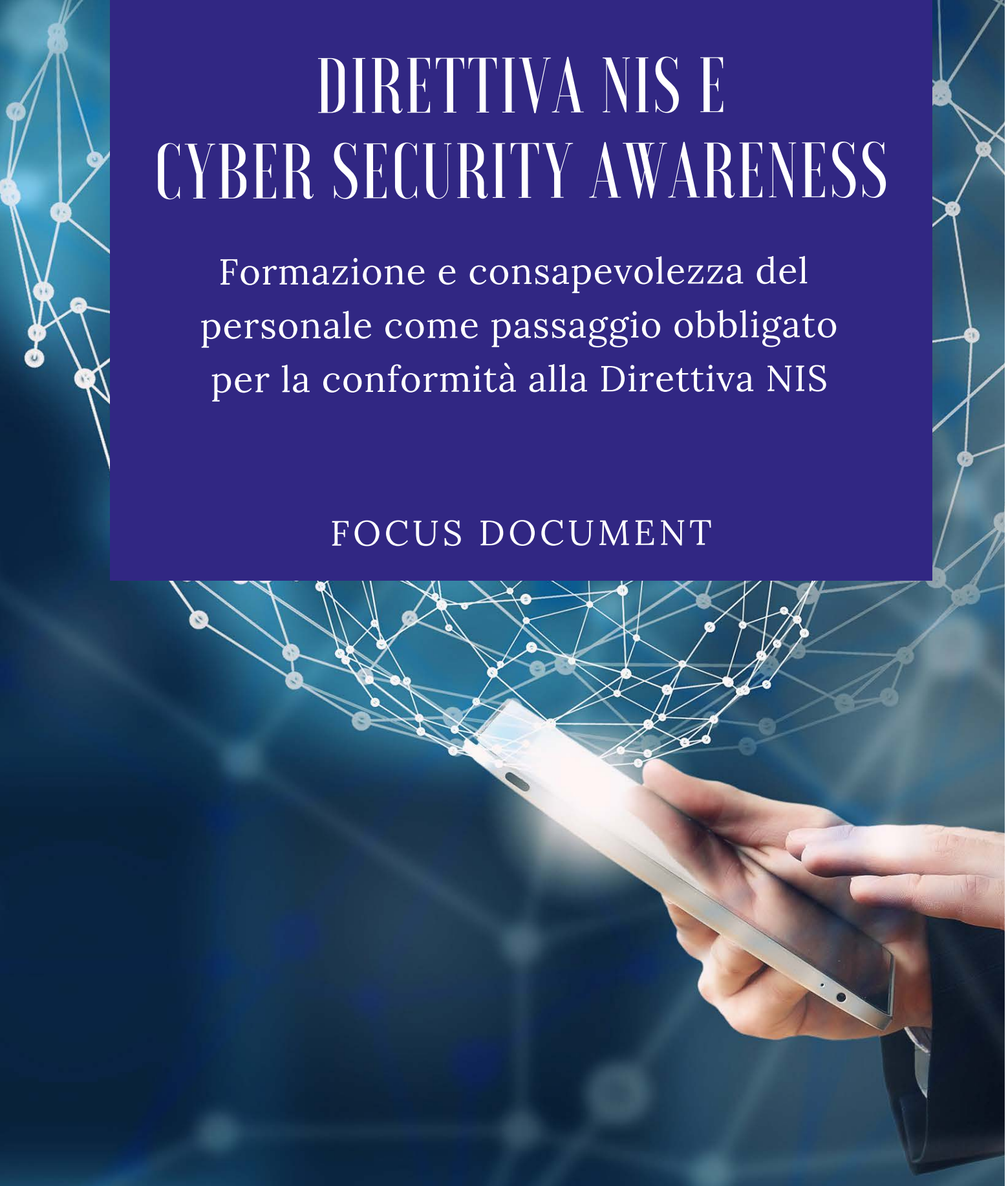
DIRETTIVA NIS E CYBER SECURITY AWARENESS

Formazione e consapevolezza del personale come passaggio obbligato per la conformità alla Direttiva NIS

FOCUS DOCUMENT



Cyber Guru

SOMMARIO

DIRETTIVA NIS

Il **30 giugno 2020** rappresenta una scadenza importante per i 465 Operatori di Servizi Essenziali (da ora in poi OSE), soggetti alla **Direttiva NIS** (da ora in poi NIS), e in particolare per i loro CISO.

