# Information Security Policy

## 1. Introduzione

Le caratteristiche operative di Inarcassa hanno portato l'Associazione a operare in un contesto molto vasto e complesso: le informazioni aziendali sono, ormai, quasi interamente gestite in forma elettronica e i sistemi informatici sono utilizzati da un numero crescente di persone, interne ed esterne, con una variabilità elevata di utenti e di collegamenti.
Questa realtà, se da un lato assicura la disponibilità di informazioni sempre aggiornate, dall'altro enfatizza il sorgere di rischi connessi alla loro protezione e controllo, che richiedono la presenza di misure idonee a rendere sicuro il patrimonio informativo.
Inarcassa ritiene prioritario assicurare la sicurezza delle informazioni nei sistemi e nei processi organizzativi connessi.
La confidenzialità, integrità e disponibilità delle informazioni gestite da Inarcassa costituiscono infatti caratteristiche critiche per la realizzazione della *mission* aziendale. Inoltre, tali caratteristiche possono costituire, in luce della normativa esistente, degli obblighi di natura cogente, soggetti ad attività di audit e la cui mancata tutela potrebbe risultare in sanzioni amministrative. La salvaguardia del patrimonio informativo aziendale è, dunque, una scelta strategica manageriale volta a consentire e favorire il raggiungimento degli obiettivi di business attraverso:

- la tutela delle risorse informative nel loro valore funzionale e reddituale;
- la garanzia della qualità del servizio, venendo incontro alla domanda di fiducia degli utenti e degli *stakeholder* interni ed esterni;
- la garanzia della continuità operativa, prevenendo l'interruzione delle funzioni minime di business in caso di incidente.

All'interno del presente documento vengono pertanto definiti:

- gli obiettivi di sicurezza;
- l'ambito di applicazione;
- i riferimenti normativi;
- i ruoli e le responsabilità per la sicurezza delle informazioni;
- i principi per la concreta realizzazione degli obiettivi di sicurezza;
- il processo per la gestione delle eccezioni a tali principi.

## 2. Obiettivi di sicurezza

Obiettivo principale in ambito Sicurezza delle Informazioni per Inarcassa è consentire, attraverso una sistematica attività di identificazione, valutazione e trattamento dei rischi, il raggiungimento di un adeguato livello di sicurezza nella gestione del patrimonio informativo, in termini di:

- riservatezza (accesso alle informazioni consentito unicamente alle persone autorizzate);
- integrità (garanzia di accuratezza e completezza delle informazioni e dei processi di trattamento / elaborazione delle stesse);
- disponibilità (accessibilità alle informazioni, da parte delle persone autorizzate, nel momento in cui ne hanno bisogno).

Una corretta gestione della Sicurezza delle Informazioni rappresenta inoltre un vantaggio rilevante per Inarcassa anche in termini di business, in quanto consente di conseguire ulteriori benefici / obiettivi, tra cui:

- ottimizzare gli investimenti per la Sicurezza delle Informazioni;
- tutelare e rafforzare l'immagine aziendale;
- aumentare la fiducia dei propri stakeholder e partner;
- ridurre l'incidenza di incidenti e violazioni di sicurezza;
- rispettare i vincoli normativi di livello nazionale ed internazionale;
- garantire un continuo aggiornamento delle proprie infrastrutture tecnologiche ed organizzative;
- garantire un continuo aggiornamento/revisione delle proprie policy e procedure aziendali;
- ridurre l'impatto di eventuali minacce sui servizi/asset;
- limitare i rischi di frode e corruzione.

Al tal fine, Inarcassa individua come elementi imprescindibili al raggiungimento degli obiettivi di tale sistema i seguenti principi:

- aggiornamento continuo dei rischi e conseguente analisi;
- coinvolgimento attivo e consapevole di tutto il personale interessato alle specifiche procedure in relazione al ruolo organizzativo esercitato;
- miglioramento evolutivo del sistema di individuazione e valutazione dei rischi;
- attività periodica di verifica e controllo dell'efficacia del sistema;
- coinvolgimento attivo e consapevole di fornitori e terze parti.

.

