazioni ed erogazione dei servizi.

InfoCamere monitorizza, riesamina e sottopone ad audit l'erogazione dei servizi da parte dei fornitori, relativamente al rispetto dei requisiti di sicurezza delle informazioni nella fornitura, ove applicabili.

I cambiamenti alla fornitura dei servizi da parte dei fornitori vengono gestiti tenendo conto della criticità delle informazioni, dei sistemi e dei processi coinvolti, basandosi su di una costante rivalutazione dei rischi.

14 Gestione degli incidenti relativi alla sicurezza delie informazioni

La gestione degli incidenti relativi alla sicurezza delle informazioni (nell'ambito del processo generale di gestione degli incidenti), incluse le comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza, è considerata essenziale da InfoCamere.

InfoCamere, nel proprio ambito di responsabilità, in accordo con le disposizioni di Politica specifica e nell'ambito del processo aziendale di gestione degli incidenti, opera per assicurare una risposta rapida, efficace ed ordinata agli incidenti relativi alla sicurezza delle informazioni.

Gli eventi relativi alla sicurezza delle informazioni vengono segnalati il più velocemente possibile attraverso appropriati canali gestionali.
È richiesto a tutto il personale e ai collaboratori che utilizzano i sistemi informativi e servizi dell'organizzazione di registrare e segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi.
Vengono valutati gli eventi relativi alla sicurezza e ne consegue la decisione sull'opportunità di classificarli come incidenti relativi alla sicurezza delle informazioni.

Si risponde agli incidenti relativi alla sicurezza delle informazioni in accordo con le procedure documentate.

La conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni è utilizzata per ridurre la probabilità o l'impatto degli incidenti futuri.

InfoCamere, nel proprio ambito di responsabilità, dà idonee istruzioni al personale per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze.

14.1 Fasi della gestione

Il processo di gestione dell'incidente prevede le seguenti fasi/azioni:

- Identificazione e Registrazione dell'incidente
- Presa in carico
- Diagnosi ed eventuale escalation
- Risoluzione
- Chiusura dell'incidente.

Il principale obiettivo del processo di "*Problem Management*" è l'identificazione delle cause primarie dell'Incident e conseguente adozione di misure atte ad impedire il ripresentarsi della malfunzione; adotta sostanzialmente fasi/azioni analoghe al processo di Incident Management.

Il processo di Incident e Problem Management, è formalmente definito e adottato da tutte le forze aziendali che concorrono alla continuità di erogazione del servizio. L'adozione di *best practices* e strumenti automatici per l'escalation funzionale e gerarchica, garantiscono un immediato innesco del processo.

Il team di Incident e Problem Management è da considerarsi punto di contatto persistente, relativamente a qualsiasi attività informativa sullo stato di evoluzione di un incidente o problema, mantenendo in tal modo i requisiti di agilità, efficacia e aderenza all'organizzazione aziendale.

14.2 Incidenti di sicurezza delle informazioni

La gestione degli incidenti di sicurezza può seguire percorsi diversificati, in base alla natura ed estensione dell'incidente:

- **Analisi segnalazione di sicurezza**, ovvero analisi di uno o più eventi di sicurezza correlati, che richiedono di essere valutati;
    - Se, in base all'analisi, si tratta di falso allarme, la segnalazione viene chiusa subito;
    - altrimenti l'evento di sicurezza diventa un incidente "confermato".
- **Gestione di un incidente di sicurezza**:
    - Se l'incidente è **elementare** (quando è richiesta l'applicazione di una contromisura standard contenuta in apposite istruzioni tecniche) l'incidente può essere gestito e chiuso rapidamente
    - altrimenti si aprono due percorsi alternativi:
        - **incidente di sicurezza "complesso",** che viene affrontato e risolto con un insieme di azioni prettamente in ambito tecnico/operativo;
        - **incidente di sicurezza "esteso"**, che, oltre ad un insieme di azioni tecnologiche, richiede il coinvolgimento di Responsabili "non tecnici" (Sicurezza, Privacy, Uff. legale, Risorse Umane …) per le eventuali azioni necessarie.
- **Revisione finale,** con emissione di un report periodico o (per gli eventi più gravi) specifico per il singolo evento, conclude la sequenza di passi operativi.

14.3 Gestione del Data-Breach

InfoCamere è dotata di una procedura che regola le modalità di attuazione delle norme relative ai casi in cui si verifichi una violazione di dati personali (c.d. data-breach).
In questo modo InfoCamere dà attuazione alle disposizioni contenute:

- ✓ nel **Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016** per la parte relativa alle prescrizioni di cui agli **artt. 33** - **Notifica di una violazione dei dati personali all'autorità di controllo** e **34** - **Comunicazione di una violazione dei dati personali all'interessato**;
- ✓ nel **Provvedimento del Garante della Privacy del 4 aprile 2013** "in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali" **(c.d. data-breach).**

Il processo di incident prevede casistiche che possono dare adito alla notifica di un data breach.