Infatti in quella data si completa il **ciclo di 12 mesi concesso agli operatori per adeguarsi alle linee guida per la gestione dei rischi, la prevenzione e la mitigazione degli incidenti** che hanno un impatto rilevante sulla continuità e sulla fornitura dei servizi essenziali, e quindi, per essere conformi alla NIS.

Le nuove linee guida destinate agli OSE, sono basate sul **Framework Nazionale per la Cybersecurity**, che inserisce tra i controlli essenziali di Cyber Security **la formazione e la consapevolezza del personale**, affinché lo stesso sia adeguatamente sensibilizzato e formato sui rischi di Cyber Security e sulle pratiche da adottare.

L'offerta **Cyber Guru di Cyber Security Awareness,** consente di indirizzare questi controlli in modo particolarmente efficace e quindi di garantire all'operatore di servizi essenziali la massima conformità alla NIS sui temi specifici della formazione e della consapevolezza.

CRONOLOGIA NORMATIVA

La **Direttiva (UE) 2016/1148**, la cosiddetta **NIS**, definisce le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi.

La NIS si applica agli **OSE** e ai **Fornitori di Servizi Digitali .**

La NIS è stata recepita nel nostro ordinamento con il **Decreto Legislativo 18 maggio 2018, n.65**, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018.

Le autorità nazionali competenti in materia, a luglio del 2019, hanno elaborato le **linee guida per la gestione dei rischi, la prevenzione e mitigazione degli incidenti** che hanno un impatto rilevante sulla continuità e sulla fornitura dei servizi essenziali.

Le linee guida sono basate sul **Framework Nazionale per la Cybersecurity** e definiscono le modalità operative a cui riferirsi sia in fase di prevenzione sia in fase di emergenza per mitigare le conseguenze di incidenti che impattano sulla continuità e sulla fornitura dei servizi essenziali.

Una volta partita la comunicazione formale relativa alle linee guida, gli OSE avranno **tra i quattro ed i dodici mesi** di tempo per uniformarsi alle linee guida, a seconda delle specificità settoriali.

Gli OSE sono i soggetti, pubblici o privati, che **forniscono servizi essenziali per la società** e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali.

Gli FSD sono le persone giuridiche che **forniscono servizi di e-commerce, cloud computing o motori di ricerca**, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale.

FORMAZIONE E CONSAPEVOLEZZA

Nel **Framework Nazionale per la Cybersecurity,** nella tabella 2 relativa ai Controlli Essenziali di Cybersecurity, si fa esplicito riferimento al tema della **Formazione e Consapevolezza**.

Il controllo specifico (#10) è così strutturato:

> *Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, ...). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.*

Pur nella sua inevitabile genericità, questo controllo rimanda alla **necessità di attivare programmi efficaci di Cyber Security Awareness** al fine di sensibilizzare in modo adeguato tutto il personale sui rischi di Cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti digitali. Questo riferimento alle pratiche da adottare è chiaramente correlato con la necessità di influenzare i comportamenti degli utenti "digitali".

Anche il recente **Decreto Legislativo 21 settembre 2019, n.105** ha richiamato esplicitamente il tema della **Formazione e della Consapevolezza** (Art.1, Comma 3, Punto 7) come "misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici", definendo il tutto all'interno del "**Perimetro di sicurezza nazionale cibernetica**", in un quadro caratterizzato da "**straordinaria necessità ed urgenza**".

Il Decreto Legislativo stabilisce anche il regime sanzionatorio conseguente alla mancata osservanza di quanto stabilito dal decreto stesso.

CYBER SECURITY AWARENESS

Analizzando le esigenze degli OSE possiamo fare un primo assunto: che per raggiungere la conformità rispetto alla NIS e nello stesso tempo ridurre concretamente il rischio Cyber, sia necessario avviare un **programma avanzato di Cyber Security Awareness,** in grado di raggiungere la totalità dei dipendenti e dei collaboratori.

Di seguito quattro caratteristiche fondamentali per un programma formativo di Cyber Security Awareness, realmente efficace e in grado di influenzare le pratiche del personale dipendente di un OSE:

- **Efficace** - in grado di incidere efficacemente sui comportamenti del personale, adeguandoli al livello raggiunto dalla minaccia Cyber. Questo comporta la capacità di "ingaggiare" i partecipanti e motivarli a partecipare, superando i limiti storici della formazione "aziendale".

