Opera di Firenze
Maggio Musicale
Fiorentino

Protocollo N.19
Gestione della sicurezza informatica

Approvato dal Consiglio di Indirizzo
il 26 gennaio 2016

Emesso con determinazione del Sovrintendente
n. 57 del 10 febbraio 2016

Protocollo N. 19
Gestione della sicurezza informatica

1. Scopo

Il presente protocollo definisce i requisiti fondamentali per la gestione della sicurezza informatica presso la Fondazione Teatro del Maggio Musicale Fiorentino.

Nello specifico, la Fondazione individua una propria politica di sicurezza informatica al fine di dotarsi di una struttura organizzativa che sia adeguata alla natura dell'attività svolta, alla sua dimensione, al livello dei rischi informatici ed agli obiettivi che si prefigge di raggiungere.

2. Campo di applicazione

La Fondazione persegue la diffusione e lo sviluppo dell'arte musicale e della conoscenza della musica, del teatro lirico e della danza, la formazione professionale dei quadri artistici e tecnici e l'educazione musicale della collettività.

I requisiti espressi nel presente protocollo coinvolgono sia il personale della Fondazione, sia il personale che opera nella Fondazione medesima per realizzare o mantenere in esercizio le applicazioni, i sistemi informatici ed i servizi agli utenti (ad es. appaltatori, fornitori) al fine di poter garantire il governo delle modalità con cui le informazioni sono protette, gestite e rese disponibili agli utenti. È responsabilità dei referenti della Fondazione comunicare ai propri collaboratori esterni le politiche di sicurezza adottate dalla Fondazione stessa.

3. Riferimenti

- D.Lgs. 231/01;
- ISO 38500: Corporate Governance for Information technology;
- ISO 27002: Information technology - Security techniques - Information security management systems – Requirements;
- Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01 della Fondazione (approvato dal Consiglio di Indirizzo in data 26 gennaio 2016);
- Codice Etico della Fondazione (approvato dal Consiglio di Indirizzo in data 26 gennaio 2016).

4. Termini e definizioni

Si riportano le definizioni dei principali termini specifici utilizzati nel presente documento:

- **Asset**: Qualsiasi cosa che ha valore per l'organizzazione
- **Ciclo di vita delle informazioni**: Comprende le fasi di generazione, custodia, archiviazione, accesso, trattamento, comunicazione, diffusione e distruzione delle informazioni
- **Dati personali**: Qualunque informazione relativa a persone fisiche, identificate o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale
- **Disponibilità**: Proprietà (di una risorsa) di essere accessibile ed utilizzabile, al momento della richiesta, da un'entità autorizzata
- **Information and Communication Technology (ICT)**: Qualsiasi sistema informatico e/o di telecomunicazioni costituito da dispositivi elettronici, servizi, applicazioni, database – progettato, realizzato e gestito per raccogliere, registrare, elaborare, archiviare, recuperare, visualizzare e trasmettere informazioni