InfoCamere in tali casi, ove vi sia violazione di dati personali trattati per conto di un Titolare esterno, informa il Titolare del trattamento senza ritardo e collabora attivamente con il Titolare stesso, nella raccolta documentale e in tutte le attività connesse all'eventuale notifica al Garante Privacy e ai soggetti interessati, per quanto previsto nella normativa vigente.

15 Sicurezza delle informazioni nella gestione della continuità operativa

15.1 Continuità della sicurezza delle informazioni

La continuità della sicurezza delle informazioni è integrata nei sistemi per la gestione della continuità operativa dell'organizzazione.
L'organizzazione determina i propri requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in situazioni avverse, per esempio durante crisi o disastri.
Sono fornite idonee istruzioni al personale al fine di assicurare il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa.
InfoCamere verifica, ad intervalli di tempo regolari, i controlli di continuità della sicurezza delle informazioni stabiliti e attuati, al fine di assicurare che siano validi ed efficaci durante situazioni avverse.

Tutti i servizi del sito primario sono erogati in architettura logica e fisica di Alta Affidabilità e rispondono a stringenti requisiti di politiche di backup. Sono stati analizzati i fattori di rischio mettendo in atto le opportune e possibili contromisure. La zona è al livello minimo di rischio sismico e non ci sono evidenze di rischi da fenomeni naturali. Analoghi risultati emergono consultando le mappe della protezione civile, che non evidenziano situazioni di possibili rischi ad elevata probabilità e/o magnitudo.

InfoCamere inoltre dispone di un Data Center di Disaster Recovery a Milano.

15.2 Ridondanze

InfoCamere intende assicurare la massima disponibilità possibile, in accordo con gli SLA stabiliti con i clienti e le disposizioni applicabili, delle strutture per l'elaborazione delle informazioni.
Le strutture per l'elaborazione delle informazioni sono realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità.

16 Conformità alle disposizioni di legge e normative

InfoCamere intende evitare violazioni a obblighi normativi cogenti o obblighi contrattuali relativi alla sicurezza delle informazioni e dei requisiti di sicurezza stabiliti e prevede, tra l'altro alcune Politiche specifiche, rispettivamente in materia di

- Privacy
- Utilizzo di Posta Elettronica, Internet e servizi di Collaboration e Comunicazione
- Amministratori di Sistema

Alcuni servizi erogati da InfoCamere adottano ulteriori regole e misure di sicurezza previste da normative e standard specifici.

16.1 Conformità ai requisiti cogenti e contrattuali

Per ogni sistema informativo significativo per l'organizzazione e il business (per tutti i Servizi, in generale) vengono definiti e al contempo mantenuti aggiornati i requisiti cogenti e contrattuali pertinenti e l'approccio dell'organizzazione per soddisfarli. Vengono attuate delle procedure adeguate a garantire la conformità ai requisiti cogenti e contrattuali per l'uso del materiale sul quale potrebbero insistere diritti di proprietà intellettuale e per l'uso di prodotti software proprietari.
Le registrazioni sono protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato in conformità ai requisiti cogenti, contrattuali e di business.

InfoCamere cura l'adeguatezza delle misure di sicurezza (tecniche e organizzative) agli standard emanati con le "Misure minime di sicurezza ICT per le pubbliche amministrazioni", pubblicate in Gazzetta Ufficiale il 5 maggio 2017 (circolare AgID n. 2/2017 del 18 aprile 2017).

16.2 Privacy e protezione dei dati personali

Tutto il personale e terze parti interessate operano per assicurare la privacy e la protezione dei dati personali, come richiesto dalla legislazione e dai regolamenti pertinenti o applicabili. Tutto il personale è tenuto a rispettare le Politiche specifiche e le istruzioni in tema di Privacy.