## 3. Ambito di applicazione

Il presente documento si applica, a vario titolo e con varie finalità, a tutte le Direzioni aziendali e, in generale, a tutto il personale dipendente di ogni livello, nonché ai soggetti terzi che, a qualsiasi titolo, svolgono, anche temporaneamente, attività di lavoro per Inarcassa (ivi inclusi fornitori, consulenti, partner).

## 4. Riferimenti

### Riferimenti Esterni

| ID | Titolo | Descrizione |
|---|---|---|
| [1] | **DPCM 27 gennaio 2014 - Strategia nazionale per la sicurezza cibernetica (Quadro strategico nazionale)** | Sostituito dal nuovo Piano nazionale adottato con DPCM 31 marzo 2017 |
| [2] | **DPCM 17 mar 2017 - Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali** | Piano nazionale per la protezione cibernetica e la sicurezza informatica |
| [3] | **ISO/IEC 27000:2018** | Information Technology - Security Techniques - Information security management systems - Overview and vocabulary |
| [4] | **ISO/IEC 27001:2022** | Information security, cybersecurity and privacy protection — Information security management systems — Requirements |
| [5] | **ISO/IEC 27002:2022** | Information security, cybersecurity and privacy protection — Information security controls |
| [6] | **D.Lgs. 30 giugno 2003 n. 196** | Codice in materia di protezione dei dati personali |
| [7] | **Regolamento Europeo n.679/2016** | Regolamento Europeo n.679/2016 sulla tutela e la protezione dei dati personali delle persone fisiche con riguardo al trattamento e la libera circolazione |
| [8] | **D.Lgs. 10 agosto 2018, n. 101** | Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio |
| [9] | **D.Lgs. 08 giugno 2001 n. 231** | Disciplina della Responsabilità Amministrativa del-le Persone Giuridiche, delle Società e delle Associazioni |
| [10] | **Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016** | Direttiva recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione |
| [11] | **Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015** | Misure minime di sicurezza ICT per le pubbliche amministrazioni |
| [12] | **NIST Cybersecurity Framework v1.1** | Linee guida sulla sicurezza informatica aiutando le organizzazioni a prevenire, rilevare e rispondere agli attacchi informatici |

**Riferimenti Interni**

Tutta la pertinente documentazione organizzativa e normativa vigente, applicabile a Inarcassa (disposizioni organizzative aziendali, policy aziendali, regolamenti, procedure, comunicazioni, modelli, etc.).

Nel caso eventuale in cui emerga un contrasto tra la presente policy (ivi incluse le procedure organizzative che ne conseguono) e le disposizioni organizzative aziendali (ruoli organizzativi, perimetri organizzativi e responsabilità assegnate), il soggetto che lo riscontra deve in ogni caso segnalarlo al Dirigente della UO Responsabile, al fine di valutare le modifiche ritenute più opportune ai fini diuna coerente armonizzazione. In attesa che queste siano formalizzate, prevalgono in ogni caso le disposizioni organizzative aziendali vigenti.

