REGIONE EMILIA-ROMAGNA
Atti amministrativi
GIUNTA REGIONALE

Atto del Dirigente DETERMINAZIONE

Num. 12807 del 03/08/2018 BOLOGNA

Proposta:	DPG/2018/13194 del 02/08/2018
Struttura proponente:	SERVIZIO ICT REGIONALE DIREZIONE GENERALE RISORSE, EUROPA, INNOVAZIONE E ISTITUZIONI
Oggetto:	DISCIPLINARE TECNICO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA E DATA BREACH
Autorità emanante:	IL DIRETTORE - DIREZIONE GENERALE RISORSE, EUROPA, INNOVAZIONE E ISTITUZIONI
Firmatario:	FRANCESCO RAPHAEL FRIERI in qualità di Direttore generale
Responsabile del procedimento:	Stefania Papili

Firmato digitalmente

'IL DIRETTORE'

Premesso che:

- Il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (di seguito Regolamento), è entrato il vigore dal 25 maggio 2018 ed è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri;
- tra le disposizioni ivi previste rilevano in particolare:
  - l'art. 33 che prevede l'obbligo di notifica di una violazione dei dati personali (c.d. data breach) al Garante per la protezione dei dati personali;
  - l'art. 34 che prevede l'obbligo di comunicare, in alcuni casi, le violazioni di dati personali anche agli interessati

Richiamato il Piano Triennale per l'informatica nella pubblica amministrazione 2017-2019 che dispone che tutte le Pubbliche amministrazioni sono tenute a monitorare e segnalare prontamente al CERT-PA gli incidenti informatici e ogni situazione di potenziale rischio, utilizzando i canali di comunicazione riportati nella sezione dedicata del sito AgID.

Vista la deliberazione di Giunta regionale n. 622/2017 "Approvazione della politica generale sulla sicurezza delle informazioni";

Vista la propria determinazione n. 7222 del 30/05/2012 avente ad oggetto "Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna";

Considerato che:

- per l’adempimento dell’onere di cui agli artt. 33 e 34 del Regolamento europeo n. 679/2016 occorre assicurare la corretta gestione degli incidenti di sicurezza e dei data breach;

- la gestione degli incidenti e dei data breach costituisce misura atta ad evitare o di minimizzare la compromissione dei dati dell’Ente in caso di incidente;

- il governo degli incidenti di sicurezza e dei data breach permette inoltre, attraverso l’analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell’incidente, di migliorare continuamente la capacità di prevenire incidenti a tutela della sicurezza dei sistemi e delle informazioni gestite dall’Ente;

Considerato che:

- il Servizio ICT Regionale ha avviato negli ultimi anni un percorso di certificazione del proprio Sistema di Gestione della Sicurezza Informatica, che si è concluso con il rilascio della Certificazione ISO 27001 in data 26/5/2017, rinnovato anche per l’anno 2018;

- nell’ambito del processo di Certificazione ISO 27001 sono state evidenziate alcune modalità di gestione delle informazioni e delle strumentazioni considerate idonee ad accrescere i livelli di sicurezza ed efficienza del sistema informativo regionale;

Ritenuto pertanto che sussista la necessità di aggiornare le disposizioni vigenti adottando un nuovo Disciplinare che risponda agli obiettivi, ai programmi e alle azioni precedentemente richiamati;

Vista la proposta elaborata dal Servizio ICT Regionale allegata al presente provvedimento e ritenuto che sia meritevole di approvazione;

Dato atto del parere positivo del DPO espresso in data 02/08/2018.

Dato atto che il responsabile del procedimento ha dichiarato di non trovarsi in situazione di conflitto, anche potenziale, di interessi;

Attestata la regolarità amministrativa del presente atto

D E T E R M I N A

1) di approvare l'allegato "Disciplinare tecnico per la gestione degli incidenti di sicurezza e data breach", che sostituisce integralmente la determinazione n. 7222/2012;
2) di disporre la pubblicazione del Disciplinare nell'apposita sezione Privacy di Orma nonché la notifica alle strutture regionali e agli Enti interessati;

Disciplinare tecnico per la gestione degli incidenti di sicurezza e data breach

INDICE

1. Scopo ed obiettivi

Con il presente Disciplinare si definisce la policy della Regione Emilia Romagna allo scopo di regolamentare la gestione degli incidenti di sicurezza informatica che possono occorrere ai servizi ed ai dati gestiti.