InfoCamere pertanto si occupa di garantire l'esecuzione delle disposizioni del Reg. (UE) 2016/679 (GDPR) applicabili, in particolare:

- garantisce i diritti degli interessati previsti (art. 15 e ss.);
- prevede procedure che garantiscono l'effettiva attuazione dei principi di privacy "by design" e "by default" per le attività di trattamento di dati personali (art. 25);
- effettua la nomina dei responsabili del trattamento (art. 28);
- cura il proprio Registro dei trattamenti (sia in veste di titolare che in veste di responsabile) ai sensi dell'art. 30;
- effettua le valutazioni di impatto, ove richiesto, secondo quanto stabilito all'art.35;
- ha proceduto alla nomina del Responsabile della Protezione dei Dati (RPD o DPO) ai sensi dell'art. 37 e ss. del Regolamento Europeo suddetto (i riferimenti per contattare il RPD sono disponibili sul sito www.infocamere.it),

nonché le ulteriori disposizioni di carattere nazionale, previste dal D.Lgs 196/2003 e dai Provvedimenti dell'Autorità Garante per la protezione dei dati personali. In primo luogo, si menziona il Provvedimento "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" del 27 novembre 2008 così come modificato in base al provvedimento del 25 giugno 2009. A tal fine si è dotata di apposita procedura ed effettua un audit annuale sul rispetto delle indicazioni del provvedimento.

In accordo alla vigente normativa in materia di protezione dei dati personali, InfoCamere si è dotata inoltre in particolare di istruzioni specifiche per:

- Attuare il Provvedimento sugli Incaricati per sistemi di videosorveglianza;

- Attuare la normativa in tema di Sicurezza dei dati di Traffico Telefonico e Telematico;
- Gestire i diritti degli interessati previsti dal GDPR.

InfoCamere si impegna ad individuare, designare e controllare gli eventuali sub-responsabili del trattamento ai sensi dell'art.28 GDPR, imponendo loro gli impegni assunti con il Titolare del trattamento e fornire adeguata informazione a quest'ultimo riguardo alle attività di trattamento delegate a ciascun sub-responsabile

16.2.1 Impegni come responsabile del trattamento

InfoCamere, nei casi in cui effettua il trattamento in qualità di responsabile del trattamento, ai sensi dell'art. 28 del Reg. (UE) 2016/679, si fa carico di:

- trattare i dati personali secondo le istruzioni del Titolare del trattamento;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure di sicurezza tecniche e organizzative così come disciplinate dal Regolamento, tenendo conto in particolare del rischio per i diritti e le libertà delle persone fisiche;
- rispettare le condizioni previste dal Regolamento al fine di ricorrere ad un altro responsabile del trattamento;
- assistere il Titolare, tenendo conto della natura del trattamento, con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;
- assistere il Titolare del trattamento nel garantire il rispetto degli obblighi, previsti dal Regolamento, relativamente all'attuazione delle misure di sicurezza, alla comunicazione in caso di violazione dei dati personali e alla valutazione di impatto sulla protezione dei dati tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- cancellare e/o restituire, su scelta del Titolare, tutti i dati personali dopo che è terminata la prestazione dei servizi relativi a ciascun trattamento;
- mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal Regolamento;
- contribuire alle attività di verifica del rispetto del Regolamento, comprese le ispezioni, realizzate dal Titolare o da altro soggetto da questi incaricato.

16.3 Regolamentazione sui controlli crittografici

I controlli crittografici vengono utilizzati in conformità a tutti gli accordi, la legislazione e i regolamenti pertinenti.

16.4 Riesami della sicurezza delle informazioni

È indispensabile per InfoCamere assicurare che la sicurezza delle informazioni sia attuata e gestita in conformità alle politiche e alle procedure: a tal fine sono effettuati audit e controlli interni.
Il Sistema di gestione della sicurezza delle informazioni e i processi attuativi sono riesaminati in modo indipendente ad intervalli pianificati essendo InfoCamere soggetta, tra l'altro, a verifiche periodiche di riesame della sicurezza delle informazioni da parte di Enti Certificatori esterni, in quanto certificata secondo lo standard ISO27001.
I responsabili riesaminano regolarmente la conformità dei processi di elaborazione delle informazioni rispetto alle politiche, alle norme e a ogni altro requisito appropriato per la sicurezza.
I sistemi informativi sono regolarmente riesaminati per conformità con le politiche e con le norme per la sicurezza dell'organizzazione.
InfoCamere esegue ciclicamente le analisi dei rischi di sicurezza delle informazioni, in un'ottica di miglioramento continuo. I rischi identificati sono trattati con appositi piani di trattamento dei rischi che comprendono le misure tecniche e organizzative opportune da adottare.

17 Sicurezza delle informazioni e privacy nel cloud computing

InfoCamere ha esteso la certificazione ISO/IEC 27001 del proprio sistema di gestione della sicurezza delle informazioni secondo gli standard ISO/IEC 27017 e ISO/IEC 27018, con riferimento al settore del cloud computing.
I servizi erogati in modalità cloud computing, pertanto, oltre ai requisiti di sicurezza di cui allo standard ISO/IEC 27001, dove applicabile, rispondono anche a quanto prescritto dalle norme internazionali citate.