| ID | Titolo | Descrizione |
|---|---|---|
| [13] | **Raci Matrix** | Matrice dei ruoli e relative responsabilità in ambito sicurezza delle informazioni |
| [14] | **Policy per il corretto utilizzo delle risorse informative** | Disciplina l'utilizzo delle risorse informative |
| [15] | **Procedura per la gestione delle utenze** | Disciplina la gestione delle utenze |
| [16] | **Politica per la gestione del controllo accessi logici e delle password** | Descrive le politiche generali di accesso per le utenze informatiche standard e per quelle privilegiate |
| [17] | **Procedura per la Gestione delle Richieste di Cambiamento dei Sistemi Informativi** | Procedura per la Gestione delle Richieste di Cambiamento dei Sistemi Informativi |
| [18] | **Procedura di Vulnerability e Patch Management** | Procedura di Vulnerability e Patch Management |
| [19] | **Linee guida per lo sviluppo sicuro** | Fornisce delle linee guida per lo sviluppo di applicazioni informatiche sicure |
| [20] | **Procedura per la gestione dei fornitori** | Delinea le regole per profilare i fornitori ed eseguire la loro revisione di due diligence in conformità con la ISO27001 |
| [21] | **Procedura di gestione degli incidenti IT** | Descrive le procedure adottate da INARCASSA per consentire un approccio strutturato e sistematico alla gestione degli incidenti IT |
| [22] | **Politica per la definizione dei periodi di conservazione dei dati trattati (Retention)** | Definisce i periodi di conservazione dei dati trattati |
| [23] | **Processo di gestione delle nomine degli Amministratori di Sistema** | Gestione della nomina degli Amministratori di Sistema in conformità alla normativa vigente |
| [24] | **Procedura per il controllo degli accessi fisici** | Descrive le modalità di accesso ai locali ove si svolgono le attività aziendali |
| [25] | **Procedura di gestione del Ciclo di vita degli Asset IT** | Descrive il ciclo di vita di un asset IT |
| [26] | **Politica per la classificazione delle informazioni** | Definisce la metodologia da adottare per la classificazione delle informazioni trattate da INARCASSA |
| [27] | **Procedura di Log Management** | Delinea le linee guida per una corretta gestione dei log |
| [28] | **Politica sull'uso e sull'applicazione della crittografia** | Definisce le strategie e le regole per l'uso della crittografia al fine di garantire una gestione sicura delle informazioni |

| ID | Titolo | Descrizione |
|---|---|---|
| [29] | **Politica per il Backup e Restore dei dati** | Fornisce le linee guida e le best practice essenziali a garantire l'affidabilità dei sistemi IT attraverso le pratiche di Backup e Restore dei dati |
| [30] | **Procedura per la Gestione delle Utenze** | Definisce le modalità di gestione, le regole operative per la creazione e per l'assegnazione e la modifica dei profili autorizzativi informatici<br>tracciatura e la cessazione delle utenze, per l'assegnazione e la modifica dei profili autorizzativi<br>informatici e per l'abilitazione delle applicazioni ai ruoli |

## 5. Termini e Acronimi

| Termini | Definizioni |
|---|---|
| **SGSI** | Sistema di gestione della sicurezza delle informazioni. |
| **Sys Admin** | Amministratori di Sistema |
| **IT** | Information Technology |
| **DPIA** | Data Protection Impact Analysis |
| **Titolare del Trattamento** | Inarcassa, in qualità di soggetto che determina le finalità e i mezzi del trattamento dei dati personali dell'interessato rappresentata legalmente dal Presidente e la cui gestione amministrativa è attribuità al Consiglio di Amministrazione. |
| **GDPR** | General Data Protection Regulation |
| **DPO** | Data Protection Officer |
| **Responsabile Alta Direzione** | Il Presidente sovrintende il funzionamento di Inarcassa esercitando tutte le funzioni a lui demandate dallo Statuto, dalle altre fonti normative in materia, dal Consiglio di Amministrazione e dalla Giunta Esecutiva.<br>Il Direttore Generale dirige, coadiuvato dagli altri dirigenti, il funzionamento degli uffici di INARCASSA e svolge funzioni di sovrintendenza e di coordinamento |
| **Alta Direzione** | Il Direttore Generale e l'alta dirigenza che svolge compiti di sovrintendenza gestionale |
| **NDA** | Non-Disclosure Agreement |
| **BIA** | Business Impact Analysis |
| **SLA** | Service Level Agreement |
| **BC** | Business Continuity |
| **SDLC** | Software Development Life Cycle |

| Termini | Definizioni |
|---|---|
| **IDS** | Intrusion Detection System |
| **IPS** | Intrusion Protection System |

I requisiti e le responsabilità esplicitati nei successivi paragrafi sono pienamente allineate alle normative e alle direttive vigenti applicabili in materia, al fine di garantire il rispetto dei requisiti legali, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili.
Le attività di gestione della Sicurezza delle Informazioni in Inarcassa inoltre recepiscono le best practice e gli standard internazionali applicabili al contesto, al fine di assicurarne l'allineamento con le più recenti e consolidate tecniche di gestione e mitigazione del rischio cyber.

