# Pla de Ciberseguretat

Matalassos Soler

# Índex

# 1. Introducció

El Pla de Ciberseguretat, o Pla de Seguretat de la Informació (PSI) de la nostra empresa de venda de matalassos té com a finalitat principal garantir la confidencialitat, integritat i disponibilitat de la informació i les dades crítiques per al funcionament del negoci. Aquest document està dissenyat per protegir les nostres dades i sistemes contra amenaces cibernètiques i altres riscos de seguretat.

# 2. Objectius

Els objectius del nostre PSI inclouen:

- Protegir les dades dels clients i les dades financeres de l'empresa.
- Garantir la disponibilitat dels nostres sistemes i la continuïtat de les operacions.
- Prevenir l'accés no autoritzat a la nostra xarxa i als nostres recursos.
- Promoure la consciència en ciberseguretat entre els empleats.

# 3. Àmbit i Context

El PSI s'aplica a tots els empleats i a tots els recursos informàtics de l'empresa, incloent-hi el nostre servidor, els equips informàtics i les connexions de xarxa. Es focalitza amb les següents amenaces:

- Infeccions de malware.
- Exfiltració d'informació sensible.
- Accés no autoritzat a la xarxa i als sistemes.

# 4. Polítiques de Seguretat

Les polítiques de seguretat són les bases que guiaran les pràctiques de seguretat dins de l'organització. Aquestes polítiques són fonamentals per establir un enfocament consistent i coherent cap a la seguretat de la informació i garantir que tot el personal entengui les seves responsabilitats i les expectatives en matèria de seguretat. A continuació, es detallen les polítiques de seguretat clau que es posaran en pràctica:

## 4.1. Política de Contrasenyes

La contrasenya és un element crític en la protecció de les nostres dades i sistemes. La política de contrasenyes estableix els següents requisits i procediments:

- **Complexitat:** Les contrasenyes han de ser complexes, amb una combinació de lletres, números i caràcters especials.
- **Canvi Regular:** Les contrasenyes han de canviar cada 90 dies com a mínim.
- **No Compartir:** Les contrasenyes no es poden compartir amb altres persones.

- **Autenticació de Doble Factor:** S'ha d'habilitar l'autenticació de doble factor per a tots els comptes d'accés a sistemes crítics.

### 4.2. Política d'Accés i Control

La política d'accés i control determina com es gestiona l'accés als nostres sistemes i dades:

- **Nivells d'Accés:** Es definiran nivells d'accés específics per als diferents rols i empleats, assegurant que només tinguin accés al que és necessari per al seu treball.
- **Gestió de Credencials:** Les credencials d'accés es gestionaran de manera segura i es revisaran periòdicament.
- **Control d'Accés Físic:** Es garantirà que les àrees on es troben els sistemes i la informació siguin segures i només accessibles per a personal autoritzat.
- **Auditoria d'Accés:** Es realitzarà una auditoria d'accés per revisar els registres i garantir que no hi hagi accés no autoritzat.

### 4.3. Política de Correu Electrònic Segur

El correu electrònic és una de les vies més comunes per a l'atac cibernètic. La política de correu electrònic segur inclourà:

- **Filtratge d'Atacs:** S'utilitzarà un programari de filtratge per identificar i bloquejar correus electrònics maliciosos.
- **Educació de l'Usuari:** El personal rebrà formació en la identificació de correus electrònics de phishing i altres amenaces.
- **Us de Firmes Digitals:** Es fomentarà l'ús de firmes digitals per verificar la autenticitat dels correus electrònics.

### 4.4. Política de Còpies de Seguretat

La política de còpies de seguretat és fonamental per a la protecció de les nostres dades:

- **Programa de Còpies de Seguretat:** Es desenvoluparà un programa de còpies de seguretat regulars per a tots els sistemes i dades crítics.
- **Almacenament Segur:** Les còpies de seguretat es mantindran en ubicacions segures, fora del lloc de treball principal.
- **Proves de Restauració:** Es realitzaran proves periòdiques per assegurar que les dades es puguin restaurar eficaçment en cas de pèrdua.

