

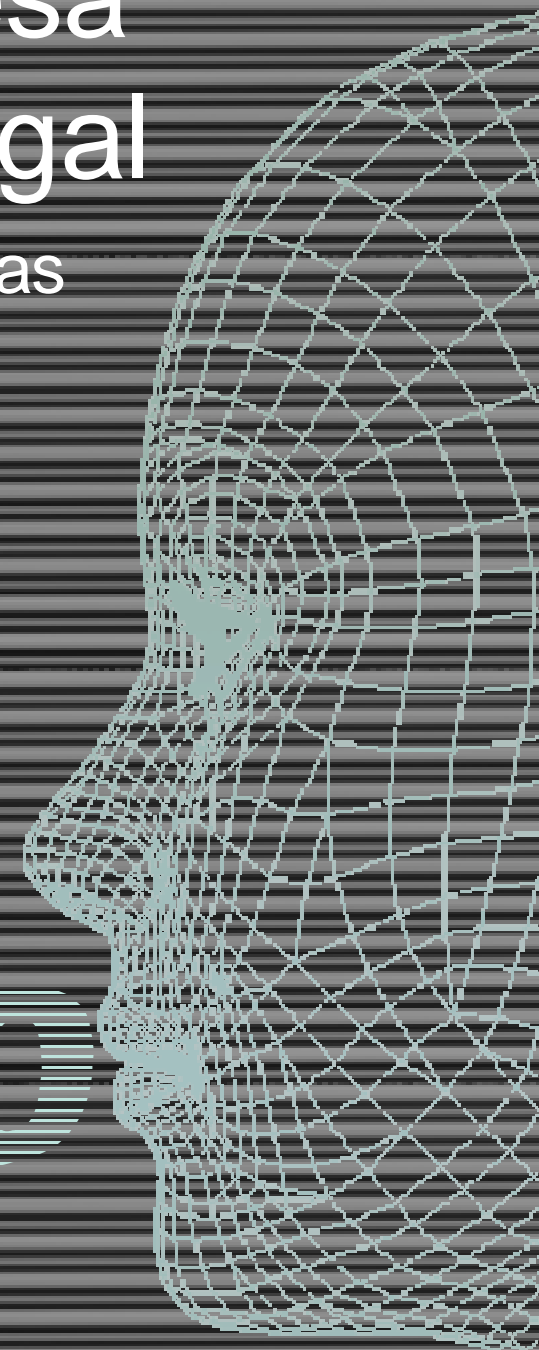
Vigilancia en la empresa

Una visión técnica y legal

Control de herramientas informáticas

Javier Prenafeta
Gabriel del Molino

00101100



IberCaja

Salud y Cuentas

¡Así que sí!

Vigilancia en la empresa. Una visión técnica y legal.



Javier Prenafeta
Abogado
Gabriel del Molino
Gerente de CAMYNA

VIGILANCIA EN LA EMPRESA

- 17-1-2006

Vigilancia con cámaras

- 24-1-2006

Control de herramientas informáticas (internet, correo, etc)

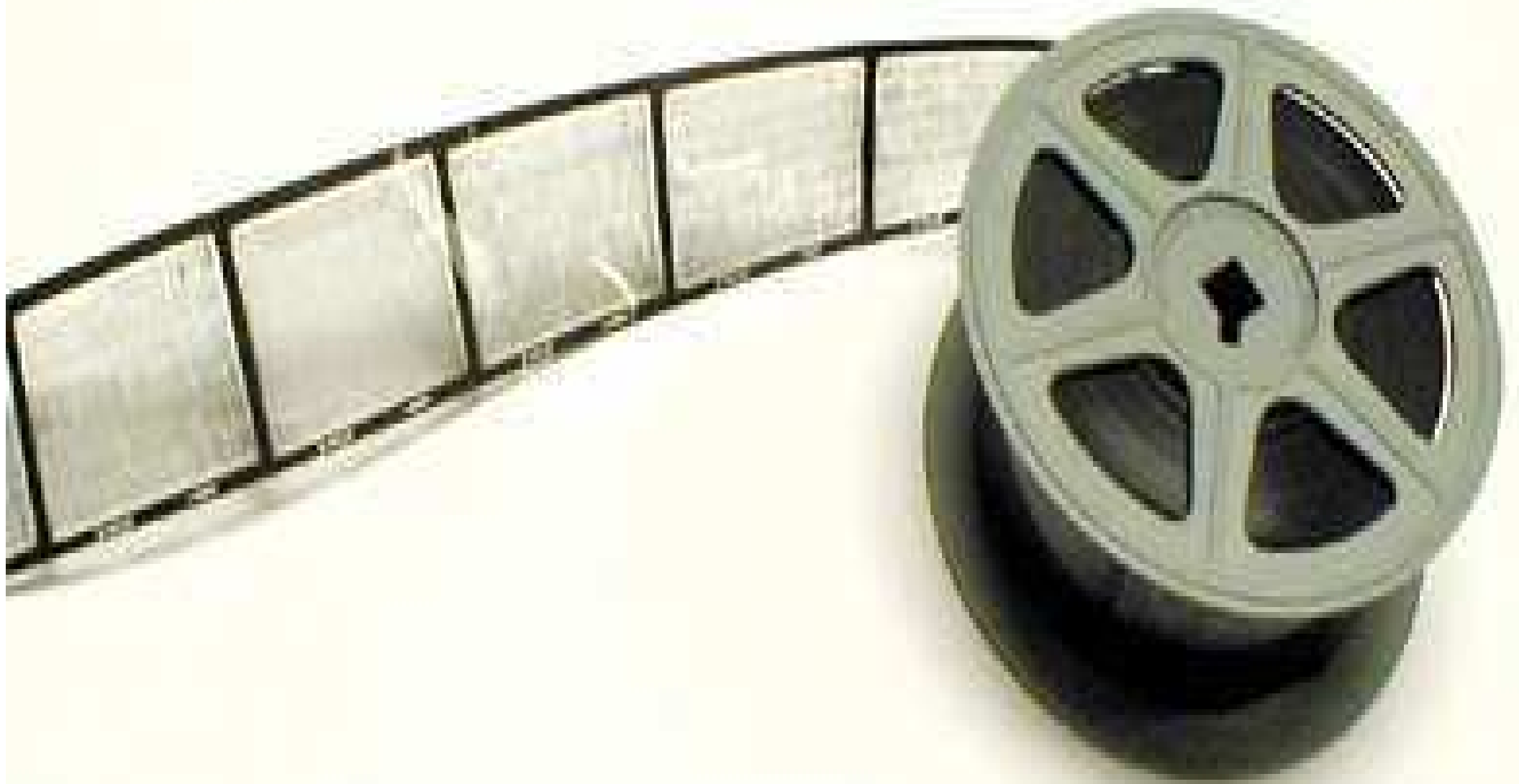


¿Seguridad?



¿Intromisión?

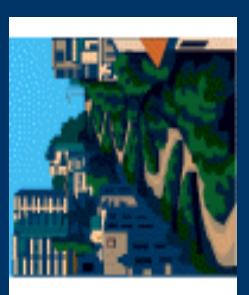
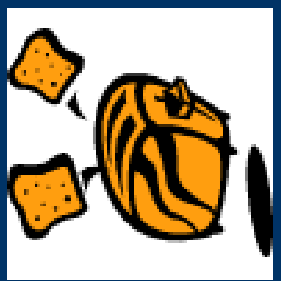
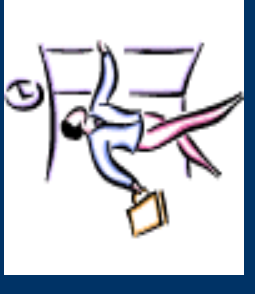
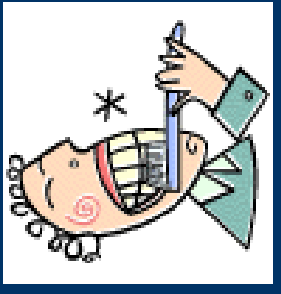
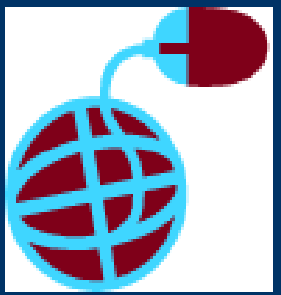
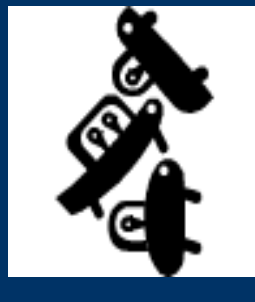
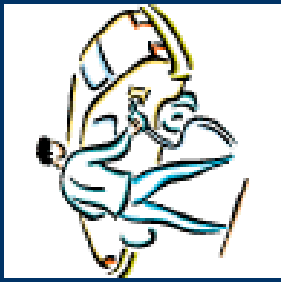




ZENTRUM GOLDEN MAYER PRESENTA:

Un día en la vida de.....





Pero... ¿que ha ocurrido durante este día?

Ha sido visto (y grabado) por mas de 100 cámaras

- En el garaje
- En la calle
- En la gasolinera
- En su empresa
- En la empresa de su cliente
- En el metro
- ...



CORREO ELECTRÓNICO

Técnico / Legal

Posibles riesgos e infracciones

- Fuga de información confidencial y datos personales
- Entrada y difusión de virus, troyanos y programas nocivos
- Envío de comunicaciones comerciales no deseadas (spam)
- Pérdida de tiempo de trabajo
- Lesión de imagen de empresa
- Amenazas, injurias o calumnias

Soluciones

- Correo POP3 / IMAP
- Control del correo
- Uso del antivirus

Net Logger pro

Outlook Attachment Sniffer

Titularidad y usos permitidos

Privacidad y accesos

- Correo corporativo
- Correo personal

ACCESOS INALAMBRICOS

Técnico / Legal

Posibles riesgos

Vulnerabilidad en la seguridad informática

Accesos no deseados a información confidencial de la empresa

Fuga de propiedad intelectual y datos personales

Soluciones

Formación adecuada

Conocimiento real de la situación

Actualizaciones de software

Utilizar políticas restrictivas de uso

Net Stumbler

AirSnare

Boingo

Aircrack

INTERNET

Técnico / Legal

Posibles riesgos e infracciones

- Entrada de virus, troyanos y programas nocivos
- Acceso a contenidos nocivos o ilegales
- Pérdida de tiempo de trabajo
- Acceso a banca on-line

Usos permitidos

Soluciones

- Control de tráfico
- Log de visitas
- Cookies
- Histórico
- Chat / Messenger

Parent tools for AIM

Silius Log Analyzer

Web cop

Intimidación y privacidad del trabajador

USO P2P

Técnico / Legal

Posibles riesgos e infracciones

Descarga de contenidos ilegales o nocivos

Infracción de propiedad intelectual o industrial de terceros

Introducción y difusión de información confidencial de la empresa en redes P2P

Soluciones

Política de puertos

Cortafuegos

Instalación de software

Control de tráfico

FjSniffer

Zone Alarm

Programas anti-instalación software

Posible responsabilidad civil/penal de la empresa frente a terceros

ACCESO REMOTO

Técnico / Legal

Control remoto de máquinas

Posibles riesgos

Accesos no deseados a información confidencial y datos personales de la empresa

Soluciones

Mecanismos de control de acceso
Detección de pulsaciones
Monitoreo

Remote Desktop Inspector

Sys Keylog

OTRAS INCIDENCIAS

Técnico / Legal

Instalación de *software*
Uso de *pen-drive* / *USB Disk*
Memorias Flash

Posibles riesgos

Fuga de información confidencial y datos personales de la empresa
Introducción de virus, troyanos y programas nocivos

Soluciones

“Congelación” de ordenadores

Programas anti-instalación software

TECNICAS FORENSES

Técnico / Legal

Se realizan una vez cometido el delito
Son técnicas lentas

Análisis de las otra técnicas comentadas

Logs

Caché

Cookies

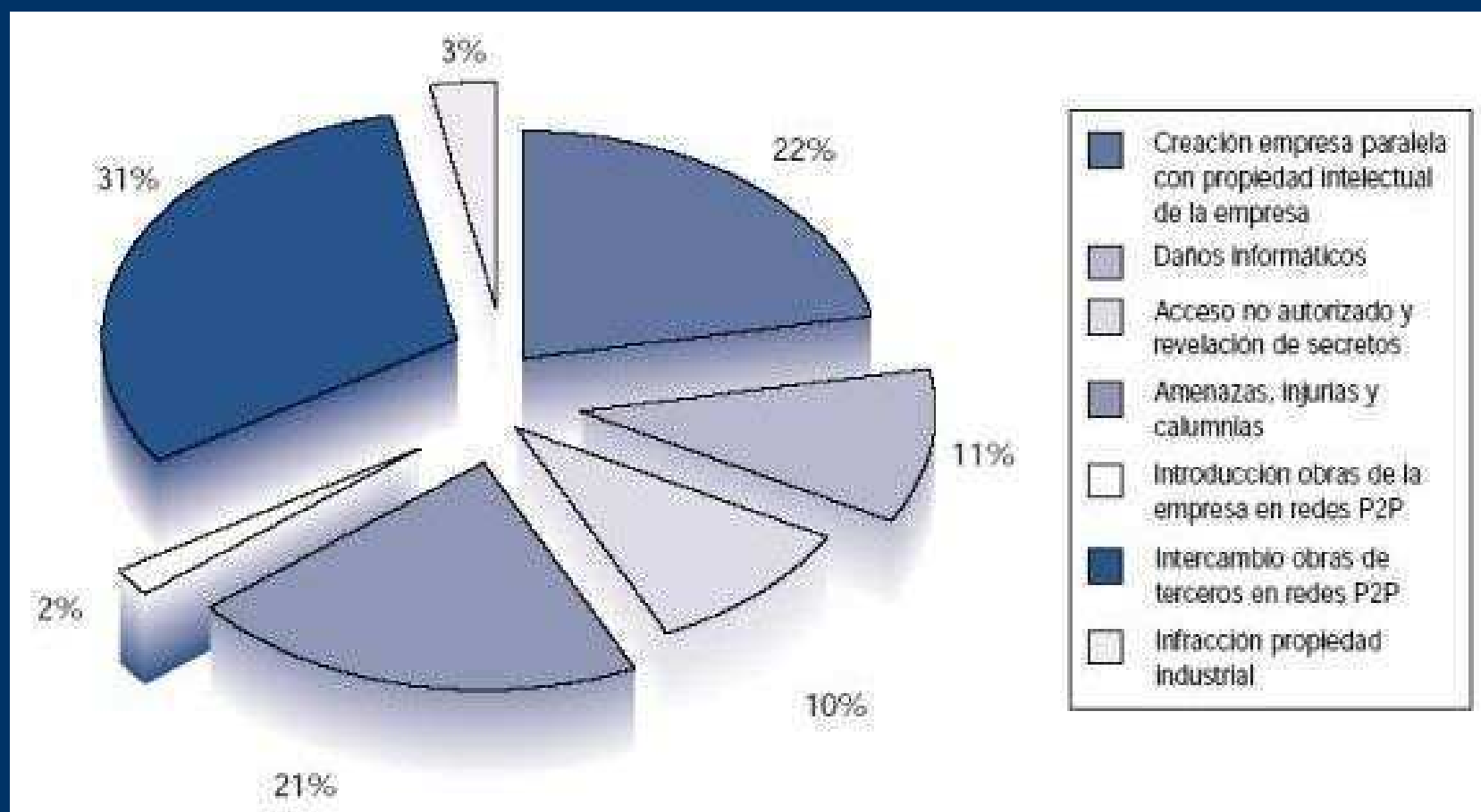
Disco duro

Soluciones

“Congelación” de ordenadores

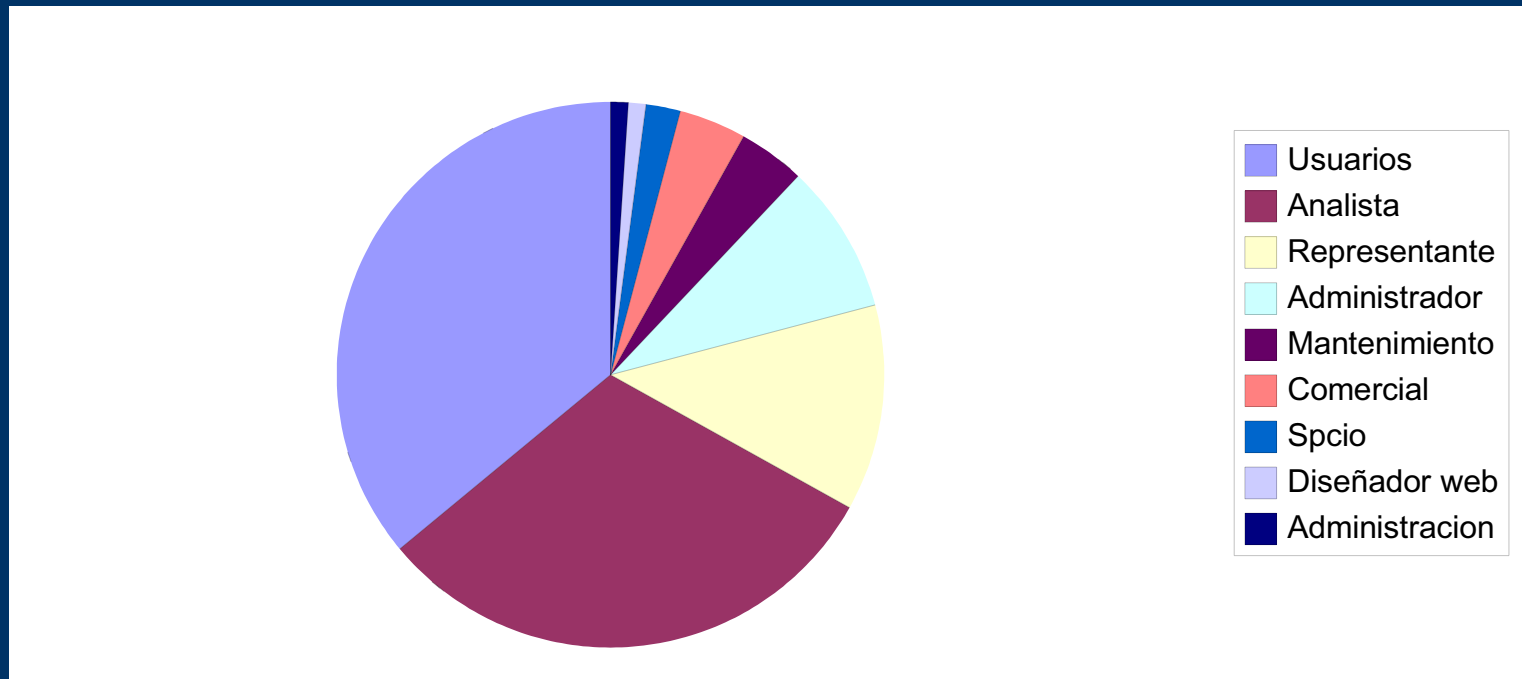
Uso de memorias flash

Infracciones más habituales



Fuente: "Actos desleales de trabajadores usando sistemas informáticos e Internet"
Landwell – PriceWaterhouseCoopers 2004

El 36% de los infractores son usuarios genéricos de la red corporativa.



*Fuente: "Actos desleales de trabajadores usando sistemas informáticos e Internet"
Landwell – PriceWaterhouseCoopers 2004*

El motivo principal (55%), es el ánimo de lucro, seguido muy de cerca por el conflicto laboral o despido injusto.

El 81% de los casos, los perjuicios no llegan a 60.000 €

*Fuente: "Actos desleales de trabajadores usando sistemas informáticos e Internet"
Landwell – PriceWaterhouseCoopers 2004*

Política de Empresa

Uso de las herramientas informáticas

1. Objeto y finalidad
 2. Propiedad y especificaciones de los equipos
 3. Posición de la empresa en cuanto al uso de herramientas informáticas
 4. Acceso y medidas de seguridad de los equipos
 - Política de contraseñas
 - Gestión de incidencias
 - Gestión de copias de seguridad y respaldo
 5. Uso del correo electrónico
 - Riesgos y ventajas
 - Correo personal y correo de empresa
 - Seguridad y confidencialidad
 - Status legal de los mensajes
 - Información que debe incluirse en el mensaje y firma
 - Gestión de los mensajes
 - Corrección y tono de los mensajes
 - Responsabilidad del usuario
 - Tratamiento de mensajes inapropiados recibidos
 - Seguimiento y control del correo electrónico
-
-

Política de Empresa

uso de las herramientas informáticas

1. Navegación por Internet
 - Riesgos y ventajas
 - Medidas de seguridad
 - Restricciones a la navegación
2. Programas y dispositivos de control y monitorización
3. Uso de dispositivos portátiles de almacenamiento
4. Consecuencias derivadas del incumplimiento de la Política
 - Infracciones laborales
 - Sanciones disciplinarias
 - Posible responsabilidad civil/penal

Cláusulas contractuales:

- uso de herramientas informáticas
 - confidencialidad
-
-

Vigilancia en la empresa. Una visión técnica y legal.



No olviden preguntar

Javier Prenafeta Abogado (jp@jprenafeta.com)

Gabriel del Molino Gerente de CAMYNA (info@camyna.com)

[Presentación disponible en : www.camyna.com/zentrum](http://www.camyna.com/zentrum)