## 6. Ruoli e Responsabilità

La realizzazione delle misure di Sicurezza delle Informazioni, in conformità alla politica adottata, richiede la partecipazione attiva di tutti i collaboratori, oltre che la presenza di appropriate strutture organizzative specialistiche che indirizzino e coordinino le iniziative.
Tutti i ruoli aziendali e le relative responsabilità sono attribuiti in dettaglio, ai diversi livelli della struttura organizzativa di INARCASSA, all'interno del documento "Security Raci Matrix" [13].
Responsabilità e compiti specifici possono essere definiti nell'ambito di specifiche policy e procedure operative, referenziate nell'ambito del presente documento.

## 7. Principi per la concreta realizzazione degli obiettivi di sicurezza

Il presente capitolo fornisce principi da seguire per la concreta realizzazione degli obiettivi di sicurezza di Inarcassa nello svolgimento di tutte le attività dell'Associazione. Tali principi possono, in caso la complessità dell'argomento meriti un trattamento più ampio, essere rappresentati in documenti separati, referenziati all'interno degli specifici paragrafi.

### 7.1. Gestione del personale

- Tutto il personale aziendale, in particolare quello destinato a ricoprire ruoli di gestione della sicurezza, deve essere attentamente selezionato sulla base di criteri di affidabilità e competenza, in modo da limitare il più possibile il rischio di compromissione dell'integrità, della disponibilità e della riservatezza delle informazioni e delle risorse, cartacee ed informatiche, utilizzate ai fini del trattamento delle stesse.
- Devono essere previste azioni, sia periodiche, sia in concomitanza di eventi specifici (e.g. *on-boarding*, modifiche normative significative) per la formazione e la sensibilizzazione di tutto il personale in materia di Sicurezza delle Informazioni e sulle specifiche policy aziendali. È inoltre necessario valutare l'erogazione di formazione specialistica per il personale addetto alla sicurezza delle informazioni e per gli Amministratori di Sistema, al fine di assicurare che in azienda siano presenti tutte le competenze necessarie in ambito. Le attività di formazione e sensibilizzazione devono essere gestite nel rispetto della specifica Procedura di gestione della Formazione.
- Deve essere prevista una procedura formalmente definita per la gestione del termine del rapporto lavorativo con l'azienda e dei cambiamenti organizzativi che assicuri la tempestiva rimozione dei privilegi e la restituzione degli asset informativi.
- Le condizioni contrattuali stabilite nella definizione dei rapporti di collaborazione di qualsiasi natura devono dare comunicazione delle politiche e delle responsabilità relative alla sicurezza delle informazioni ed alla protezione dei dati.

- Devono essere predisposte idonee istruzioni per il personale aziendale contenenti indicazioni circa le modalità di corretto utilizzo delle Risorse Informative nonché le responsabilità, anche giuridiche, derivanti in caso di inosservanza [14].

### 7.2. Gestione degli asset

- Deve essere predisposto e costantemente aggiornato un inventario di tutti gli asset associati alle informazioni e di tutte le strutture di elaborazione delle informazioni. Tale inventario dovrebbe comprendere almeno le risorse software e le risorse hardware.
- Devono essere individuati i responsabili di riferimento per tutti gli asset censiti, incaricati di garantire l'inventariazione degli asset, di assicurare che siano adeguatamente protetti nonché che vengano dismessi secondo le procedure esistenti.
- Il personale, gli utenti e le terze parti devono utilizzare gli asset e le risorse aziendali nei limiti dell'autorizzazione assegnata e per esclusive finalità lavorative.
- L'utilizzo degli asset deve sempre ispirarsi ai principi di diligenza e correttezza che sono alla base di ogni atto o comportamento posto in essere nell'ambito del rapporto lavorativo e/o professionale, in coerenza con le vigenti previsioni normative, di contratto, procedurali, regolamentari e con le ulteriori disposizioni aziendali
- Devono essere predisposte idonee istruzioni per il personale aziendale contenenti indicazioni circa le modalità di corretto utilizzo delle Risorse Informative nonché le responsabilità, anche giuridiche, derivanti in caso di inosservanza [14]).
- Devono essere definite delle regole per l'assegnazione, utilizzo e riconsegna degli asset individuali [14].
- La protezione delle informazioni deve essere garantita durante tutte le fasi del ciclo di vita dell'asset che le contiene. Devono essere adottate precauzioni per la dismissione delle apparecchiature in conformità con la normativa vigente e secondo i principi di sicurezza. La dismissione degli asset deve avvenire in modo sicuro, assicurandosi che le informazioni siano state irreversibilmente distrutte [25].
- Le informazioni trattate nell'ambito delle attività di Inarcassa devono essere gestite e protette in base alla loro rilevanza e criticità. A tal fine, dovrebbero essere predisposte adeguate pratiche aziendali contenenti i criteri per la classificazione delle informazioni, in conformità della normativa vigente in materia di tutela del trattamento dei dati personali, e tenendo conto degli impatti conseguenti alla compromissione della confidenzialità, integrità e disponibilità [26].