### 4.5. Política de Comunicació i Notificació d'Incidents

La política de comunicació i notificació d'incidents assegura una resposta ràpida i eficaç als incidents de seguretat:

- **Notificació d'Incidents:** Tots els incidents de seguretat s'han de notificar immediatament al responsable de seguretat.

- **Comunicació a les Parts Interessades:** Es comunicarà als afectats i a les parts interessades qualsevol incident de seguretat important.
- **Registres d'Incidents:** Es mantindran registres detallats de tots els incidents, les accions preses i

### 4.6. Protecció de Dades

La protecció de dades és essencial per mantenir la confidencialitat i la integritat de la informació. Aquestes mesures inclouran:

- **Xifrat:** Les dades sensibles emmagatzemades i en trànsit es xifrarà per protegir-les de l'accés no autoritzat.
- **Polítiques de Retenció:** Es definiran les polítiques de retenció de dades per garantir que les dades es conservin el temps necessari i s'eliminin de manera segura quan ja no siguin necessàries.
- **Protecció contra Malware:** S'implementarà programari de protecció contra malware en tots els sistemes per prevenir infeccions i atacs.

## 5. Procediments i Mesures de Seguretat

Aquest apartat descriu les mesures i els procediments de seguretat que s'implementaran per protegir els nostres sistemes, xarxes i dades.

### 5.1. Monitorització de la Xarxa

La monitorització de la xarxa és essencial per detectar activitats sospitoses i amenaces a temps. Les següents mesures es prendran per assegurar una monitorització adequada de la xarxa:

- **Firewall:** S'utilitzarà un firewall perimetral per controlar i supervisar el trànsit de xarxa que entra i surt de l'empresa. El firewall estarà configurat per bloquejar els ports no utilitzats i les connexions no autoritzades.

### 5.2. Monitorització dels Equips

La monitorització dels equips permet identificar la presencia de malware o l'ús maliciós dels equips a temps, bloquejant l'activitat i oferint capacitats de resposta.

- **Sistema d'Anàlisi i Resposta d'Endpoints (EDR):** Cada equip comptarà amb un EDR per a la detecció i la resposta a amenaces en temps real. Aquest sistema registrarà i analitzarà els comportaments anòmals i notificarà al personal de seguretat quan es detectin anomalies.

### 5.3. Centralització de Registres i SIEM

La centralització de registres i l'ús d'un Sistema d'Informació i Gestió d'Esdeveniments de Seguretat (SIEM) ajudarà a gestionar les dades de seguretat i a detectar amenaces de manera més efectiva:

- **SIEM:** S'implementarà un SIEM per a la recopilació, l'arxivament i l'anàlisi de registres de seguretat de tots els sistemes i equips. Això permetrà una visió centralitzada de l'entorn de seguretat i facilitarà la detecció d'activitats anòmales.

### 5.4. Implementació de VPN

Per garantir la seguretat de les connexions remotes a la xarxa de l'empresa, s'implementarà una xarxa privada virtual (VPN):

- **VPN:** S'establirà una VPN per a les connexions remotes, garantint que totes les comunicacions estiguin xifrades i segures. Els usuaris hauran d'utilitzar la VPN per accedir a recursos empresarials des de fora de l'oficina.

### 5.5. Autenticació de Doble Factor (2FA)

Per millorar la seguretat de l'accés als sistemes, s'implementarà l'autenticació de doble factor (2FA) per a tots els usuaris:

- **2FA:** Tots els usuaris hauran de configurar l'autenticació de doble factor per a tots els comptes d'accés a sistemes i aplicacions empresarials. Això afegirà una capa addicional de seguretat a les credencials d'accés.

### 5.6. Servei de Cyber Threat Intelligence (CTI)

Per estar al corrent de les amenaces actuals i les credencials exfiltrades, s'implementarà un servei de Cyber Threat Intelligence:

- **CTI:** S'utilitzarà un servei de CTI per obtenir informació actualitzada sobre amenaces cibernètiques, inclouent l'ús de credencials exfiltrades. Això permetrà prendre mesures proactives per protegir-se contra amenaces conegudes.

## 6. Gestió de Riscos

La gestió de riscos és un component fonamental per identificar, avaluar i abordar els riscos potencials per a la seguretat de la informació de l'empresa. Aquesta secció descriu les accions que es realitzaran per garantir una gestió eficaç dels riscos de seguretat:

### 6.1. Identificació de Riscos

S'identificaran tots els possibles riscos de seguretat que puguin afectar els sistemes, les dades i les operacions de l'empresa. Aquesta identificació inclourà:

- **Anàlisi de Vulnerabilitats:** Es realitzarà una anàlisi de les vulnerabilitats dels sistemes i les xarxes per identificar punts febles.
- **Avaluació de Threat Intelligence:** Es mantindrà un seguiment de la informació d'intel·ligència per conèixer les amenaces actives i emergents.

- **Revisió de Polítiques i Pràctiques Actuals:** Es revisaran les polítiques i les pràctiques actuals per identificar àrees on es puguin millorar les mesures de seguretat.

### 6.2. Avaluació de Riscos

Un cop identificats els riscos, es durà a terme una avaluació per determinar la seva probabilitat i impacte. Aquesta avaluació es basarà en:

- **Gravetat del Risc:** S'assignaran puntuacions de gravetat a cada risc, que inclouran impactes potencials en la confidencialitat, la integritat i la disponibilitat.
- **Probabilitat de Risc:** Es determinarà la probabilitat que es materialitzi cada risc, basant-se en dades històriques i informació de Threat Intelligence.

### 6.3. Mitigació de Riscos

Un cop avaluats els riscos, es prendran mesures per mitigar-los. Això inclourà:

- **Priorització de Riscos:** S'assignaran prioritats als riscos basant-se en la seva gravetat i probabilitat. Es donarà més atenció als riscos més alts.
- **Definició de Mesures de Mitigació:** Es desenvoluparan i implementaran mesures de mitigació específiques per a cada risc identificat. Aquestes mesures poden incloure la millora de polítiques de seguretat, la implementació de controls tècnics o canvis en les pràctiques operatives.
- **Assegurament de la Continuïtat de Negoci:** Les mesures de mitigació també es centraran en garantir la continuïtat de les operacions de l'empresa en cas de riscos importants o incidents de seguretat.

### 6.4. Revisió i Actualització Continua

La gestió de riscos no és un esforç únic, sinó un procés continu. Per tant:

- **Revisió Periòdica:** Es realitzaran revisions periòdiques de la gestió de riscos per assegurar-se que les mesures de mitigació siguin eficaces i s'adaptin als canvis en l'entorn de seguretat.
- **Actualització de Polítiques i Pràctiques:** Si es detecten canvis importants en els riscos o en les amenaces, es revisaran i actualitzaran les polítiques i les pràctiques de seguretat segons sigui necessari.
- **Formació i Consciència:** Es mantindrà una formació i una consciència contínua sobre la gestió de riscos per tot el personal de l'empresa per assegurar-se que estiguin al corrent dels riscos i les mesures de seguretat.

## 7. Formació i Consciència en Ciberseguretat

S'oferirà formació en ciberseguretat a tots els empleats per assegurar que siguin conscients de les amenaces cibernètiques i les millors pràctiques de seguretat.

### 7.1. Programa de Formació en Ciberseguretat

Es desenvoluparà un programa de formació en ciberseguretat que abasti tot el personal de l'empresa, independentment del seu rol. Aquest programa inclourà:

- **Sessions de Formació Inicial:** Tots els nous empleats rebran formació sobre les polítiques de seguretat de l'empresa i les millors pràctiques en ciberseguretat com a part de la seva inducció.
- **Formació Continuada:** Es proporcionarà formació regular a tot el personal per mantenir-los actualitzats sobre les amenaces actuals, les noves tècniques d'atac i les polítiques de seguretat actualitzades.
- **Simulacions d'Atacs:** Es realitzaran simulacions d'atacs per ajudar els empleats a reconèixer i respondre a amenaces cibernètiques reals. Aquestes simulacions també avaluaran la seva capacitat de resposta en cas d'incidents.

### 7.2. Consciència de la Ciberseguretat

A més de la formació, es promourà la consciència de la ciberseguretat a tot l'entorn de l'empresa:

- **Campanyes de Sensibilització:** Es realitzaran campanyes regulars de sensibilització en ciberseguretat per recordar al personal la importància de les mesures de seguretat i les seves responsabilitats.
- **Comunicació de les Amenaces Actuals:** El personal rebrà informació regular sobre les amenaces de ciberseguretat actuals, les tècniques d'atac i les tendències per mantenir-se alerta.
- **Polítiques de Denúncia d'Incidents:** Es proporcionarà als empleats una forma de denunciar incidents de seguretat o comportaments sospitosos, fomentant una cultura de reportar possibles amenaces.

### 7.3. Avaluació de la Formació i la Consciència

Es realitzaran avaluacions periòdiques per garantir l'eficàcia del programa de formació i consciència en ciberseguretat:

- **Proves de Coneixement:** Es realitzaran proves i avaluacions per assegurar-se que el personal comprengui les polítiques de seguretat i les millors pràctiques.
- **Simulacions d'Atacs i Escenaris:** Es realitzaran simulacions d'atacs i escenaris per avaluar la capacitat de resposta i l'aplicació de les habilitats apreses.
- **Enquestes d'Opinió:** Es realitzaran enquestes periòdiques per recollir les opinions del personal sobre el programa de formació i consciència, amb l'objectiu de millorar-lo contínuament.
- **Revisió de Resultats:** Es revisaran els resultats de les avaluacions per identificar àrees d'aprimament i realitzar ajustos en el programa segons sigui necessari.

## 8. Monitorització i Avaluació

Es realitzarà una supervisió contínua de la seguretat de la xarxa i dels sistemes per identificar possibles anomalies.

## 8.1. Supervisió en Temps Real

Es realitzarà una supervisió en temps real de les xarxes i els sistemes informàtics per identificar possibles incidents de seguretat. Això inclourà:

- **Sistemes de Registre:** Es configuraran sistemes de registre per registrar activitats i esdeveniments en els servidors i els dispositius de la xarxa.
- **Sensors de Seguretat:** Es desplegaran sensors de seguretat per supervisar el trànsit de la xarxa i identificar anomalies.
- **Alertes Automàtiques:** S'establiran alertes automàtiques per notificar l'equip de seguretat sobre possibles amenaces o activitats sospitoses.

## 8.2. Resposta a Incidents

Es desenvoluparà i es posarà en pràctica un pla de resposta a incidents per abordar ràpidament les amenaces de seguretat quan es detectin. Això inclourà:

- **Procediments d'Informe:** Es definiran procediments per informar sobre incidents de seguretat, incloent-hi el qui, el què i el com es notificarà a les parts interessades.
- **Classificació d'Incidents:** Es classificaran els incidents segons la seva gravetat i es respondrà en conseqüència.
- **Equip de Resposta a Incidents:** Es designarà i s'entrenarà un equip de resposta a incidents per abordar i mitigar les amenaces.
- **Seguiment i Informe Post-Incident:** Es realitzarà un seguiment i es prepararà un informe després de cada incident per aprendre'n i millorar les mesures de seguretat.

## 8.3. Auditoria de Seguretat

Es realitzaran auditories de seguretat periòdiques per avaluar el compliment de les polítiques de seguretat i les mesures implementades. Això inclourà:

- **Procediments d'Auditoria:** Es desenvoluparan procediments per realitzar auditories de seguretat, que inclouran la revisió de registres, la revisió de configuracions i l'avaluació de polítiques.
- **Auditories Internes i Externes:** Es podran realitzar auditories interns i, si escau, auditories externes realitzades per tercers de confiança.
- **Informes d'Auditoria:** Es generaran informes d'auditoria que destaquen les àrees d'èxit i les possibles àrees d'ampliació.
- **Accions Correctives:** Es prendran accions correctives en cas de trobar-se incompliments de polítiques o vulnerabilitats.

## 8.4. Actualització de Mesures

Es mantindran actualitzades les mesures de seguretat per adaptar-se a les amenaces en evolució i les noves tecnologies. Això inclourà:

- **Revisió Periòdica de Polítiques:** Es revisaran periòdicament les polítiques de seguretat per assegurar que siguin efectives i actuals.

- **Actualització de Programari:** Es mantindrà actualitzat el programari de seguretat, incloent-hi els sistemes operatius, els antivirus i altres eines de seguretat.
- **Avaluació de Vulnerabilitats:** Es realitzarà una avaluació regular de vulnerabilitats per identificar i abordar punts febles potencials.
- **Educació Continuada:** El personal de seguretat i tots els usuaris rebran formació continuada per estar al dia amb les noves amenaces i les millors pràctiques de seguretat.

## 9. Planificació de Continuïtat de Negoci

La planificació de continuïtat de negoci és una part crítica del nostre PSI, ja que ens permet assegurar que les operacions de l'empresa es puguin mantenir o restaurar ràpidament en cas d'incidents de seguretat, desastres naturals o altres esdeveniments inesperats. A continuació, es detallen els components i les accions associades a aquesta planificació:

### 9.1. Identificació de Funcions i Processos Clau

Hem identificat les funcions i els processos de l'empresa que són crítics per a la continuïtat de les operacions. Això inclou la gestió d'inventari, la gestió de vendes, les operacions de magatzem i el servei d'atenció al client. Cada un d'aquests processos es documentarà en detall per assegurar que es puguin recuperar ràpidament.

### 9.2. Avaluació de Riscos

Es realitzarà una avaluació de riscos específica per a la continuïtat de negoci per identificar les amenaces que poden afectar a aquests processos crítics. Aquesta avaluació ajudarà a prioritzar les mesures de mitigació de riscos.

### 9.3. Desenvolupament de Plans de Continuïtat

Es desenvoluparan plans de continuïtat detallats per a cada funció i procés crític identificat. Aquests plans inclouran les següents components:

- **Procediments d'Emergència:** Descripció de les accions a seguir en cas d'incident de seguretat o altres emergències.
- **Assignació de Responsabilitats:** Designació de responsables per a cada funció i procés en cas d'incident.
- **Recursos de Suport:** Identificació de recursos necessaris, com ara personal, equips i tecnologia, per a la recuperació.
- **Línies de Comunicació:** Establiment de línies de comunicació internes i externes per a notificar les parts interessades sobre l'incident i les accions preses.
- Procediments de Restauració: Descripció detallada de com restaurar els sistemes i les operacions a la normalitat.

- **Proves i Exercicis:** Programació de proves i exercicis regulars per assegurar que els plans de continuïtat siguin efectius.

### 9.4. Infraestructura de Reserva

Es disposarà d'una infraestructura de reserva fora del lloc de treball principal per a l'emmagatzematge de còpies de seguretat, l'operació de sistemes de backup i altres necessitats d'emergència. Aquesta infraestructura es mantindrà actualitzada i s'avaluarà periòdicament.

### 9.5. Formació i Consciència

S'ofereixrà formació específica en les accions de continuïtat de negoci per al personal responsable de la seva execució. Això garantirà que els membres de l'empresa siguin conscients de les seves responsabilitats en cas d'incident.

### 9.6. Proves i Revisions

Es realitzaran proves i revisions regulars dels plans de continuïtat per assegurar que estiguin actualitzats i siguin efectius. Aquestes proves ajudaran a identificar possibles mancances i àrees de millora.