- **Aperto a tutti** – in grado di raggiungere tutta la popolazione aziendale, indipendentemente dal ruolo ricoperto all'interno dell'organizzazione. Questo comporta una particolare attenzione al linguaggio, che deve essere divulgativo e lontano da ogni ortodossia tecnologica.

- **Continuo** – in grado di mantenere elevato nel tempo il livello di attenzione sulle minacce Cyber. Questo comporta un programma di lunga durata che si rinnova costantemente seguendo l'evoluzione delle tecniche di attacco.

- **Compatibile** – in grado di avere un impatto minimo sui tempi e sugli impegni professionali. Quindi con un approccio diluito nel tempo e con l'erogazione di pillole formative brevi e autoconsistenti.

Programma avanzato

A fronte della continua evoluzione della minaccia Cyber e del rapido mutamento del quadro normativo di riferimento, possiamo dare per scontato che prima di Giugno 2020, la maggior parte delle organizzazioni avranno adottato o avranno in progetto di adottare, programmi avanzati di **Cyber Security Awareness**, che tengano conto delle quattro caratteristiche sopra elencate.

Sviluppare consapevolezza sui rischi Cyber, alzare il livello di attenzione degli utenti adeguando i loro comportamenti al rischio raggiunto dalla criminalità informatica, è un passaggio obbligato per raggiungere la conformità alla NIS.

Conformità alla NIS

CYBER GURU AWARENESS

L'INNOVATIVO SISTEMA DI E-LEARNING CHE CONSENTE DI COINVOLGERE L'ORGANIZZAZIONE IN UN PERCORSO DI APPRENDIMENTO EFFICACE

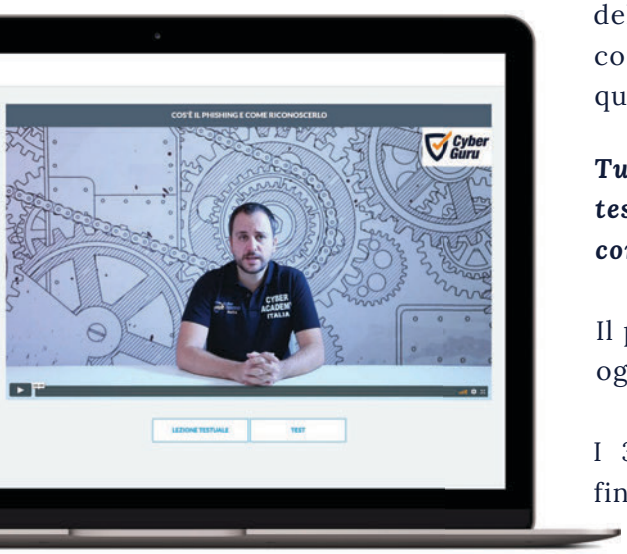
Cyber Guru Awareness (da ora in poi CGA) è un programma formativo in grado di sviluppare un elevato grado di consapevolezza nell'uso delle tecnologie digitali e nella navigazione Web.

Con Cyber Guru Awareness ogni singolo membro dell'organizzazione viene reso parte attiva delle difese informatiche. Di conseguenza si rafforza complessivamente la postura di sicurezza dell'intera organizzazione e si riduce drasticamente il rischio di subire danni.

Ogni elemento di Cyber Guru Awareness è stato progettato e realizzato per massimizzare l'efficacia del contributo formativo, minimizzando l'effetto dispersivo e annullando i costi di gestione: **"massimo risultato formativo con il minor impatto organizzativo ed economico"**

Sistema di e-learning

LA PIATTAFORMA DI CYBER GURU AWARENESS



La **video lezione**, con l'attore coach, rappresenta l'elemento base del percorso formativo e, insieme alla **gamification**, la leva che consente di ingaggiare l'utente e coinvolgerlo in questo percorso.

Tutti i contenuti formativi vengono forniti anche in formato testuale, per consentirne la migliore fruizione, in tutte le condizioni.

Il percorso formativo è costituito da **36 moduli auto-consistenti** ognuno dedicato ad uno specifico argomento.

I 36 moduli sono organizzati su **3 livelli formativi annuali**, finalizzati a realizzare un percorso continuativo e progressivo.

I moduli sono suddivisi in **3 lezioni brevi**, ognuna delle quali si conclude con un **test di apprendimento**.