### 7.3. Accessi logici [16] [30]

- Devono essere definiti specifici profili di autorizzazione per l'accesso alle informazioni da parte degli utenti del sistema informatico (personale aziendale, nonché dipendenti di imprese esterne e/o i consulenti cui l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali).
- I profili di autorizzazione devono consentire di individuare a quali informazioni l'utente può accedere nonché quali azioni può compiere. Al riguardo, le elaborazioni/operazioni devono essere limitate a quelle strettamente necessarie allo svolgimento delle mansioni assegnate, conformemente al principio del "*need to know*" e del "*least privilege*".
- In particolare, ai dipendenti di imprese esterne e/o ai consulenti deve essere consentito l'accesso alle informazioni aziendali solo ed esclusivamente in funzione del proprio incarico.
- Devono essere definite procedure di gestione e controllo del ciclo di vita dei profili di autorizzazione degli utenti, ivi inclusa assegnazione, creazione, aggiornamento, disattivazione e revoca.
- Devono essere definite specifiche politiche e procedure per l'assegnazione, la gestione ed il controllo dei profili ad elevati privilegi.

- Devono essere definiti standard, procedure ed istruzioni per la gestione delle credenziali di accesso in conformità alle normative vigenti, con particolare riferimento a quelle in materia di protezione dei dati personali.
- Il codice identificativo per le identità digitali aziendali (*user-id*) deve essere univoco e non riutilizzabile successivamente.
- Devono essere definiti standard per la complessità delle password. Devono essere inoltre definite le istruzioni idonee a rendere edotti gli utenti sullo standard di sicurezza da attuare in merito alla scelta ed all'utilizzo delle password e sulle cautele per assicurarne la segretezza.
- Tutti i diritti di accesso assegnati al personale aziendale, nonché ai dipendenti di imprese esterne e/o i consulenti cui l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali, devono essere regolarmente controllati ed aggiornati.
- Deve essere prevista la modifica/disattivazione dei diritti d'accesso in caso di revisione/revoca dei profili autorizzativi assegnati (ad esempio a seguito della cessazione del rapporto lavorativo).
- Il personale aziendale deve essere informato delle conseguenze, disciplinari e anche giuridiche, derivanti da un uso improprio (volontario o involontario) delle credenziali di accesso.
- Gli accessi a sistemi, reti ed applicazioni devono essere monitorati e regolarmente verificati.
- Devono essere adottati appropriati sistemi di autenticazione per il controllo degli accessi remoti alla rete.
- Devono essere attuati idonei controlli atti ad impedire l'accesso alla rete da parte di utenti non autorizzati.
- I sistemi devono essere configurati in modo da prevedere la chiusura automatica della sessione lavorativa dopo un periodo predefinito di inattività e la riattivazione della stessa solo previa autenticazione informatica.
- Per l'accesso ad informazioni e ad applicazioni particolarmente critiche è opportuno che l'identificazione avvenga tramite meccanismi di autenticazione dedicati proporzionati al livello di criticità dei dati ivi contenuti.
- Devono essere definite idonee procedure e controlli di sicurezza per proteggere le informazioni e le applicazioni dai rischi derivanti dall'utilizzo di computer portatili e di strumenti di comunicazione.
- Nel caso in cui si utilizzino soluzioni per il telelavoro devono essere definite ed attuate specifiche politiche e procedure di sicurezza.