- **Incidente relativo alla sicurezza delle informazioni**: Evento o serie di eventi relativi alla sicurezza delle informazioni, non voluti o inattesi, con una significativa probabilità di compromettere le operazioni relative al business e di minacciare la salvaguardia delle informazioni
- **Informazione**: Qualsiasi comunicazione o rappresentazione della conoscenza come fatti, dati o pareri in qualsiasi forma o mezzo (documenti, disegni, immagini, filmati, ecc.)
- **Integrità**: Proprietà correlata con la salvaguardia dell'accuratezza e completezza di una risorsa; preservare l'integrità dell'informazione significa proteggere anche i metodi utilizzati per processarla e gestirla
- **Media**: Dispositivi atti ad immagazzinare informazioni e dati ed a mantenerli nel tempo (es. CDROM, DVD, nastri magnetici, hard-disk, memorie flash, ecc.)
- **Minaccia**: Potenziale causa di incidente che può portare un danno all'organizzazione o ad un suo sistema
- **Organizzazione**: Gruppo, società, azienda, impresa, ente o istituzione, ovvero loro parti o combinazioni, in forma associata o meno, pubblica o privata, che abbia una propria struttura funzionale e amministrativa
- **Rischio**: Potenzialità che una determinata minaccia sfrutti le vulnerabilità di un Asset o di un gruppo di Asset e causi danni alla Fondazione e/o agli individui
- **Riservatezza**: Proprietà per cui l'informazione non è resa disponibile o comunicata a individui, entità o processi non autorizzati
- **Sicurezza delle informazioni**: Conservazione delle proprietà di riservatezza, integrità e disponibilità delle informazioni; possono essere coinvolte, inoltre, altre proprietà quali l'autenticità, la responsabilità, il non ripudio e l'affidabilità
- **Sicurezza Informatica**: L'insieme delle misure organizzative, operative e tecnologiche finalizzate a salvaguardare i trattamenti delle informazioni effettuati mediante strumenti elettronici
- **Sistema Informativo**: Un insieme discreto e delimitato di risorse informative progettato, costruito, gestito e mantenuto per raccogliere, registrare, elaborare, archiviare, recuperare, visualizzare e trasmettere determinate informazioni
- **Tipologia di Informazione**: Una specifica categoria di Informazioni (es. privacy, commerciale, finanziaria, investigativa, ambientale, ecc.) definita ed utilizzata all'interno di un'organizzazione o derivata da altre circostanze, ad esempio da leggi, direttive, politiche, regolamenti, ecc.
- **Standard**: Un documento "riconosciuto" che contiene un insieme di regole con lo scopo di indirizzare lo sviluppo e la gestione di materiali, prodotti, servizi, tecnologie, attività, processi e sistemi
- **Vulnerabilità:** Debolezza di un *Asset* o di un gruppo di *Asset* che può essere sfruttata da una o più minacce
- **Modello 231**: Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01 della Fondazione
- **Fondazione**: Fondazione Teatro del Maggio Musicale Fiorentino

5. Procedura – Politica per la gestione della sicurezza informatica

5.1 Identificazione dei pericoli e valutazione dei rischi

La protezione delle informazioni gestite dalla Fondazione, siano esse di uso interno o collegate ai servizi erogati ai clienti, deve passare attraverso la salvaguardia dei seguenti requisiti di sicurezza:

- **Riservatezza**: garantisce che un'informazione sia accessibile solo a chi è autorizzato;
- **Integrità**: salvaguarda l'accuratezza e la completezza delle informazioni durante la sua creazione, elaborazione, trasmissione e ricezione;
- **Disponibilità**: garantisce, quando richiesto e autorizzato, l'accesso alle informazioni e ai beni associati.

Per garantire tali requisiti, la Fondazione deve gestire il rischio secondo una metodologia, articolata nelle seguenti fasi:

- valutazione del rischio: identifica e valuta le minacce esterne e le vulnerabilità intrinseche che mettono a rischio le informazioni;
- trattamento del rischio: pianifica gli opportuni accorgimenti tecnici ed organizzativi per fronteggiare eventuali attacchi che sfruttano le minacce e le vulnerabilità identificate;
- accettazione del piano di trattamento del rischio e del rischio residuo proposto;
- attuazione degli interventi pianificati;
- monitoraggio e controllo della loro efficacia;
- attivazione del ciclo di miglioramento continuo del processo di gestione del rischio.

La gestione del rischio deve essere condotta in modo da:

- rispettare i requisiti definiti dagli standard di riferimento;
- rispettare i principi, obiettivi e regole della Fondazione, che rappresentano le norme comportamentali che la Fondazione stessa definisce al suo interno per supportare le proprie attività.

5.2 Obiettivi e programmi

Sul complesso delle risorse informative di una Fondazione gravano, in generale, una serie di minacce riconducibili a tipiche aree di rischio, tra cui errori ed omissioni, frodi e furti, sabotaggi, perdite di funzionalità di infrastrutture ICT.

La Fondazione deve pertanto operare per conoscere e comprendere costantemente le minacce e le vulnerabilità a cui sono esposte le risorse informative di competenza al fine di individuare le giuste ed idonee misure di protezione.

La Fondazione deve, inoltre, mettere in opera tutte le azioni necessarie per perseguire obiettivi di sicurezza congrui con il grado di criticità delle Informazioni, attraverso la tutela degli attributi di Riservatezza, Integrità, Disponibilità.

5.3 Politiche di dettaglio

L'efficacia di una politica di gestione della sicurezza delle informazioni si basa su una struttura organizzativa adeguata e con responsabilità definite, personale addestrato, comunicazioni e documenti chiari e completi, controllo delle attività operative e disponibilità di procedure/piani per le emergenze.

Vengono di seguito descritte le Politiche di dettaglio per ciascuno degli ambiti inerenti la gestione della sicurezza delle informazioni.

5.3.1 Gestione dei beni

La Fondazione all'interno delle sue sedi deve possedere un Inventario dei beni che comprende sia gli asset di tipo informativo che le infrastrutture che trattano le informazioni.

Nelle sedi della Fondazione devono esistere, e dovranno essere regolarmente mantenute, una serie di regole per l'utilizzo corretto dei beni.

Tutte le informazioni trattate hanno bisogno di essere classificate in funzione del loro valore, della loro criticità, sensibilità e in relazione alle prescrizioni normative e legali. Inoltre devono essere sviluppate delle procedure per l'etichettatura ed il trattamento delle informazioni.

5.3.2 Sicurezze delle Risorse Umane

Per il personale dipendente interno, collaboratori e terze parti, devono essere definiti i ruoli e le responsabilità per la gestione della sicurezza delle informazioni.

Tutti i candidati per l'impiego devono essere adeguatamente selezionati nel rispetto della legislazione e dei regolamenti vigenti.

Il personale dipendente interno, collaboratori e terze parti devono accettare e sottoscrivere i termini e le condizioni d'impiego, che devono precisare le reciproche responsabilità della Fondazione e del personale circa la sicurezza delle informazioni.

Al personale deve essere erogata un'adeguata formazione e un aggiornamento tecnico in merito alla sicurezza e alla privacy.

La violazione delle regole di sicurezza è soggetta a procedure di valutazione, che possono comportare sanzioni disciplinari.

Per i dipendenti interni, collaboratori e terze parti, che variano il loro impiego o lasciano l'organizzazione, devono essere definite le responsabilità, affinché questo processo avvenga in modo controllato. I beni della Fondazione in possesso dei dipendenti collaboratori e terze parti devono essere restituiti al termine del loro contratto d'impiego.

Devono essere rimossi o modificati i diritti di accesso alle informazioni e alle strutture di elaborazione delle informazioni, per i dipendenti interni, collaboratori e terze parti al termine o in caso di variazione dell'impiego.

5.3.3 Formazione

La Fondazione deve stabilire quali competenze deve avere il personale per poter svolgere attività relative alla prevenzione e protezione della salvaguardia delle informazioni.

Bisogna quindi predisporre un "Piano di Formazione" che consenta la sensibilizzazione di tutti i lavoratori alle tematiche inerenti alla sicurezza delle informazioni.

5.3.4 Sicurezza Fisica e Ambientale

Le aree in cui sono trattate le informazioni devono essere opportunamente perimetrate e gli accessi a tali aree devono essere controllati, secondo procedure specifiche, al fine di consentire l'accesso al solo personale autorizzato.

Per il trattamento e la conservazione di informazioni critiche devono essere previste aree dedicate con livelli di protezione specifici e devono essere previste delle modalità per operare nelle aree sicure.

Gli apparati informatici devono essere adeguatamente posizionati e protetti in modo tale da ridurre i rischi provenienti da minacce (sia interne che esterne), da pericoli ambientali e da accessi non autorizzati.

Devono essere assicurati i servizi necessari quali, ad esempio, l'adeguata erogazione della potenza elettrica e la fornitura di condizioni ambientali ottimali.

I cablaggi per l'alimentazione elettrica e per le telecomunicazioni dedicati alla trasmissione dei dati e per l'erogazione dei servizi, devono essere protetti e assicurati da possibili intercettazioni o danneggiamenti.

Gli apparati devono essere sottoposti a opportuni piani di manutenzione per garantire la loro disponibilità ed integrità.