I 3 LIVELLI FORMATIVI

PRIMO LIVELLO

1. **Phishing**
2. ***Password***
3. ***Social Media***
4. ***Privacy & GDPR***
5. ***Mobile & App***
6. ***Fake News***
7. ***Dispositivi USB***
8. ***e-Mail Security***
9. ***Malware***
10. ***Web Browsing***
11. ***Critical Scenarios***
12. ***Social Engineering***

SECONDO LIVELLO

1. **Clean Desk**
2. ***Personal Information***
3. ***Information Classification***
4. ***IoT Device***
5. ***Away from Office***
6. ***Spear Phishing***
7. ***Smishing & Vishing***
8. ***Phone Scam***
9. ***Sneaky Phishing***
10. ***Bluetooth & Wi-Fi***
11. ***Data Protection***
12. ***Social Engineering 2***

TERZO LIVELLO

1. **Privacy**
2. ***Social & Cyberbullying***
3. ***Legal Aspect***
4. ***Real Scams 1***
5. ***Real Scams 2***
6. ***Malware 2***
7. ***e-Commerce***
8. ***Holiday & Business trip***
9. ***Cyber Hygiene***
10. ***Backup & Restore***
11. ***Best Practice***
12. ***Social Engineering 3***

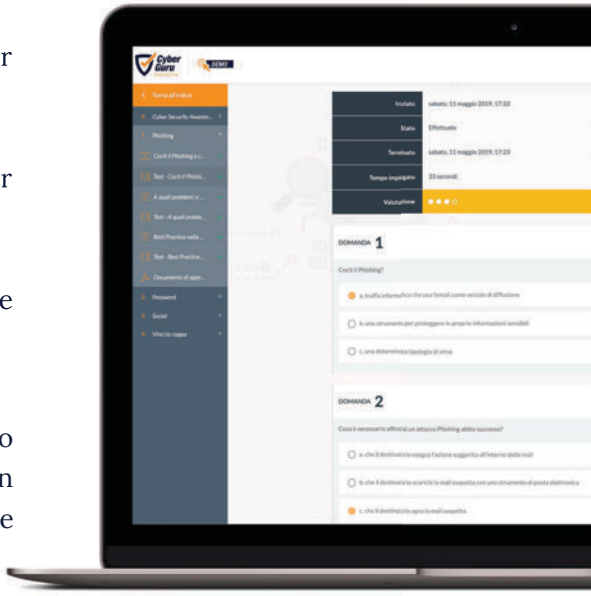
Piattaforma e livelli

IL SISTEMA DI GAMING

Per ottenere il massimo del coinvolgimento formativo Cyber Guru Awareness si avvale di:

- **un sistema di Gaming individuale,** con la possibilità per chi partecipa di acquisire medaglie e coppe;
- **un sistema di Gaming a squadre,** con una competizione "virtuosa" che stimola la partecipazione corale.

I test rappresentano un elemento necessario per valutare o migliorare il proprio livello di apprendimento, ma sono anche un elemento cruciale per supportare i meccanismi di Gaming che sono insiti nel percorso formativo.



PERCHE' SCEGLIERE CYBER GURU AWARENESS

- **PERCHÉ SUPERA I LIMITI DELLA FORMAZIONE TRADIZIONALE, CHE HA UN EFFETTO EFFIMERO E CHE NON È IN GRADO DI SEGUIRE LA RAPIDA EVOLUZIONE DELLE TECNICHE DI ATTACCO.**
- **PERCHÉ INTRODUCE I CONCETTI DI FORMAZIONE CONTINUA, AUMENTANDO LA CONSAPEVOLEZZA E LA PERCEZIONE CONDIVISA DELLE MINACCE.**
- **PERCHÉ COINVOLGE TUTTA L'ORGANIZZAZIONE IN UN UNICO PERCORSO FORMATIVO.**
- **PERCHÉ NON HA UN APPROCCIO IMPOSITIVO, MA STIMOLA COSTANTEMENTE LA QUALITÀ DELLA PARTECIPAZIONE, PUNTANDO ANCHE SUI BENEFICI DI CARATTERE PERSONALE, OLTRECHÉ SU QUELLI DI CARATTERE PROFESSIONALE.**

Perchè Cyber Guru

DIRETTIVA NIS E CYBER SECURITY AWARENESS

Cyber Guru Awareness

www.cyberguru.it
contatti@cyberguru.it
Numero verde 800.741.423