

# Pla de Formació de Ciberseguretat

Matalassos Soler



# Índex

<b>1. Introducció.....</b>	<b>3</b>
<b>2. Objectius.....</b>	<b>3</b>
<b>3. Públic Objectiu .....</b>	<b>3</b>
<b>4. Metodologia .....</b>	<b>3</b>
<b>5. Formació en Ciberseguretat .....</b>	<b>4</b>
<b>5.1 Objectius de la Formació.....</b>	<b>4</b>
<b>5.2 Recursos de Formació .....</b>	<b>4</b>
<b>5.3 Exercicis de Simulació de Phishing i Red Teams .....</b>	<b>5</b>
<b>6. Seguiment i Avaluació .....</b>	<b>5</b>
<b>6.1 Avaluació de l'Aprendentatge .....</b>	<b>5</b>
<b>6.1 Indicadors de Seguiment.....</b>	<b>5</b>
<b>6.2 Retroalimentació i Millores.....</b>	<b>6</b>
<b>7. Cronograma.....</b>	<b>6</b>
<b>7.1 Calendari de Formació .....</b>	<b>6</b>
<b>7.2 Duració de les Sessions .....</b>	<b>7</b>
<b>7.3 Planificació de les Activitats.....</b>	<b>7</b>
<b>8. Pressupost .....</b>	<b>8</b>
<b>8.1 Despeses Relacionades amb la Formació .....</b>	<b>8</b>

## 1. Introducció

La ciberseguretat és un element crític en l'entorn empresarial actual. Amb l'augment de les amenaces cibernètiques i l'ús creixent de la tecnologia a les organitzacions, la protecció de la informació i la infraestructura empresarial s'ha convertit en una prioritat essencial. Matalassos Soler reconeix la importància de la ciberseguretat i s'ha compromès a protegir les seves dades i la confidencialitat de les seves operacions.

## 2. Objectius

El present Pla de Formació de Ciberseguretat té com a principal objectiu proporcionar als membres de Matalassos Soler les habilitats, coneixements i eines necessàries per prendre les precaucions adequades enfront de les amenaces cibernètiques. Els objectius específics d'aquest pla són els següents:

1. Augmentar la consciència en matèria de ciberseguretat entre tot el personal de Matalassos Soler.
2. Capacitar els empleats per identificar i respondre adequadament a les amenaces cibernètiques.
3. Millorar les pràctiques de seguretat en l'ús de la tecnologia i la gestió de la informació.
4. Reduir el risc de pèrdua de dades i interrupcions en les operacions de l'empresa.
5. Garantir la conformitat amb les polítiques de seguretat de la informació i les regulacions aplicables.

## 3. Públic Objectiu

Aquest Pla de Formació està dissenyat per l'equip directiu i els responsables d'IT de Matalassos Soler.

## 4. Metodologia

La formació en ciberseguretat es durà a terme mitjançant una combinació de sessions presencials i en línia, així com recursos de formació auto-didàctics. Es promourà la participació activa dels empleats a través d'activitats pràctiques i d'exemples rellevants per al seu entorn de treball. S'avaluarà l'aprenentatge mitjançant proves i exercicis pràctics per garantir que els coneixements i les habilitats apreses es posin en pràctica de manera efectiva.

Aquest Pla de Formació de Ciberseguretat és un compromís de Matalassos Soler per protegir la seva informació i les seves operacions, i és un pas essencial per reforçar la seguretat cibernètica dins de l'organització. Amb la participació activa de tots els membres, assegurarem un entorn més segur i resistent davant les amenaces cibernètiques en constant evolució.

## 5. Formació en Ciberseguretat

La formació en ciberseguretat és un component essencial del nostre Pla de Formació, i es basa en diverses fonts de recursos, incloent-hi el **Institut Nacional de Ciberseguretat (INCIBE)**, formacions presencials i en línia, i exercicis de simulació de phishing o Red Teams. Aquesta secció descriu detalladament com s'abordarà la formació en ciberseguretat per garantir que els membres de Matalassos Soler estiguin ben preparats i conscients de les amenaces cibernètiques.

### 5.1 Objectius de la Formació

- Consciència en Ciberseguretat:** La formació començarà amb una sèrie de sessions de consciència en ciberseguretat. Els empleats aprendran les bases de la ciberseguretat, com les amenaces cibernètiques més comunes i com identificar-les. Aquesta etapa promourà una cultura de seguretat a tota l'organització.
- Protecció de Dades:** S'establiran sessions especialitzades per a la protecció de dades, assegurant que els membres entenguin la importància de la confidencialitat de la informació i com gestionar-la de manera segura.
- Seguretat de la Xarxa:** Es proporcionarà formació perquè els empleats comprenguin els riscos associats a les xarxes i com protegir-se contra atacs comuns, com ara el malware, els atacs de denegació de servei (DDoS) i els atacs de phishing.
- Gestió de Riscos:** S'ensenyarà com avaluar els riscos i com aplicar les millors pràctiques per mitigar-los. Això inclourà com gestionar les vulnerabilitats i com respondre a incidents de seguretat.

### 5.2 Recursos de Formació

- INCIBE:** Col·laborarem amb el **Institut Nacional de Ciberseguretat (INCIBE)** per proporcionar materials de formació de qualitat i actualitzats. Aquests materials inclouran guies, vídeos i casos pràctics relacionats amb les últimes amenaces cibernètiques i les millors pràctiques de seguretat.
- Formacions Presencials:** Organitzarem sessions de formació presencials periòdiques. Aquestes sessions estarán a càrec d'experts en ciberseguretat i inclouran tallers pràctics i oportunitats per a preguntes i debats.
- Formacions en Línia:** Per a la comoditat dels empleats, es proporcionarà accés a cursos de formació en línia. Això permetrà als membres de Matalassos Soler aprendre a la seva pròpia velocitat i en els horaris que els siguin més convenient.

## 5.3 Exercicis de Simulació de Phishing i Red Team

Per assegurar-nos que els membres de Matalassos Soler estiguin ben preparats per afrontar amenaces reals, es realitzaran exercicis de simulació de phishing i Red Team. Aquests exercicis permetran als empleats:

- Experimentar simulacions realistes d'atacs de phishing per aprendre com identificar-los i respondre-hi adequadament.
- Ser objecte d'avaluacions periòdiques realitzades per equips d'experts en ciberseguretat (Red Team) per identificar possibles punts febles en les nostres defenses i millorar-ne la seguretat.

Aquestes activitats de formació i exercicis de simulació estan dissenyats per augmentar la preparació de Matalassos Soler davant de les amenaces cibernètiques i garantir que tots els membres de l'organització estiguin ben informats i capacitats per protegir la nostra informació i infraestructura.

## 6. Seguiment i Avaluació

L'èxit del Pla de Formació de Ciberseguretat per a Matalassos Soler no només depèn de la implementació, sinó també de la capacitat per mesurar i avaluar el progrés i els resultats obtinguts. Per això, establim un sòlid sistema de seguiment i avaluació que ens permetrà assegurar-nos que la formació sigui eficaç i s'ajusti a les necessitats de l'organització.

### 6.1 Avaluació de l'Aprenentatge

**1. Proves d'Avaluació:** Després de cada mòdul de formació, es realitzaran proves d'avaluació per mesurar el coneixement adquirit pels empleats. Aquestes proves inclouran preguntes que avaluaran la comprensió dels conceptes clau en ciberseguretat.

**2. Retroalimentació dels Participant:** Es recollirà la retroalimentació dels participants sobre la qualitat i l'eficàcia de la formació. Aquesta informació serà fonamental per millorar els continguts i la metodologia de formació.

**3. Seguiment de l'Aplicació Pràctica:** A més de les proves, s'avaluarà la capacitat dels empleats per aplicar els coneixements adquirits a la seva tasca quotidiana. Això es realitzarà mitjançant l'observació i la revisió de les pràctiques de seguretat implementades.

### 6.1 Indicadors de Seguiment

1. **Taxa de Participació:** Es mesurarà la taxa de participació a les sessions de formació, tant presencials com en línia, per assegurar-nos que una proporció significativa del personal estigui completant la formació.

2. **Reducció d'incidents de Seguretat:** El seguiment dels incidents de seguretat permetrà avaluar si les pràctiques de seguretat han millorat després de la formació. Una reducció en els incidents relacionats amb la seguretat indicarà un progrés significatiu.
3. **Retroalimentació Positiva dels Empleats:** Es farà seguiment de les respostes dels empleats en les enquestes de satisfacció després de la formació per avaluar què aspectes de la formació han funcionat bé i quins necessiten millora.

## 6.2 Retroalimentació i Millores

Basant-nos en els resultats de l'avaluació i el seguiment, es realitzaran les següents accions:

1. **Millora Contínua:** S'utilitzaran les dades obtingudes per identificar les àrees d'èxit i aquelles que necessiten millora. Això inclourà la revisió i l'actualització dels materials de formació i de la metodologia en funció de les necessitats canviants.
2. **Sessió de Retroalimentació:** Es realitzaran reunions regulars per revisar els resultats de l'avaluació i el seguiment. Aquestes reunions permetran identificar punts forts i febles i definir les accions concretes a emprendre per millorar el Pla de Formació.
3. **Comunicació de Resultats:** Es comunicaran els resultats de l'avaluació i el seguiment als membres de Matalassos Soler per mantenir-los informats sobre el progrés en la formació i les accions de millora.

## 7. Cronograma

El cronograma del Pla de Formació de Ciberseguretat per a Matalassos Soler és una part crítica per assegurar-se que la formació es desenvolupi de manera sistemàtica i que tots els membres de l'organització tinguin accés a la informació i les habilitats necessàries per protegir-se davant les amenaces cibernetiques. A continuació, es presenta el cronograma general de la formació:

### 7.1 Calendari de Formació

#### Trimestre 1: Sensibilització en Ciberseguretat

- **Mes 1**
  - Inici de la formació en línia sobre consciència en ciberseguretat amb materials d'INCIBE.
- **Mes 2**
  - Continuació de la formació en línia sobre consciència en ciberseguretat.
- **Mes 3**

- Inici de sessions presencials de sensibilització en ciberseguretat per a tot el personal.

#### **Trimestre 2: Protecció de Dades i Seguretat de la Xarxa**

- **Mes 4**
  - Inici de la formació en línia sobre protecció de dades i seguretat de la xarxa amb materials d'INCIBE.
- **Mes 5**
  - Continuació de la formació en línia sobre protecció de dades i seguretat de la xarxa.
- **Mes 6**
  - Sessions presencials per aprofundir en la protecció de dades i la seguretat de la xarxa.

#### **Trimestre 3/4: Gestió de Riscos i Exercicis de Simulació**

- **Mes 7**
  - Formació en línia sobre gestió de riscos i metodologies d'avaluació de riscos amb material d'INCIBE.
- **Mes 8**
  - Realització d'exercicis de simulació de phishing per tot el personal a càrrec d'empresa externa.
- **Mes 9-12**
  - Exercici de Red Team per avaluar la resposta i les capacitats de seguretat.

### **7.2 Duració de les Sessions**

Les sessions tindran les següents duracions:

- **Formació en Línia:** Cada mòdul de formació en línia tindrà una duració aproximada de 2 a 4 hores, en funció del contingut i la complexitat.
- **Sessions Presencials:** Les sessions presencials es realitzaran durant una jornada completa i es distribuiran al llarg de diversos dies per acomodar les diferents àrees i equips de treball.
- **Simulació de Phishing:** Exercici d'un mes de duració.
- **Exercici de Red Team:** Aquest exercici tindrà una duració de 3 mesos entre l'inici i la seva evaluació.

### **7.3 Planificació de les Activitats**

La planificació de les activitats es realitzarà tenint en compte les necessitats i la disponibilitat del personal de Matalassos Soler. Es procurarà que la formació sigui accessible i que no interfereixi en les tasques operatives diàries. Les dates exactes de les sessions presencials i les proves de simulació de phishing es comunicaran amb prou antelació perquè els empleats puguin programar la seva participació.

## 8. Pressupost

La implementació efectiva del Pla de Formació de Ciberseguretat per a Matalassos Soler requereix recursos financers per garantir que la formació sigui de qualitat i s'ajusti a les necessitats de l'organització. A continuació, es presenta una estimació del pressupost necessari per dur a terme aquest pla:

### 8.1 Despeses Relacionades amb la Formació

1. **Formació en línia d'INCIBE:** La formació en línia realitzada amb els materials facilitats per l'Institut Nacional de Ciberseguretat (INCIBE) no té un cost associat però implica la dedicació a temps complert durant 3 mesos de la persona encarregada de preparar els materials.
2. **Exercicis de Simulació de Phishing:** L'organització de simulacions de Phishing implica la col·laboració amb empreses especialitzades. Estimem un cost de 2.000 euros per a aquesta activitat.
3. **Exercicis de Simulació de Red Team:** L'organització d'exercicis de Red Team implica la col·laboració amb empreses especialitzades. Estimem un cost de 8.000 euros per a aquesta activitat.

A nivell de resum, el cost total de l'aplicació d'aquest Pla de formació és de 10.000 euros més els tres mesos de dedicació del responsable de les formacions.