L'utilizzo di qualsiasi apparato informatico fuori dalle sedi della Fondazione deve seguire un processo autorizzativo al fine di garantire un livello di sicurezza delle informazioni adeguato.

Tutte le informazioni contenute negli apparati o nei supporti in dismissione, o in manutenzione presso soggetti esterni, devono essere preventivamente rimosse in modo sicuro.

Le rimozioni e i trasferimenti di apparati devono essere autorizzati e opportunamente documentati.

5.3.5 Gestione delle Comunicazioni e dell'Operatività

Deve essere assicurato il corretto e sicuro funzionamento delle componenti IT, gestendo e controllando i cambiamenti, definendo le responsabilità operative e curando le necessarie separazioni delle funzioni.

Per i nuovi sistemi informativi si devono stabilire dei criteri di approvazione, sia in caso di aggiornamenti che di nuove versioni. Prima di mettere in esercizio un sistema o un suo componente deve essere eseguito con successo il piano di test, comprensivo degli aspetti di sicurezza.

Per i servizi di gestione forniti da terze parti (ad esempio assistenza utenti, trasporto di supporti magnetici e documenti) dovranno essere analizzati i rischi e previsti dei controlli adeguati che dovranno essere inseriti anche nei relativi contratti.

Per prevenire problemi, di riduzione o interruzione dei livelli di servizio, ogni sistema in esercizio deve essere soggetto a un opportuno monitoraggio delle prestazioni e a valutazioni periodiche di efficienza e capacità, anche a fronte dei futuri maggiori carichi previsti (capacity planning).

Devono essere attuati controlli di prevenzione e rilevazione per salvaguardare l'integrità del software e delle informazioni da corruzioni dovute a codice malevolo e mobile (esempio *applet* o *activeX*).

Per mantenere l'integrità e la disponibilità dei sistemi informativi e dei servizi di comunicazione devono essere prodotte e regolarmente testate copie di backup delle informazioni e del software. Le copie di backup devono essere conservate in locali diversi da quelli che custodiscono i dati originari e devono essere adeguatamente protette, in funzione del livello di riservatezza dei dati.

Deve essere assicurata la sicurezza delle informazioni in transito sulle reti e la protezione delle infrastrutture di supporto. A tal fine devono essere resi operativi gli opportuni controlli e i sistemi di monitoraggio per la sicurezza della rete, e dei servizi erogati in rete.

Le informazioni trasmesse o scambiate devono essere protette da accessi e/o modifiche non autorizzati o da corruzione. A tal fine devono essere definite e redatte politiche, procedure e controlli per proteggere lo scambio di informazioni attraverso l'uso della voce, del fax e delle video conferenze e della posta elettronica.

Inoltre, i dati destinati alla pubblicazione, per esempio su siti web, devono essere preventivamente autorizzati in modo formale.

Tutti gli accessi ai sistemi, da parte degli amministratori, e i cambiamenti delle configurazioni devono essere tracciati in appositi registri operativi (*"operation log"*), che devono essere adeguatamente conservati e protetti.

Gli errori tecnici degli apparati devono essere registrati cronologicamente, analizzati e devono innescare le adeguate misure conseguenti.

5.3.6 Controllo Accessi

Devono essere redatte regole per il provisioning delle utenze (creazione, cancellazione e sospensione), per la gestione delle password e, più in generale, delle credenziali di autenticazione. Tali diritti di accesso devono essere rivisti e validati a intervalli regolari.

L'accesso ad un sistema deve essere controllato in maniera commisurata alla criticità del servizio tramite misure quali l'individuazione del terminale, procedure di logon che identifichi e autentichi l'utente, adeguata gestione delle credenziali di autenticazione.

Gli utenti devono seguire specifiche procedure di sicurezza per la scelta e l'utilizzo delle password.

Il personale è tenuto ad adottare misure per prevenire accessi non autorizzati di utenti e la compromissione o il furto di informazioni o di strumenti di gestione dell'informazione.

5.3.7 Accessi alla Rete

L'accesso alle reti deve essere protetto prevedendo opportune regole d'uso, specifiche per tipologie di accesso (telelavoro, connettività alla rete, ecc.).