Tale policy mira alla corretta gestione degli incidenti di sicurezza che è misura che consente di evitare o di minimizzare la compromissione dei dati dell'organizzazione in caso di incidente; permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti.

Inoltre, con specifico riferimento all'obbligo di cui all'art. 33 del Regolamento europeo n. 679/2016 (di seguito Regolamento o GDPR), il presente documento individua quali siano le violazioni che ricadono nell'ambito della suddetta normativa, i casi in cui l'Ente deve notificare i data breach al Garante per la protezione dei dati personali (di seguito anche Garante) ed agli interessati, le misure atte a trattare il rischio e la documentazione da produrre.

Si rappresenta che l'art. 32 del Regolamento dispone che devono essere approntate misure tecniche e organizzative adeguate a garantire un livello adeguato di sicurezza dei dati personali. Individuare, indirizzare e segnalare tempestivamente un incidente di sicurezza, come una violazione di dati, è espressione dell'adeguatezza delle misure implementate dall'Ente.

Il Piano Triennale per l'informatica nella pubblica amministrazione 2017-2019 dispone che tutte le Pubbliche amministrazioni sono tenute a monitorare e segnalare prontamente al CERT-PA gli incidenti informatici e ogni situazione di potenziale rischio, utilizzando i canali di comunicazione riportati nella sezione dedicata del sito AgID.

Il presente atto definisce principi, attori e regole per la gestione degli incidenti di sicurezza e data breach, la cui specifica e peculiare implementazione è demandata ad apposita Procedura, formulata con un separato documento (di seguito, "Procedura").

2. Campo di applicazione

Con riferimento ai soli incidenti di sicurezza, l'ambito di applicazione del presente disciplinare è rappresentato dai servizi sistemistici infrastrutturali e applicativi tecnologicamente gestiti dalle strutture della Giunta Regionale.

Con riferimento ai casi di data breach, l'ambito di applicazione del presente disciplinare è determinato dalla titolarità dei trattamenti dei dati personali in capo alla Giunta Regionale effettuati a mezzo dei servizi.

Vengono presi in considerazione incidenti che possono scaturire attraverso sia l'azione di un attacco informatico portato da elementi esterni all'organizzazione sia generati da un eventuale

comportamento negligente o scorretto, di natura ostile con obiettivi frodatori da parte di un collaboratore dell'ente Regione Emilia Romagna.

L'obbligo di cui agli artt. 33 e 34 del Regolamento trova applicazione nei soli casi in cui la violazione riguardi dati personali, come definiti dall'art. 4 n. 1).

Tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

3. Cos'è un incidente di sicurezza

Ai sensi del presente documento, per incidente di sicurezza deve intendersi la violazione, la minaccia imminente di violazione di una policy di sicurezza informatica, di politiche di utilizzo accettabili o di prassi standard di sicurezza, correlato ad una violazione di dati o informazioni[1].

Esempi di incidenti sono:

> Un utente malintenzionato esegue comandi di botnet al fine di inviare un numero elevato di richieste di connessione ad un server web, provocandone l'arresto anomalo
> Gli utenti sono indotti ad aprire un file allegato alla mail che in realtà è un malware; l'esecuzione del tool ha infettato i pc e stabilito connessioni con un host esterno
> Un utente malintenzionato ottiene dati sensibili e minaccia di utilizzarli illecitamente

4. Cos'è un data breach ai sensi del GDPR

Il regolamento definisce la violazione dei dati personali come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Le violazioni declinate dalla norma sono sintetizzabili come

> **"Violazione della riservatezza"**, che si ha in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.
> **"Violazione dell'integrità"**, che si ha in caso di alterazione non autorizzata o accidentale dei dati personali
> **"Violazione della disponibilità"**, che si ha in caso di perdita o distruzioni di dati personali o di impossibilità di accesso ai dati personali da parte di soggetti autorizzati

Va sottolineato che una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione di queste.

Gli effetti di una violazione possono causare danni fisici, materiali o immateriali, ovverosia la perdita del controllo degli interessati sui propri dati personali, la limitazione dei loro diritti,

1 NIST Special Pubblication 800-61R2

discriminazione, furto d'identità o frode, perdita finanziaria, inversione non autorizzata di pseudonimizzazione, danno alla reputazione e perdita di riservatezza dei dati personali protetti dal segreto professionale. Può anche includere qualsiasi altro significativo svantaggio economico o sociale per gli interessati.