### 7.4. Accessi fisici [24]

- Il perimetro di sicurezza delle aree deve essere chiaramente definito. Tutte le uscite di sicurezza del perimetro e le finestre non sorvegliate devono essere allarmate e tenute chiuse.
- Quando non presidiate, le aree devono essere tenute chiuse e controllate periodicamente.
- L'accesso fisico alle strutture aziendali deve essere controllato e consentito solo al personale previamente identificato ed autorizzato.
- Il personale che fornisce servizi di supporto e di manutenzione è autorizzato all'accesso nelle aree laddove necessario e in maniera limitata (anche temporalmente).
- I visitatori delle aree (ad esempio i dipendenti di imprese esterne e/o i consulenti) devono essere preventivamente identificati e registrati agli ingressi ed alle uscite delle sedi aziendali. Il loro accesso deve essere consentito solo per i compiti specifici e limitati alle attività di competenza.

- I diritti di accesso devono essere regolarmente verificati e revocati al personale aziendale o agli esterni (dipendenti di imprese esterne e/o consulenti) che lasciano gli incarichi per i quali era previsto l'ingresso alle aree stesse.

### 7.5. Sicurezza fisica e ambientale [24]

- Gli uffici e le stanze devono essere classificati e protetti in funzione della criticità delle risorse informative ivi trattate e custodite.
- L'accesso agli uffici ed alle stanze deve essere consentito solo al personale aziendale autorizzato ed ai dipendenti di imprese esterne e/o ai consulenti preventivamente identificati e registrati agli ingressi della sede aziendale.
- Gli strumenti di lavoro devono essere fisicamente protetti dai rischi di accesso non autorizzato e da conseguenti manomissioni o furti.
- Devono essere adottate adeguate precauzioni per la regolamentazione ed il controllo degli accessi agli strumenti da parte del personale autorizzato alla gestione/manutenzione degli stessi.
- Devono essere progettati ed implementati idonei sistemi di sicurezza fisica per la protezione ed il controllo delle aree sensibili (e.g. Data Center).
- Devono essere definite procedure organizzative per la gestione dell'accesso alle aree sensibili da parte del personale aziendale, dei dipendenti di imprese esterne e/o dei consulenti.
- Tutte le aree sensibili devono essere dotate di equipaggiamento di sicurezza come rilevatori di fumo e di fiamme, allarmi antincendio, controllo delle temperature, attrezzature per l'estinzione e uscite di sicurezza, sistemi antiallagamento, sistemi di protezione dalle interferenze nella fornitura elettrica e radiazioni elettromagnetiche.
- Tali equipaggiamenti devono essere controllati periodicamente per accertarne lo stato di conservazione e l'efficienza seguendo le istruzioni dei costruttori e dei responsabili preposti.
- Il cablaggio deve essere collocato in posizione priva di rischi dovuti a perdita di fluidi e/o disturbi elettromagnetici indotti da altri sistemi e tale da consentirne un'agevole e sicura manutenzione.

### 7.6. Sicurezza delle Attività Operative

- Le procedure operative inerenti ai processi di gestione dei sistemi informatici aziendali devono essere documentate, manutenute e rese facilmente disponibili a tutto il personale incaricato di attuarle.
- Qualsiasi modifica inerente ai sistemi e gli strumenti di gestione delle informazioni deve essere autorizzata, controllata, documentata, e deve tener conto delle esigenze della sicurezza *[17]*.
- Gli ambienti di sviluppo e collaudo devono essere separati da quelli di produzione al fine di ridurre al minimo i rischi di accessi o modifiche non autorizzate o anche accidentali dei sistemi operativi.
- Deve essere monitorato e messo a punto l'uso delle risorse affinché la disponibilità delle stesse non venga meno.
- L'integrità delle informazioni e delle risorse informatiche deve essere preservata dalla possibile compromissione da parte di software malevolo (ad esempio *virus*, *worm*, *trojan,* etc.).
- A tal fine, tutto il personale deve essere reso consapevole dei danni potenziali arrecati alle Risorse Informative aziendali dall'introduzione di software malevoli.
- I programmi antivirus devono essere gestiti e controllati in maniera tale da assicurarne una capillare diffusione ed un frequente aggiornamento.

- Devono essere definite idonee procedure atte a gestire gli eventi dannosi (isolamento, ripristino) ed a fornire supporto agli utenti coinvolti [21].
- Deve essere vietato l'utilizzo di software non espressamente autorizzato.
- Tutto il software installato sui sistemi informativi deve essere conforme ai brevetti e/o ai termini delle licenze (vincoli d'uso) ed utilizzato per esclusive finalità lavorative.
- Devono essere previsti periodici backup delle informazioni, anche in conformità agli obblighi normativi di natura cogente, al fine di preservare la disponibilità ed integrità dei dati aziendali (ad esempio in caso di manomissioni, atti vandalici, contaminazione da virus, perdita o distruzione anche involontaria).
- Deve essere previsto un meccanismo di raccolta e conservazione (per un periodo di tempo ritenuto idoneo in conformità degli obblighi di natura cogente) dei log degli eventi, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza.
- È inoltre necessario che i log raccolti vengano monitorati ai fini della verifica della corretta operatività dei sistemi e delle applicazioni ed al fine di rilevare eventuali comportamenti anomali, possibile indicazione di malware e/o attacchi mirati.
- Le strutture di raccolta dei log devono essere sicure e protette da manomissioni e accessi non autorizzati.
- Tutte le attività degli amministratori e degli operatori privilegiati devono essere sottoposte a log e devono essere esaminate periodicamente.
- Tutti i sistemi devono essere sincronizzati tramite protocollo Network Time Protocol.
- I controlli e le chiavi crittografiche devono essere gestite in conformità alle vigenti normative nazionali e agli standard internazionali [28].

### 7.7. Gestione delle vulnerabilità tecniche [18]

- Deve essere definito un processo di gestione delle vulnerabilità e delle relative patch così da garantire la valutazione dell'impatto e la tempestiva applicazione di azioni correttive.
- L'azienda deve ottenere in modo tempestivo le informazioni sulle vulnerabilità tecniche dei sistemi informativi sia eseguendo attività di scansione dei propri sistemi, sia partecipando a canali di information sharing con soggetti esterni.
- Deve essere definita una *timeline* per la gestione delle vulnerabilità che tenga conto dei possibili rischi ed esse associati e che scaturisca nell'applicazione di patch o altre misure correttive.

### 7.8. Sicurezza delle comunicazioni

- La sicurezza delle reti deve essere gestita e controllata per garantire la protezione delle informazioni nei sistemi e nelle applicazioni.
- A tal fine, tutta l'infrastruttura di rete deve essere protetta da accessi abusivi, tentativi di *tampering* e intercettazione.
- Dove applicabile, deve essere prevista la segregazione delle reti tra aree aziendali diverse.
- Laddove sia necessario consentire l'accesso remoto alla rete interna di Inarcassa tramite rete pubblica, devono essere impiegati protocolli comunicativi sicuri (e.g. VPN).
- Le informazioni scambiate attraverso reti pubbliche devono essere protette dai rischi di frode, accessi non autorizzati e alterazioni mediante adeguati controlli crittografici [28].

### 7.9. Ciclo di vita dello sviluppo sicuro e requisiti di sicurezza delle applicazioni

- L'acquisizione di nuovi sistemi o di parti di sistemi esistenti deve includere, in accordo con le necessità di business e le politiche di sicurezza aziendali, la definizione di specifici requisiti e controlli di sicurezza.

- Le applicazioni, sia commerciali sia sviluppate appositamente per Inarcassa, devono rispettare le politiche e gli standard di sviluppo sicuro aziendali [19].
- A seguito delle modifiche, le applicazioni critiche aziendali devono essere controllate e testate al fine di scongiurare eventuali malfunzionamenti dell'operatività e della sicurezza aziendale.
- Le modifiche ai pacchetti software devono essere limitate allo stretto necessario e, qualora effettuate, strettamente controllate.

