**Incidentes de ciberseguridad**

# TAXONOMÍA y notificación de 3 delitos relevantes

# 

# 

**Índice**

[**TAXONOMÍA y notificación de 3 delitos relevantes**](#_sl9r1sd4meb8) **1**

[**Índice**](#_z77repcs18xk) **2**

[**Enunciado**](#_ky10xjqo1y5) **3**

[**Introducción**](#_uum4xmq3fbs7) **4**

[**Objetivo**](#_qewkki8jx475) **4**

[**Contexto**](#_xe6k5fv8eg) **4**

[Nivel de peligrosidad según la guía nacional de notificación y gestión de incidentes](#_sm6g6upa758g) 5

[Delitos](#_fldx3eng97ur) 7

[Revelación de secretos](#_7dyufmc583va) 7

[Clasificación:](#_m8a0475skvqn) 8

[Estafas bancarias y de páginas web.](#_ptehxoxstda) 8

[Clasificación:](#_yy3lihkkhqe8) 8

[Estafa del CEO](#_pdrtd0pauncj) 8

[Clasificación](#_tkgyljm5w5ua) 9

[Notificación](#_5w33no1p9e8f) 9

# Enunciado

1. INVESTIGA 3 de los delitos de la policía A QUE SE REFIERE Y COMO AFECTA A LA EMPRESA (con una breve introducción) Y A QUE TIPO DE INCIDENTE CORRESPONDE SEGÚN EL CUADRO DE LA TAXONOMÍA.

Clasificación del incidente y ¿Por qué lo clasificas ahí?