5. Quando effettuare la notifica al Garante e la comunicazione agli interessati

5.1 La valutazione del rischio per i diritti e le libertà delle persone fisiche

In caso di data breach l'Ente deve valutare i rischi per i diritti e le libertà delle persone fisiche, registrando le evidenze di tale analisi.

Nell'eventualità che tale valutazione rappresenti elementi di rischio per i diritti e le libertà delle persone fisiche l'Ente effettua la notifica delle violazioni di dati personali al Garante.

La valutazione è effettuata dal Data protection officer.

Quando le violazioni di dati comportano un rischio che viene valutato come elevato per i diritti e le libertà delle persone fisiche, le stesse devono essere comunicate agli interessati senza ingiustificato ritardo, fornendo loro specifiche informazioni in ordine alle salvaguardie che devono adottare per proteggere loro stessi dalle conseguenze della violazione.

Questo rischio esiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone i cui dati sono stati violati. Tale rischio è presunto quando il data breach riguarda le categorie particolari di dati di cui all'art. 9 del GDPR.

I criteri che devono guidare la valutazione del suddetto rischio sono i seguenti:

la tipologia di violazione
la natura dei dati violati
il volume dei dati violati
il numero di individui cui si riferiscono i dati violati
caratteristiche speciali degli individui cui si riferiscono i dati violati
il grado di identificabilità delle persone
la gravità delle conseguenze per gli individui

L'assessment è condotto secondo la metodologia indicata in apposita Procedura.

5.2 Il termine per effettuare la notifica

L'Ente notifica la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è stata rilevata. Oltre tale

termine, la notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni sono fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il termine inizia dal momento in cui l'Ente raggiunge un ragionevole grado di certezza che si è verificato un incidente di sicurezza che ha compromesso i dati personali.

L'Ente può tardare la notifica al Garante, nei casi in cui tale notifica possa produrre effetti negativi sugli individui.

La notifica al Garante viene, comunque, effettuata anche nei casi in cui l'Ente disponga di informazioni solo parziali della violazione.

Il Garante può richiedere, in ogni caso, la notifica della violazione agli interessati.

La comunicazione della violazione agli interessati può essere ritardata nei casi in cui tale comunicazione possa pregiudicare le indagini su cause, natura e conseguenze della violazione, anche su indicazione delle varie Autorità di controllo.

L'Ente utilizza lo strumento più efficace affinché tale notifica sortisca il maggiore effetto possibile.

6. Notifica al Cert-Pa

Il CERT-PA (Computer Emergency Readiness/Response Team, ovvero "squadra per la risposta ad emergenze informatiche" a supporto dei sistemi informatici della Pubblica amministrazione), organismo operante all'interno dell'AgID, supporta le Pubbliche amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica del dominio costituito dalle Pubbliche amministrazioni. Il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019, nelle Linee di azione, individua la segnalazione di incidenti informatici al Cert-PA.

L'Ente, pertanto, sia in caso di incidenti di sicurezza che di data breach informa, nelle modalità previste, il Cert-PA o organismo equivalente.

7. Ruoli e responsabilità

La criticità del processo di gestione degli incidenti di sicurezza informatica e del data breach deve essere opportunamente affrontata da una struttura operativa competente, in possesso di adeguata formazione ed in grado di prendere rapidamente le decisioni imposte dalla delicatezza del compito assegnato.

7.1 Il gruppo di Gestione Operativa della Sicurezza ICT (GOS-ICT)

E' istituito il gruppo per la Gestione Operativa della Sicurezza ICT (GOS-ICT) con le seguenti competenze:

- rappresentare il punto di riferimento e coordinamento univoco;

- gestire tutte le attività inerenti l'analisi e la gestione di un incidente di sicurezza, ivi comprese quelle relative alla sua notifica e documentazione;
- garantire la disponibilità delle liste di contatti (es.: personale dipendente, collaboratori, fornitori), necessarie per la gestione di un incidente di sicurezza;
- garantire che il processo di gestione incidenti sia sempre adeguato alle esigenze dell'ente, provvedendo che sia sempre aggiornato:
  - a seguito di cambiamenti tecnologici, infrastrutturali e organizzativi;
  - a fronte di incidenti di sicurezza che mettano in evidenza aspetti di miglioramento nella Procedura stessa.