### 7.10. Relazioni con i fornitori

- Nell'acquistare bene e servizi devono essere concordati e formalmente definiti i requisiti di sicurezza delle informazioni che i fornitori sono tenuti a rispettare [20].
- Devono essere previste specifiche clausole per garantire la riservatezza e la non-divulgazione delle informazioni aziendali critiche ed il rispetto del Copyright delle Risorse Informative accedute ed utilizzate dai soggetti terzi (fornitori, consulenti, partner), secondo quanto previsto dalle normative vigenti.
- L'erogazione di servizi da parte dei fornitori deve essere monitorata regolarmente, riesaminata e sottoposta ad attività di audit al fine di assicurare il rispetto delle policy di sicurezza e di quanto concordato nei contratti.
- Devono essere definiti contrattualmente con l'outsourcer, in accordo con le politiche, le procedure di sicurezza aziendali nonché le normative cogenti, i controlli da attuare per assicurare un adeguato livello di protezione delle informazioni trattate, i livelli di servizio da garantire ai fini della continuità operativa, nonché le relative responsabilità, anche giuridiche, derivanti in caso di inosservanza.
- Inoltre l'outsourcer dovrà essere informato sulle politiche, le procedure e le istruzioni di sicurezza aziendali relativamente al tipo di attività che dovrà svolgere in Inarcassa.

### 7.11. Gestione degli incidenti [21]

- Devono essere definite procedure per la gestione degli incidenti rilevanti ai fini della sicurezza delle informazioni in conformità alle vigenti normative nazionali ed aziendali ed alle *best practice* di riferimento.
- Tali procedure devono descrivere le finalità, le modalità, i criteri di protezione, di utilizzo ed i tempi di tenuta dei log rilevanti ai fini della ricostruzione degli incidenti.

### 7.12. Prontezza dell'ICT per la continuità operativa

- Deve essere predisposto un piano di continuità operativa aziendale. Tale piano deve descrivere i criteri, le procedure e gli strumenti adottati per la gestione delle emergenze e per il ripristino delle condizioni operative antecedenti il verificarsi di un evento dannoso.
- Devono essere pianificati dei test sulla base degli obiettivi di continuità operativa [29];
- Il piano deve, altresì, definire chiaramente le strategie di continuità del business, sulla base delle attività di analisi e gestione del rischio, rispetto ad eventi di indisponibilità delle informazioni e delle risorse informatiche.
  In tale ambito, si rimanda al documento del Piano di Continuità Operativa.

### 7.13. Intelligence sulle minacce

- Le informazioni relative alle minacce alla sicurezza delle informazioni devono essere raccolte e analizzate per produrre threat intelligence;
- Le informazioni sulle minacce esistenti o emergenti vengono raccolte e analizzate al fine di:
  - facilitare azioni basate su informazioni per prevenire che le minacce causino danni all'organizzazione;

- ridurre l'impatto di tali minacce.

### 7.14. Diritti di Accesso privilegiato [23]

- Deve essere predisposto un processo per gestire e limitare l'assegnazione e l'uso dei diritti di accesso privilegiato.

### 7.15. Cancellazione delle informazioni [22]

- Deve prevenire l'esposizione non necessaria di informazioni sensibili e conformarsi ai requisiti legali, statutari, normativi e contrattuali di cancellazione delle informazioni.

### 7.16. Attività di monitoraggio

- Deve essere predisposto il monitoraggio dei sistemi e delle applicazioni.
- Deve essere predisposta una procedura per la valutazione e gestione di potenziali incidenti relativi alla sicurezza delle informazioni [21].
-

### 7.17. Filtraggio web [14]

- Devono essere predisposte le regole per la navigazione web.
- Devono essere identificati i tipi di siti web a cui il personale dovrebbe o non dovrebbe avere accesso.

## 8. Gestione delle eccezioni

Tutte le eccezioni motivate alla presente policy devono essere preventivamente concordate con e formalmente autorizzate dal Responsabile della Funzione Sistemi Informativi.