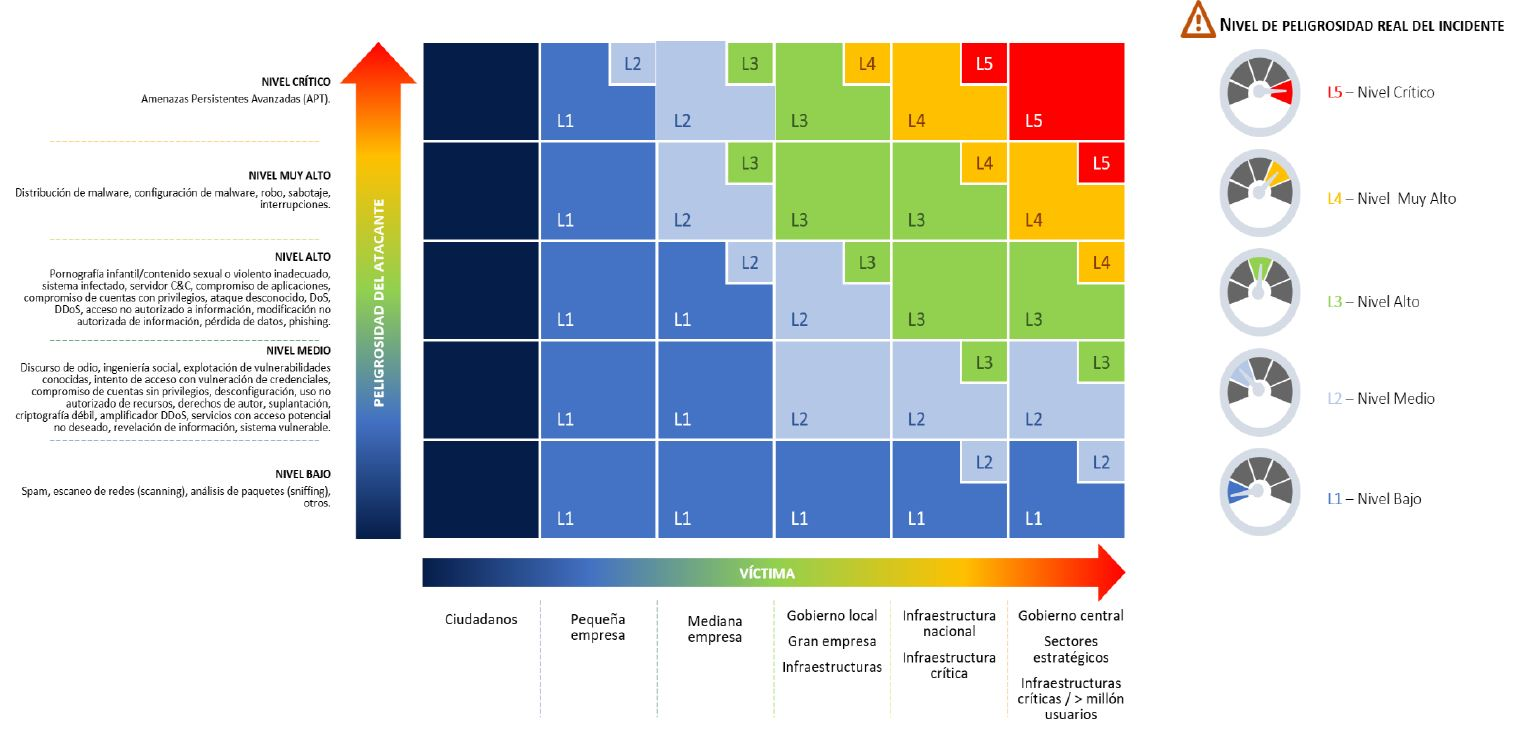
1. - LOCALIZA EL NIVEL DE PELIGROSIDAD SEGÚN LA IMAGEN

¿Tienes que notificarlo? y ¿cuál es la ventana de tiempo y tratamiento de la notificación?

Busca en la guía nacional de notificación de incidentes, s**i tengo que notificarlo y cuanto tiempo tengo**.

1. - CUANDO SEPAS EL NIVEL DE **PELIGROSIDAD** DE CADA DELITO (bajo, medio, alto muy alto, crítico) Y LAS **VENTANAS** de notificación, así como su procedimiento Investiga las entidades relacionadas.

# Introducción



# 

# 

# Objetivo

Análisis de los delitos relevantes expuestos por la guardia civil, explicación de las repercusiones a la empresa y categorización por taxonomía.

# Contexto

**Taxonomía empleada por INCIBE-CERT y la guía de Notificación y Gestión de Ciberincidentes**

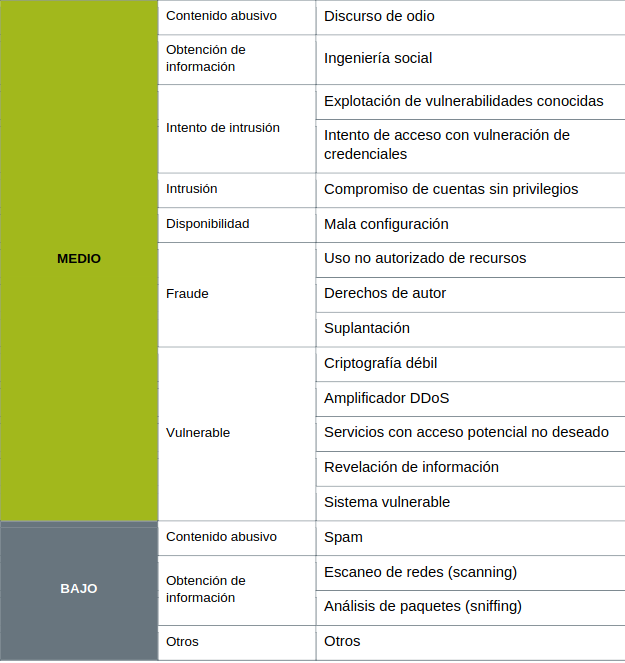
Busca armonizar los enfoques de análisis, evaluación de impacto, contención, tratamiento y estudio de incidentes, con la finalidad de establecer políticas coherentes y desarrollar respuestas colaborativas entre distintas organizaciones.