La struttura GOS-ICT è composta dalle seguenti figure regionali di riferimento:

- Responsabile della Gestione della Sicurezza Informatica (coordinatore)
- Responsabile dell'Infrastrutture ICT
- Responsabile dei Servizi Autenticazione/Autorizzazione
- Responsabile delle Applicazioni
- Responsabile del supporto gestione PdL
- Dirigenti del Servizio ICTR

Il Responsabile della Gestione della Sicurezza Informatica assume il ruolo di Incident Handling Leader, ovvero la figura che ha in carico la gestione degli incidenti descritta nella relativa Procedura. In caso di non disponibilità di questi o di gestione concomitante di più incidenti tale responsabilità è assegnata ad altro membro del Gruppo GOS-ICT.

Nel corso del processo di gestione di un incidente di sicurezza informatico e, eventualmente, di un data breach, il gruppo GOS-ICT potrà essere coadiuvato di volta in volta da amministratori di sistema, personale della struttura i cui dati sono stati oggetto di data breach, da tutti coloro che il gruppo GOS-ICT riterrà necessario coinvolgere a seconda della tipologia di incidente e della tipologia di dati coinvolti, ivi compresi i responsabili della sicurezza eventualmente designati da strutture che, dotate di autonomia, ricadono nel perimetro di applicazione del disciplinare.

Nelle attività del gruppo GOS-ICT deve essere coinvolto il Data protection officer, il quale esercita le proprie funzioni di monitoraggio della conformità anche in caso di data breach, fornendo il proprio parere in ordine alla necessità di effettuare la notifica e, quindi, sulle valutazioni di cui al par. 5.1 e 5.2 del presente documento.

In tutti i casi in cui sia riscontrato un'ipotesi di incidente di sicurezza il Responsabile del Servizio ICTR, o in sua assenza uno dei componenti del Gruppo GOS-ICT, attiva la struttura GOS-ICT.

Il Responsabile del Servizio ICTR segnala al Direttore Generale competente in materia di sistemi informativi le violazioni dei dati personali ai fini della notifica al Garante, ai sensi dell'art. 33 del

Regolamento; la notifica della violazione di dati al Garante per la protezione dei dati personali deve ricomprendere anche i riferimenti del DPO.

I responsabili delle applicazioni devono, in caso di incidente o data breach, informare senza indugio il GOS-ICT per la gestione degli incidenti di sicurezza, sia per le applicazioni installate presso il datacenter dell'amministrazione sia usufruiti come sas.

7.2 Interazione con altre strutture

Nel caso in cui l'incidente abbia impatti significativi sull'erogazione dei servizi possono essere coinvolte le Strutture di Comunicazione della Giunta Regionale, sia per le comunicazioni interne, che per quelle rivolte all'esterno.

Nel caso, durante la gestione dell'incidente, emergano responsabilità da parte di personale interno dell'Ente occorre coinvolgere la Struttura regionale competente in materia di Personale.

Nei casi in cui gli amministratori di sistema siano causa diretta o indiretta di incidente di sicurezza per aver tenuto un comportamento gravemente negligente o in palese contrasto con le policy di sicurezza della Regione Emilia-Romagna, sono cautelativamente privati dei privilegi amministrativi sui sistemi, fintantoché non siano accertate eventuali responsabilità in sede di procedimento disciplinare. La gravità della violazione delle policy di sicurezza viene valutata tenendo conto anche del parere delle figure coinvolte nella gestione dell'incidente. Tale valutazione, che terrà conto anche del danno provocato all'amministrazione, costituisce criterio per la definizione della sanzione disciplinare applicabile e dell'eventuale revoca definitiva dell'incarico di amministrazione di sistema.

Nel caso, durante la gestione dell'incidente, emergano responsabilità da parte dei soggetti fornitori dovranno essere valutate le eventuali azioni nei loro confronti.

In tutti casi sopra menzionati, è il Responsabile del Servizio ICTR, su proposta dell'Incident Handling Leader, che coinvolge le strutture regionali competenti.

Tutti gli utenti del sistema informativo regionale direttamente oppure tramite collegamento remoto sono tenuti ad osservare i principi contenuti nella presente policy ed a segnalare in modo tempestivo la presenza di condizioni che possano indurre a valutare delle anomalie riconducibili ad attacchi informatici oppure a comportamenti scorretti.

7.3 Interazione con organismi esterni

Nel caso in cui le attività di analisi dell'incidente informatico risultino di difficile soluzione oppure nell'ipotesi in cui la valutazione della portata degli impatti generati dall'evento si estenda al di fuori del campo di applicazione del presente disciplinare può essere di supporto consultare organismi esterni.

A titolo non esaustivo si riporta il seguente elenco:

- CERT-ITA o CERT-PA (Computer Emergency Response Team di riferimento nazionale oppure

specifico al settore della Pubblica Amministrazione) oppure altre strutture analoghe per ottenere informazioni e supporto nell'analisi di incidenti che sfruttano vulnerabilità complesse;

- provider dei servizi di connettività geografica in caso di riscontro di attacchi di tipo DoS (Denial of Service) oppure per ottenere informazioni sull'attaccante nel caso di intervento della Polizia Giudiziaria;
- provider di servizi o piattaforme erogati in modalità Cloud Computing nell'ambito regionale;
- autorità di pubblica sicurezza nel caso in cui l'incidente possa presentare risvolti dal punto di vista penale.

Le richieste di attivazione di collaborazione con organismi esterni sono effettuate dal Responsabile del Servizio ICTR, o delegato.

In caso di data breach il punto di contatto con il Garante è costituito dal Data protection officer.

In ragione del fatto che un incidente (o data breach) può avere origine o, comunque, coinvolgere sistemi che soggetti fornitori gestiscono (o che concorrono a gestire), nei contratti di affidamento devono essere esplicitamente disciplinati oneri e responsabilità di tali Soggetti, ivi compresa l'interazione che gli stessi devono avere con l'Ente nella gestione dell'incidente/data breach.

1. Contestualizzazione

Pur non essendo regolamentata da normative specifiche la gestione degli incidenti di sicurezza informatica è definita accuratamente in alcune linee guida e standard di settore a carattere internazionale, tra cui si possono annoverare:

- il NIST (National Institute of Standard & Technologies) americano attraverso la pubblicazione SP-800-61R2 - "Computer Security Incident Handling Guide";
- l'agenzia emanazione della Commissione Europea ENISA (European Network Information Security Agency) con la pubblicazione "Good Practice Guide for Incident Management";
- lo standard ISO/IEC 27035:2011 "Information technology — Security techniques — Information security incident management";
- Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- Piano Triennale per l'informatica nella pubblica Amministrazione 2017-2019

La Regione Emilia-Romagna ha stabilito di conformarsi a questi standard e best practice sia per il suo ruolo istituzionale che per ridurre i possibili impatti derivanti dagli eventi avversi ed in costante

aumento associabili ad un incidente di sicurezza informatica.

9. La prevenzione degli incidenti

Vi sono comportamenti, attività e regolamenti che ogni organizzazione deve necessariamente attivare per cercare di prevenire gli incidenti di sicurezza, riducendo il livello di rischio e l'esposizione a possibili attacchi informatici.

Tali contromisure, che possono essere di natura sia tecnologica che organizzativa, sono descritte in tutti i disciplinari adottati dall'Ente in materia di privacy e ICT governance e all'interno del Documento Programmatico per la Sicurezza. L''attivazione di queste contromisure è necessaria per mettere in sicurezza i sistemi della Regione e fornisce un importante aiuto per gestire e risolvere in maniera più efficiente eventuali incidenti.

10. La Procedura di gestione degli incidenti di sicurezza informatici

Deve essere sviluppata, documentata e tenuta aggiornata una Procedura per la gestione degli incidenti di sicurezza. Tale Procedura ha i seguenti obiettivi:

preparare il personale ad affrontare situazioni anomale e non codificate;

identificare un incidente in corso;

minimizzare i danni relativi all'incidente ed impedirne la propagazione;

gestire correttamente il processo di ripristino dei sistemi e delle applicazioni;

gestire correttamente il processo di notifica al Garante e di comunicazione agli interessati;

acquisire nel modo appropriato le eventuali evidenze digitali di reato;

riconoscere gli errori commessi, assumerne le responsabilità e formulare proposte volte a migliorare la Procedura stessa.

Per facilitare la gestione degli incidenti di sicurezza occorre mantenere operativo un workflow che automatizzi le varie fasi, in particolare il flusso delle comunicazioni fra i vari attori. Tale misura ha anche lo scopo di facilitare la produzione del report relativo all'incidente e di tenere aggiornate le statistiche sugli incidenti di sicurezza gestiti dal gruppo GOS-ICT.

Nel caso in cui l'incidente di sicurezza venga classificato come Disastro deve essere data attuazione a quanto previsto nella policy di Business Continuity.

I potenziali incidenti oppure comportamenti anomali dei sistemi che possano destare sospetto vanno segnalati all'Area del Servizio ICTR che ha in carico la gestione operativa della sicurezza informatica utilizzando l'indirizzo securityadmin@regione.emilia-romagna.it).

