**Diseño de un plan compliance para empresa informática**



Daniel Escaño Hernández CET Ciberseguridad

# **Índice**

[**Índice**](#_u3m2w22qmzkq) **1**

[**1. Analisis y gestion de riesgos penales**](#_yby49ic4bcux) **2**

[**2. Definición de protocolos y procedimientos para la toma de decisiones en la organización y modelo de respuesta ante el riesgo de comisión de un delito.**](#_nxv48312gmzl) **3**

[**3. Establecimiento de un Código Ético.**](#_ms4u5z4euuam) **4**

[**4. Establecimiento de un canal de denuncia interna y régimen disciplinario**](#_4omoo0smo5pr) **5**

[**5. Desarrollo e impartición de programas de formación y sensibilización**](#_kb7qw31k3btq) **6**

[**6. Establecimiento de un registro de evidencias**](#_rbje6fp43u7b) **7**

[**7. Establecimiento de un programa de auditoría y verificación periódica del plan.**](#_am2yzoeow7l8) **8**

# **1. Analisis y gestion de riesgos penales**

Lo primero es la creación de una tabla de riesgos en el que se identifiquen los riesgos a lo que se enfrenta la organización, y los delitos a los que puede estar expuesta.

Como pueden ser la gestión de la seguridad de la información y protección de datos, recursos humanos, prevención y blanqueo de capitales, marketing, propiedad intelectual, etc.

Ademas de delitos económicos, discriminación, falta de licencias, etc.

| Riesgo | Delito | Probabilidad | Impacto |
| --- | --- | --- | --- |
| Revelar datos personales | Descubrimiento y  revelación de secretos y  allanamiento  informático | Media | Alto |
| Aceptar pagos con fondos de procedencia ilícita | Descubrimiento y  revelación de secretos y  allanamiento  informático | Media | Grave |
| Operar con softwares carentes de licencias | Delito contra la propiedad intelectual | Alta | Medio |
| Discriminacion (Racial, étnica, etc..) | Delito de odio | Baja | Alto |
| Fraude (Fiscal, contractual, etc..) | Fraude | Media | Alta |

# **2. Definición de protocolos y procedimientos para la toma de decisiones en la organización y modelo de respuesta ante el riesgo de comisión de un delito.**

Los protocolos consisten en las pautas de actuación requeridas ante las posibles situaciones que se puedan dar dentro de la empresa. Estos protocolos deben ser conocidos por todos los miembros de la empresa, desde el primer trabajador hasta los altos directivos.

Suelen seguir esta estructura:

- Objetivo y finalidad.

- Ámbito de aplicación.

- Principios de actuación.

- Procedimiento y actuaciones.

- Régimen sancionador.

- Control, revisión y formación.

- Comunicación y denuncia.

| Situación | Procedimiento | Regimen sancionador |
| --- | --- | --- |
| Descubrimiento y  revelación de secretos y  allanamiento  informático | Implantación de medidas regulatorias tales como monitorización activa tanto de la información como de los empleados. | Penal |
| Delito contra la propiedad intelectual | Implantación de software especializado en detección de carencia de licencias.  Sustituir el software por una opción de código libre. | Administrativo |
| Delito de odio | Despido inmediato del trabajador | Penal/Administrativo |
| Fraude | Implementación de un contable o algún responsable a nivel de finanzas que vigile todos los movimientos económicos. | Penal |

# **3. Establecimiento de un Código Ético.**

La estructura del código ético puede seguir un modelo como el siguiente:

1. Introducción y valores corporativos.

2. Ámbito de aplicación y sujetos afectados.

3. Contenidos y medidas del código.

4. Proceso sancionador y vigencia del código ético.

Es importante para la empresa garantizar un comportamiento ético y responsable de todos sus integrantes, más allá del mero cumplimiento de la Ley.

Este Código vincula a todo el personal, independientemente de la posición y función que se desempeñe. La aplicación del Código, total o parcial, podrá hacerse extensiva a cualquier persona física y/o jurídica relacionada con la empresa, cuando así convenga para el cumplimiento de su finalidad y sea posible por la naturaleza de la relación.

Ninguna persona, independientemente de su nivel o posición, está autorizada a solicitar a un empleado que contravenga lo establecido en este código, del mismo modo que ningún empleado podrá justificar una conducta impropia o ilegal amparándose en una orden superior.

En la empresa somos conscientes de la importancia que tienen las personas que componen nuestra compañía. Los empleados son la voz y marca de la compañía, contamos con personas implicadas y comprometidas, que marcan la diferencia. Por eso es fundamental mantener los siguientes compromisos:

* Principios de no discriminación e igualdad de oportunidades, respeto por la dignidad, integridad e intimidad
* Derechos Laborales. Seguridad y Salud en el trabajo
* Selección y Evaluación
* Formación
* Confidencialidad. Información reservada y confidencial. Protección de datos.
* Relación con clientes
* Transparencia e integridad en la comunicación
* Relación con proveedores
* Administración de Código Ético

# **4. Establecimiento de un canal de denuncia interna y régimen disciplinario**

Se establecerá como canal para comunicar cualquier incidencia una dirección

de correo electrónico, con acceso restringido al responsable del canal, que actuará como Responsable de Prevención de Riesgos Penales.

Deberá garantizar el ejercicio de los derechos conferidos por la normativa vigente en materia de protección de datos, especialmente, respecto del denunciado, sus derechos de acceso, rectificación, cancelación y oposición.

En ningún caso se deberá identificar al denunciante como consecuencia del ejercicio del derecho de acceso por parte del denunciado.La naturaleza del sistema de denuncias internas hace previsible que puedan ser objeto de tratamiento datos especialmente protegidos lo que conlleva la necesidad de implantar medidas de seguridad de nivel alto.

En caso de que fuese necesario, se realizarán las denuncias de acuerdo con el sistema judicial de cada una de las jurisdicciones.

# **5. Desarrollo e impartición de programas de formación y sensibilización**

Definir el sistema establecido para la realización de actividades de sensibilización y formación del personal, actualizando constantemente sus conocimientos para un mejor comportamiento de nuestra organización.

Entrando en detalle, podemos enumerar los objetivos siguientes:

* Informar o recordar a todos los empleados la política, los objetivos y las líneas estratégicas generales.
* Modificar el comportamiento, la actitud y el enfoque de empleados

Formación dirigida a recordar ideas y conceptos generales de calidad Tiene como finalidad que la formación sea continua. La información proporcionada será muy similar a la que se aportó cuando se implantó el Sistema de Gestión de la Calidad, pero incluyendo matices nuevos.

Formación dirigida a mejorar la competencia profesional del personal Este tipo de formación es necesaria porque la competencia profesional del personal siempre se puede mejorar. Además, continuamente se producen cambios tecnológicos y organizativos en todas las organizaciones. El trabajador necesita ser formado con conocimientos teóricos y también requiere habilidades y experiencia. Conviene que tengan formación sobre los métodos y la capacitación necesaria para realizar sus tareas de forma eficaz.

Formación del personal de nuevo ingreso

Formación específica de cada puesto de trabajo El empleado tendrá que conocer los procedimientos, las instrucciones técnicas, las normas, etc… del Sistema de Gestión de la Calidad aplicables a su puesto de trabajo. Esta formación teórica se tendrá que completar con sesiones prácticas de aprendizaje.

Estos procesos de sensibilización adquieren especial relevancia en la primera etapa del proceso de desarrollo e implantación del Sistema de Gestión de la Calidad. Es en ese momento cuando la organización deberá esforzarse en establecer un entorno adecuado que propicie el cambio de cultura requerido para la aplicación de la Política de Calidad adoptada. Uno de los métodos más eficaces es el desarrollo de una acción formativa e informativa dirigida a todos los niveles de la organización.

Entre sus objetivos fundamentales tendrá la divulgación de los valores que configuren la nueva cultura de calidad de la organización y los beneficios que esto representa.

# **6. Establecimiento de un registro de evidencias**

Los registros pueden utilizarse por ejemplo, para proporcionar evidencia de verificaciones, acciones preventivas y acciones correctivas. En general los registros no necesitan estar sujetos al control del estado de revisión, como ocurre con el resto de documentos del sistema, pues una vez cumplimentados no varían.

En este procedimiento documentado ha de reflejarse qué hace la organización para asegurar la identificación de cada registro, el modo de archivarlos y de protegerlos, cuánto tiempo han de mantenerse, etc.

| Listado de evidencias | | | |
| --- | --- | --- | --- |
| Título | Código | Responsable | Tipo |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# **7. Establecimiento de un programa de auditoría y verificación periódica del plan.**

El programa de Auditoría, presenta en forma lógica las instrucciones para que el Auditor o el personal que trabaja una Auditoría, pueda seguir los procedimientos que debe emplearse en la realización del examen.

En general el programa de Auditoría, en cuanto a su contenido incluye los procedimientos específicos para la verificación de cada tipo de activo, pasivo y resultados, en el orden normal que aparecen en los estados económicos y financieros de la empresa.

El programa de Auditoría, tiene como propósito servir de guía en los procedimientos que se van adoptar en el curso de la Auditoría, y, servir de lista y comprobante de las fases sucesivas de la Auditoría, a fin de no pasar por alto ninguna verificación.

El programa no debe ser rígido, sino flexible para adaptarse a las condiciones cambiantes que se presenten a lo largo de la Auditoría que se está practicando.

El programa de Auditoría, es un enunciado lógicamente ordenado y clasificado, de los procedimientos de Auditoría que se van a emplear, la extensión que se les va a dar y la oportunidad en la que se aplicarán. En ocasiones se agregan a estas algunas explicaciones o detalles de información complementaria tendientes a ilustrar a las personas que van a aplicar los procedimientos de Auditoría, sobre características o peculiaridades que debe conocer.