Le reti condivise devono essere dotate di misure di monitoraggio per assicurare che i flussi di informazioni non siano compromessi e le modalità di connessione degli utenti siano controllate.

Le apparecchiature collegate in rete devono essere identificate per consentire l'autenticazione delle connessioni.

Devono essere adottati controlli di instradamento nelle reti per assicurare che le connessioni delle apparecchiature e il flusso delle informazioni non violino la politica per il controllo degli accessi nelle applicazioni.

5.3.8 Acquisizione, Sviluppo e Manutenzione dei Sistemi Informativi

Lo sviluppo dei programmi applicativi deve essere condotto secondo quanto definito nel processo di sviluppo e manutenzione, prevedendo la definizione dei requisiti di sicurezza. Per garantire l'integrità delle informazioni, devono essere previsti appositi controlli sui dati in ingresso e in uscita alle applicazioni, sull'elaborazione interna e sull'integrità dei messaggi.

La gestione dei cambiamenti relativamente alle applicazioni deve essere opportunamente controllato e tracciato, e le applicazioni devono essere riesaminate per assicurare che non ci siano impatti negativi sugli aspetti operativi o di sicurezza.

Devono essere limitati i cambiamenti nei pacchetti software e, se eseguiti, puntualmente controllati.

Devono essere previste procedure per controllare l'installazione dei software sui sistemi in funzione, così come l'accesso al codice sorgente dei programmi.

Deve essere implementato un processo per ottenere tempestive informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati, al fine di valutare l'esposizione a tali vulnerabilità e mettere in atto misure adeguate per poterle gestire.

5.3.9 Gestione degli Incidenti di Sicurezza delle Informazioni

Per ridurre i rischi relativi alla sicurezza del patrimonio informativo della Fondazione deve essere adottato un sistema di segnalazione degli eventi di sicurezza delle informazioni e di gestione dei relativi incidenti.

In particolare, le procedure adottate devono garantire che gli eventi di sicurezza delle informazioni e delle debolezze relative ai sistemi informativi siano segnalati il più rapidamente possibile, attraverso appropriati canali di gestione, in modo da permettere che le risposte vengano tempestivamente intraprese.

Bisogna inoltre garantire che l'approccio adottato per la gestione degli incidenti sia consistente, efficace e tempestivo attraverso l'individuazione di ruoli e responsabilità, la redazione di procedure e il costante monitoraggio degli incidenti in modo da imparare dagli errori.

A seguito di incidenti relativi alla sicurezza devono essere raccolte, conservate e preservate, le evidenze oggettive per eventuali azioni legali (civili e penali).

5.3.10 Gestione della Continuità Operativa

Per reagire ad eventuali interruzioni di disponibilità dei sistemi informativi, dovute a guasti o disastri, devono essere previsti piani di continuità, basati su una valutazione del rischio condivisa dalla Fondazione.

Tali piani devono essere sviluppati al fine di garantire la continuità delle risorse a supporto dei processi della Fondazione e dei servizi forniti.

Occorre assicurare che essi siano coerenti e che siano definite le loro priorità.

A tal fine devono essere testati e revisionati regolarmente, per assicurarne l'aggiornamento e l'efficacia.

5.3.11 Conformità

Per ogni sistema deve essere definita ed opportunamente documentata la presenza di eventuali vincoli dovuti a normativa o leggi vigenti.

Gli elementi di prova, ai fini legali e probatori, devono essere raccolti e tenuti in modo conforme alle regole di ammissibilità in giudizio.

Per garantire la conformità dei sistemi ai requisiti di sicurezza, i responsabili di struttura devono assicurare la corretta ed integrale applicazione delle procedure di sicurezza, all'interno della propria area di competenza.

In particolare si fa riferimento ai vincoli di legge civili e penali, a quelli di origine statutaria, ad obbligazioni contrattuali, ai requisiti di sicurezza, ai diritti di proprietà intellettuale e all'uso del software proprietario.

A tale proposito devono essere effettuate regolari verifiche di conformità.

Le registrazioni della Fondazione ritenute strategiche, quali informazioni amministrative e contabili, devono essere protette da perdite, distruzione e falsificazione.