L'incidente si considera chiuso con l'apposizione della firma digitale sul rapporto da parte del Responsabile del Servizio ICTR.

8. Evidenze degli incidenti ed analisi forense

A seguito di un incidente relativo alla sicurezza delle informazioni, l'Ente potrebbe essere legittimato attivamente o passivamente ad un'azione giudiziaria o legale; per tale ragione, le evidenze oggettive dell'incidente e/o del data breach devono essere raccolte e conservate con modalità tali che non possa essere contestata la loro integrità e autenticità.

Pertanto, il processo di raccolta e di conservazione delle evidenze deve essere controllabile e ripetibile.

La raccolta delle evidenze può avvenire anche qualora si voglia semplicemente procedere con indagini più approfondite, non necessariamente connesse ad un corso giudiziario/legale.

La documentazione relativa agli incidenti di sicurezza, comprensiva delle evidenze e delle valutazioni effettuate, viene elaborata minimizzando i dati personali.

Le evidenze raccolte durante gli incidenti di sicurezza che contengono dati personali sono conservate sino all'esaurimento della finalità di gestione degli incidenti e di apprendimento.

10. Controlli applicabili

Nella tabella seguente sono riportati i controlli dello standard ISO27001 che possono essere ricondotti alla presente policy:

Identificativo ISO27001	Controllo
A.06.01.03	*Contatti con le autorità*
A.06.01.04	*Contatti con gruppi specialistici*
A.07.02.03	*Processo disciplinare*
A.16.01.05	*Risposta agli incidenti relativi alla sicurezza delle informazioni*
A.16.01.07	*Raccolta di evidenze*

11. Glossario

Termine/Acronimo	Descrizione
Analisi forense	Attività che, attraverso l'analisi delle strutture di dati contenute all'interno di dispositivi e apparecchiature digitali, permette di individuare pattern di attività fraudolente.
Evidenza	Nell'ambito dell'analisi forense, si intende una "traccia" di reato. Affinché

Termine/Acronimo	Descrizione
	siano valide da un punto di vista legale, una evidenza deve essere: • Ammissibile, per poter essere utilizzabile in sede legale; • Autentica, ovvero strettamente legata ai media digitali da cui è stata rilevata; • Completa, correlando tutte le informazioni possibili; • Affidabile, per non sollevare dubbi sulla sua autenticità; • Ripetibile, permettendo a chiunque di ricostruire il processo che ha portato alla sua rilevazione ottenendo gli stessi risultati.
Evento di sicurezza	Per evento di sicurezza si intendono tutti quegli eventi che indicano attacchi o tentativi di attacco che non hanno avuto impatto sulla riservatezza, integrità o disponibilità, o per i quali non è ancora chiaro se l'impatto c'è stato o meno. Sono eventi che potrebbero preludere ad un incidente e quindi vanno considerati e approfonditi (ad es: malware rilevato dal sistema antivirus, tentativi massivi di sql injection verso una o più web application, tentativo da parte di una o più postazioni di lavoro di contattare un command & control center bloccato o meno dall'IPS)
Data breach	la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati
Incidente di sicurezza	la violazione, la minaccia imminente di violazione di una policy di sicurezza informatica, di politiche di utilizzo accettabili o di prassi standard di sicurezza, correlato ad una violazione di dati o informazioni
Incidente di sicurezza di gravità alta	Incidente di sicurezza per cui il grado di compromissione di servizi e/o sistemi è elevato. Si rilevano danni consistenti sugli asset. Il ripristino è di medio o lungo periodo. L'incidente presenta una tra le seguenti condizioni: Danni a persone e rilevanti perdite di produttività Compromissione di sistemi o di reti in grado di permettere accessi incontrollati a informazioni confidenziali Siti web violati o utilizzati a fini di propagazione di materiale terroristico o pornografico Frode o attività criminale che coinvolga servizi forniti dall'ente Impossibilità tecnica di fornire uno o più servizi critici a un elevato numero di utenti per un intervallo di tempo superiore ai 30 minuti

Termine/Acronimo	Descrizione
	nell'arco di una giornata Impossibilità tecnica di fornire uno o più servizi di criticità media per un periodo di tempo superiore ai 2 giorni lavorativi Perdita di immagine e/o reputazione nei confronti del pubblico o degli utenti
Disastro	Incidente di sicurezza con impatto sulla continuità operativa per cui il tempo di disservizio è inaccettabile per il cliente (superiore all'RTO dichiarato in sede di BIA) e che richiede l'invocazione del piano di Business Continuity.