Tipos:

* Contenido abusivo
* Contenido dañino
* Obtención de información
* Intento de intrusión
* Intrusión
* Disponibilidad
* Compromiso de la información
* Fraude
* Vulnerabilidad
* Otros (ataques dirigidos, ciberterrorismo)

## Nivel de peligrosidad según la guía nacional de notificación y gestión de incidentes

## 



## 

## Delitos

### Revelación de secretos

Este incidente involucra la divulgación no autorizada de información confidencial o secreta. Puede ocurrir en diversas situaciones, como filtraciones de datos, hackeos a sistemas informáticos, o revelación de información clasificada. La revelación de secretos puede tener graves consecuencias tanto para individuos como para organizaciones, ya que compromete la privacidad y la seguridad de la información.

#### Clasificación:

Nivel de peligrosidad **Medio**

* **Vulnerable → Revelación de información.**

##### Notificación

Las incidencias de nivel medio no son de obligada notificación.

### Estafas bancarias y de páginas web.

Se refiere a prácticas fraudulentas diseñadas para obtener acceso no autorizado a cuentas bancarias o información financiera en línea. Los estafadores utilizan diversos métodos, como phishing (engaño para obtener información confidencial), malware, o suplantación de identidad, para robar datos financieros y cometer fraudes. Estas estafas pueden resultar en pérdidas económicas significativas para las víctimas.

#### Clasificación:

Nivel de peligrosidad **Alto**

* **Fraude → phishing**

##### Notificación

Las incidencias de nivel medio no son de obligada notificación.

### Estafa del CEO

También conocida como "phishing de ejecutivos" o "fraude del presidente", esta estafa implica engañar a empleados de una empresa para que realicen transferencias de fondos u divulguen información confidencial creyendo que están siguiendo órdenes legítimas del CEO u otro alto ejecutivo. Los estafadores suelen utilizar técnicas de ingeniería social para manipular a los empleados y obtener acceso a recursos financieros de la empresa. Este tipo de estafa se basa en la confianza y la urgencia para lograr su cometido.

#### Clasificación

Nivel de peligrosidad **Medio**

* **Fraude → Suplantación.**

##### **Notificación**

“Los incidentes se asociarán a uno de los niveles de peligrosidad e impacto establecidos en este apartado, teniendo en cuenta la obligatoriedad de notificación de todos aquellos que se categoricen con un nivel **CRÍTICO, MUY ALTO O ALTO** para todos aquellos sujetos obligados a los que les sea aplicable normativa específica de acuerdo a lo contemplado en esta “Guía nacional de notificación y gestión de ciberincidentes” en función de su naturaleza”

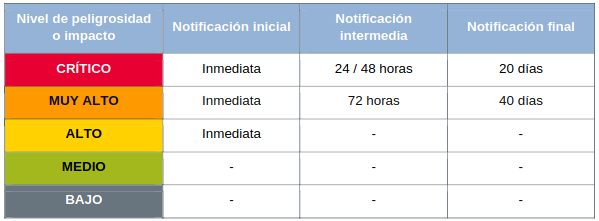
[*Guía nacional de notificación y gestion de incidentes de ciberseguridad*](https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf)

Entre los tres delitos seleccionados solo sería necesario la notificación del incidente nivel de *peligrosidad alto* relacionado con **estafas bancarias y de páginas web**.

Las notificaciones pueden contar con tres fases definidas como:

* La **notificación inicial** es una comunicación consistente en poner en conocimiento y alertar de la existencia de un incidente.
* **La notificación intermedia** es una comunicación mediante la que se actualizarán los datos disponibles en ese momento relativos al incidente comunicado.
* La **notificación final** es una comunicación final mediante la que se amplían y confirman los datos definitivos relativos al incidente comunicado

En el caso concreto de incidentes de **alto nivel**, solamente será necesaria la **notificación inicial** a las autoridades competentes.



Entidades relacionadas

Bibliografía

* <https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md>
* <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf>