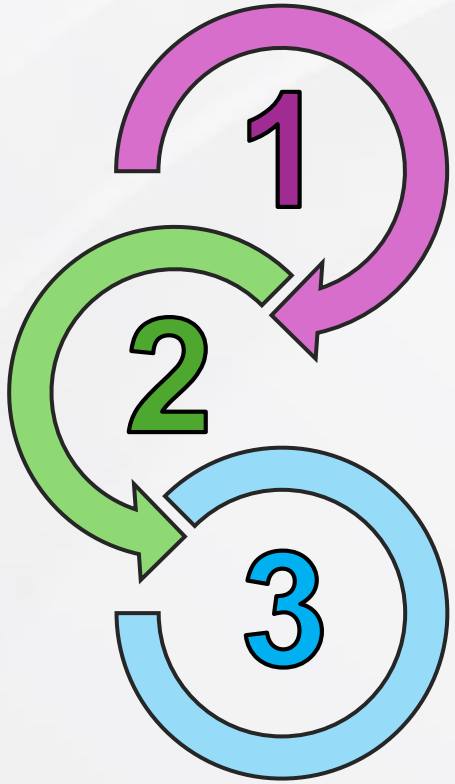
BABEL

FUNDACIÓN COMPLUTENSE

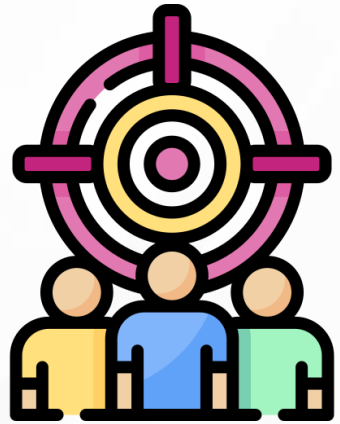
# Esquema Nacional de Seguridad

# Objetivos de la sesión formativa

La presente sesión formativa tiene por finalidad conseguir los siguientes **objetivos**:




- Introducción de **aspectos relevantes** del Real Decreto 311/2022 - Esquema Nacional de Seguridad (ENS)
- Conocer el **estado actual** de seguridad de FGUCM
- Exponer **directrices de seguridad específicas** en FGUCM



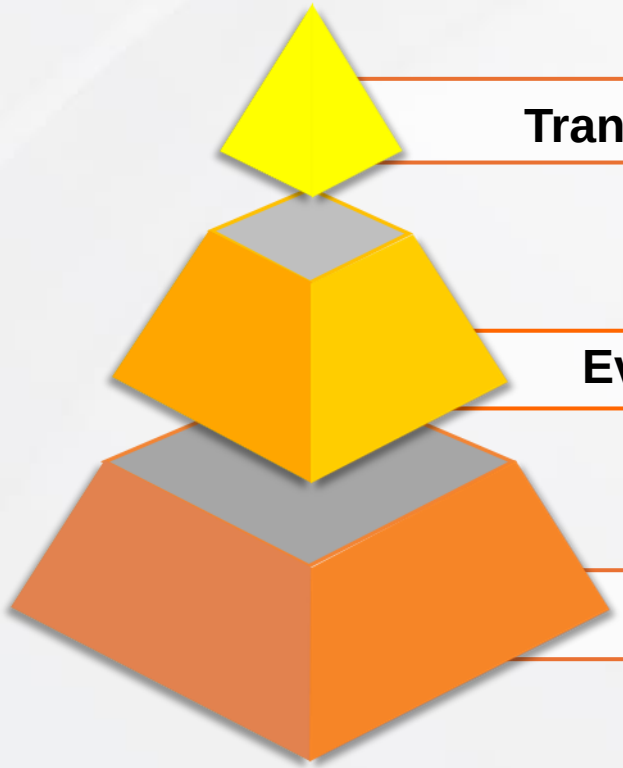
# Introducción

- Contexto y antecedentes del ENS
- Objetivos del ENS
- Importancia del ENS

# Introducción al ENS

Contexto y antecedentes del ENS

El Esquema Nacional de Seguridad (ENS) es una **norma de obligado cumplimiento** para la protección de la información de los organismos públicos y sus proveedores.



**Transformación Digital**

La creciente **digitalización de los servicios** ha aumentado la necesidad de garantizar la seguridad.

**Evolución Normativa**

Se creó en 2010, y desde entonces **ha evolucionado** para adaptarse a nuevas amenazas y tecnologías

**Ciberseguridad**

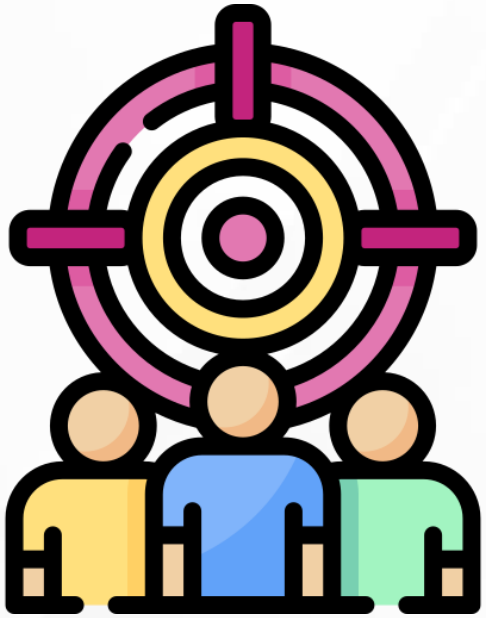
La ciberseguridad se ha convertido en un tema crítico debido al **incremento de ciberataques** tanto en frecuencia como en sofisticación

# Introducción al ENS

Objetivos del ENS

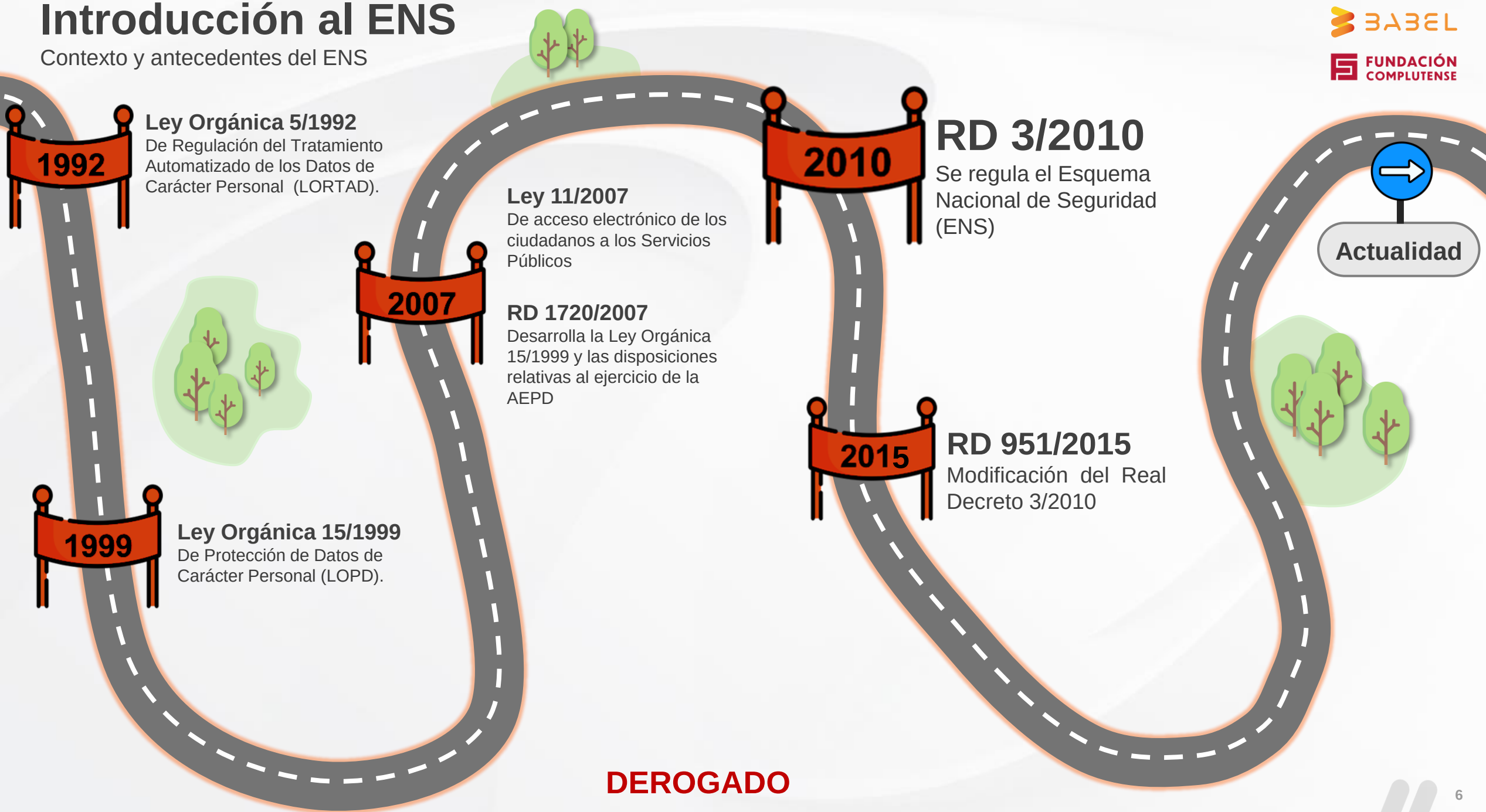
El Esquema Nacional de Seguridad tiene como **objetivos**:

1. **Proteger los sistemas.** Garantizar la protección de la información tratada y los servicios prestados por las entidades públicas.
2. **Seguridad Integral.** Establecer principios y requisitos mínimos que aseguren la seguridad de los sistemas de información.
3. **Confianza.** Generar confianza en los ciudadanos y las administraciones públicas en el uso de medios electrónicos.



# Introducción al ENS

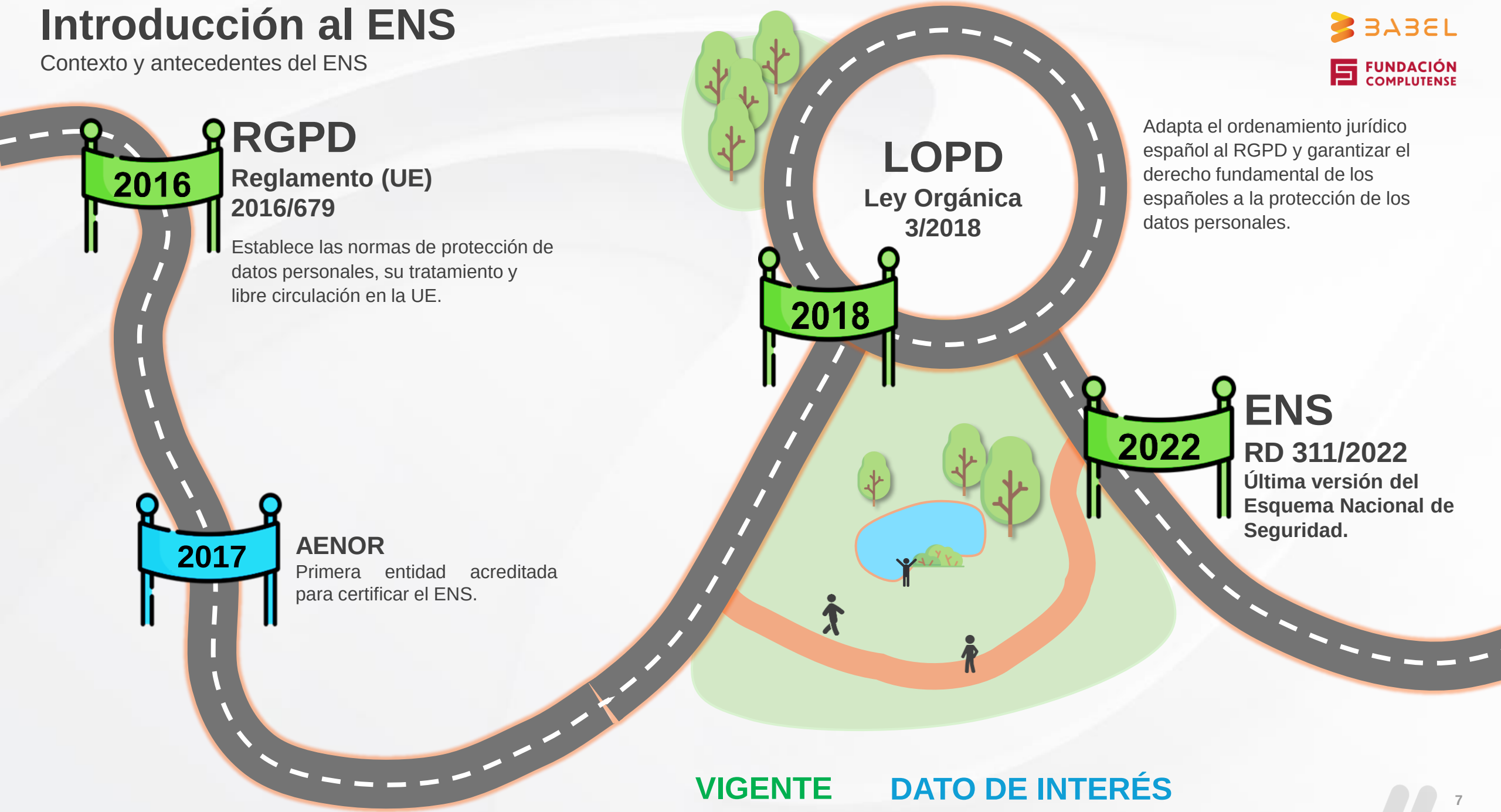
Contexto y antecedentes del ENS




**DEROGADO**

# Introducción al ENS

Contexto y antecedentes del ENS



## 2016 RGPD

**Reglamento (UE) 2016/679**

Establece las normas de protección de datos personales, su tratamiento y libre circulación en la UE.

## 2017 AENOR

Primera entidad acreditada para certificar el ENS.

## 2018 LOPD

**Ley Orgánica 3/2018**

Adapta el ordenamiento jurídico español al RGPD y garantizar el derecho fundamental de los españoles a la protección de los datos personales.

## 2022 ENS

**RD 311/2022**

**Última versión del Esquema Nacional de Seguridad.**

VIGENTE DATO DE INTERÉS

# Conceptos clave del ENS

- El Esquema Nacional de Seguridad
- Categorización de los sistemas de información
- Principios básicos vs requisitos mínimos
- Gestión de la seguridad basada en los riesgos
- Prevención, detección, respuesta y conservación
- Principales perfiles de usuario

# Conceptos clave del ENS

El Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad (ENS) establece los **principios básicos y requisitos mínimos** que deben cumplir garantizar la seguridad de los servicios.

Está constituido por:

## Principios básicos

**Aseguran la información y los servicios** para un uso seguro de los sistemas.

Así, la organización podrá:

- Cumplir sus objetivos
- Desarrollar sus funciones
- Ejercer sus competencias

## Requisitos mínimos

Exigencias mínimas sobre la información y los servicios con el objetivo de asegurar las **5 dimensiones de seguridad:**

**D** **Disponibilidad**
Que se pueda tener acceso al servicio cuando se requiera.

**I** **Integridad**
Que la información sea la que debe ser.

**C** **Confidencialidad**
Que a la información tenga acceso quien tenga permiso.

**A** **Autenticidad**
Asegurar la fuente de la información.

**T** **Trazabilidad**
Conocer hacia dónde va la información, quien la ve o modifica, etc.

# Conceptos clave del ENS

Prevención, detección, respuesta y conservación

**La seguridad tiene como objeto** minimizar las vulnerabilidades del sistema y lograr que las amenazas no se materialicen o no afecten gravemente a la información o a los servicios.

Para ello se llevan a cabo acciones que se engloban en **cuatro aspectos fundamentales**:


**Eliminar o reducir la posibilidad** de que las amenazas lleguen a materializarse.


**Descubrir la presencia** de un ciber incidente.


**Restauración** de la información y los servicios afectados y minimización de los efectos.


**Garantizar la conservación** de los datos e información en soporte electrónico.

# Conceptos clave del ENS

Principales perfiles de usuario

Las medidas tomadas y las responsabilidades y conocimientos dependerán del perfil de los usuarios. Principalmente, se pueden distinguir **tres grandes bloques de usuarios:**

## Usuarios finales

- Realizan todo tipo de actividades en la organización.
- Pueden llegar a tratar datos personales.

## Técnicos

- Gestionan y administran los sistemas, las redes y las configuraciones.
- Aportan asistencia técnica.
- Sus responsabilidades dependerán del nivel de privilegios que posean dentro de la organización.

## Directivos y responsables

- Altos cargos del a organización.
- Son responsables de la información, los sistemas, la seguridad y otros ámbitos.
- Conforman el comité de seguridad de la información.

# Conceptos clave del ENS

Controles del ENS


**[ORG]** 4 áreas de control enfocadas a dar cobertura a aspectos de **organización de la seguridad.** — **4**

**[OP]** 7 áreas de control enfocadas a securizar aspectos del **uso de los sistemas.** — **33**

**[MP]** 8 áreas de control con medidas de **protección para los activos e infraestructura tecnológica** — **36**

# Proceso de Adecuación al ENS

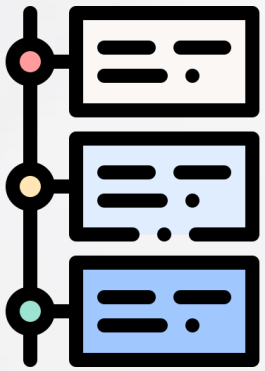
- Descripción
- Documentación necesaria
- Marco normativo
- Análisis y Gestión de Riesgos
- Plan de Tratamiento de riesgos
- Auditorías de seguridad y Certificación de Conformidad

# Proceso de Adecuación al ENS

Descripción

El proceso de adecuación de al ENS se puede dividir en las siguientes etapas:

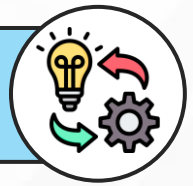
## Fases



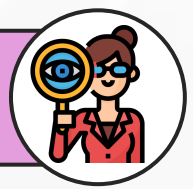
1. **Análisis de la situación actual**


2. **Definición de los niveles de seguridad**

3. **Implementación de medidas de seguridad**



4. **Evaluación y auditoría**



5. **Certificación de conformidad**

# Proceso de Adecuación al ENS

Documentación necesaria

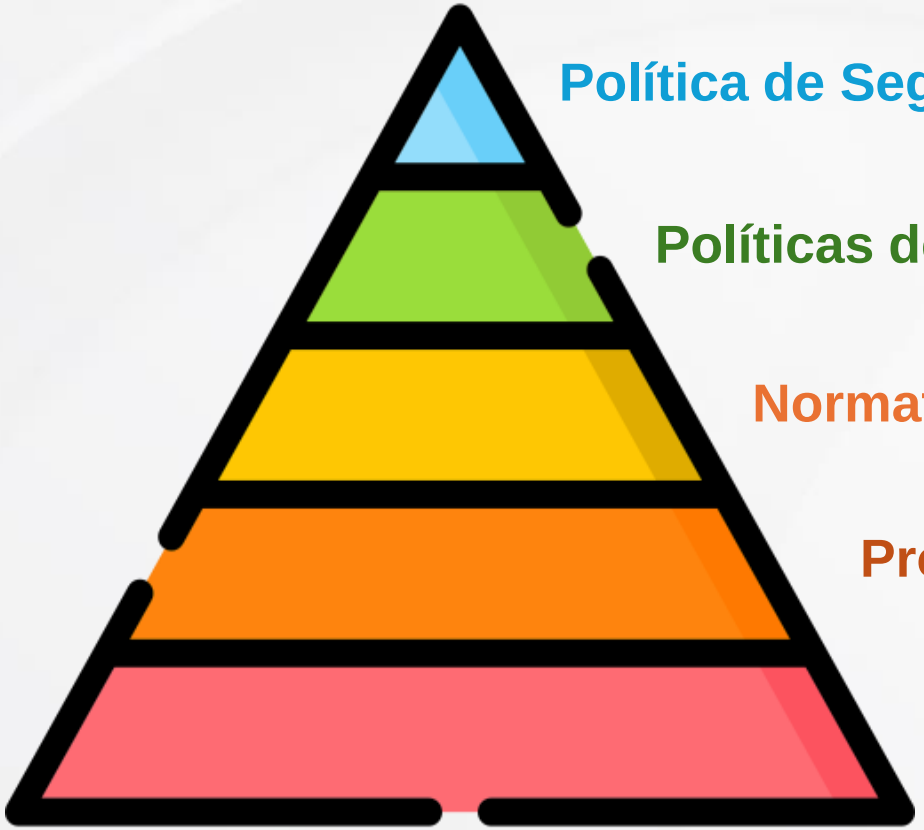
La documentación necesaria para la adecuación al ENS:

- Política de Seguridad de la Información
- Marco normativo
- Arquitectura de seguridad
- Matriz de categorización
- Declaración de aplicabilidad (SOA)
- Análisis de riesgos (AGR) + informe
- Plan de Tratamiento de riesgos
- Plan de mejora de la seguridad
- Componentes certificados
- Auditoría interna de seguridad
- Formación en materia de seguridad

# Proceso de Adecuación al ENS

Marco normativo

Para la adecuación al ENS se necesita crear y gestionar un **marco normativo** conformado por:



**Política de Seguridad de la Información**

**Políticas de seguridad específicas**

**Normativas de seguridad**

**Procedimientos de seguridad**

**Guías, Instrucciones técnicas, registros, etc.**

Con estos documentos se describen las pautas y pasos que se han de llevar a cabo para proteger a la información y a los activos de FGUCM.

# Proceso de Adecuación al ENS

Categorización de los Sistemas de Información

Los sistemas de información se deben clasificar en **categorías** de seguridad basadas en el nivel de impacto potencial que tendría un incidente de seguridad las cinco dimensiones.

## Matriz de categorización

La categoría obtenida en el control deberá ser igual o superior al nivel de seguridad de deseado.

**SISTEMA = SERVICIO + INFORMACIÓN**

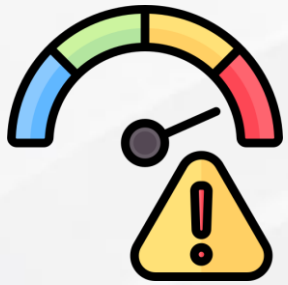
| | Niveles | | | | | |
|---|---|---|---|---|---|---|
| | **D** | **I** | **C** | **A** | **T** | **CATEGORÍA** |
| **SISTEMA 1** | Medio | Bajo | Bajo | Bajo | Bajo | MEDIA |
| **SISTEMA 2** | Alto | Alto | Alto | Alto | Alto | ALTA |
| **SISTEMA 3** | Medio | Alto | Alto | Medio | Medio | ALTA |
| **SISTEMA 4** | Bajo | Bajo | Bajo | N/A | Bajo | BÁSICA |

- **D** Disponibilidad
- **I** Integridad
- **C** Confidencialidad
- **A** Autenticidad
- **T** Trazabilidad

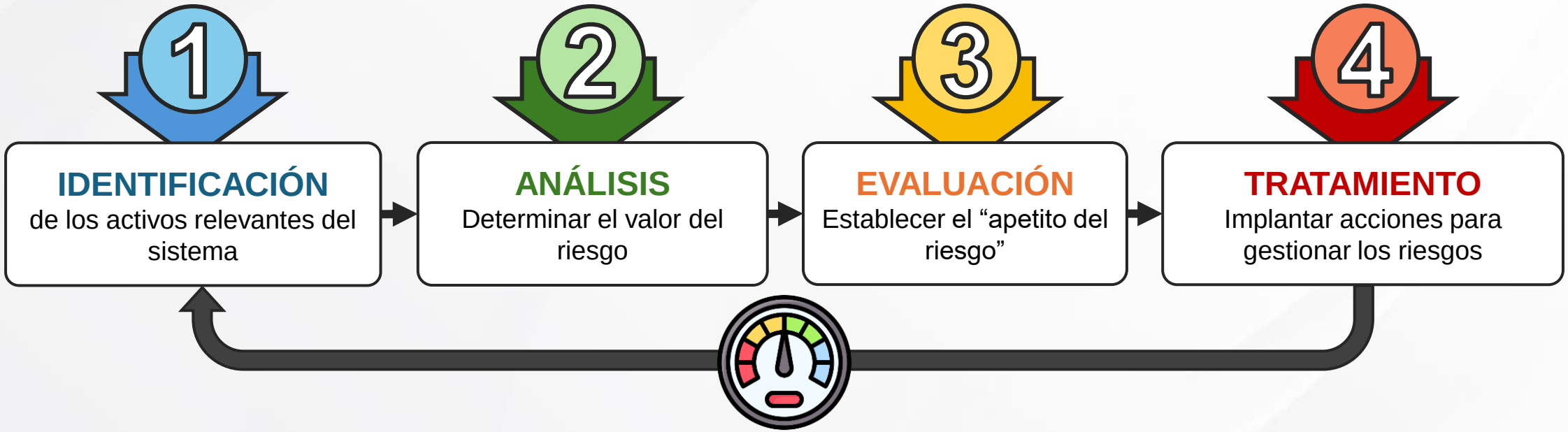
Al categorizar los sistemas, se obtiene el nivel mínimo de seguridad que debemos alcanzar para cada sistema.

# Proceso de Adecuación al ENS

Análisis y Gestión de Riesgos



La **gestión de riesgos** consiste en un proceso en cuatro etapas. Permite el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables.




El proceso de gestión de los riesgos debe ser una actividad **continua** y permanentemente actualizada.

# Proceso de Adecuación al ENS

Análisis y Gestión de Riesgos - Informe


El informe de **Análisis y Gestión de Riesgos (AGR)** recopila los resultados del de análisis de riesgos, proporcionando una base para la toma de decisiones de seguridad.

Con este documento, la alta dirección y a los responsables de seguridad tendrá acceso a un resumen detallado de los riesgos identificados y su evaluación.

Para el análisis de riesgos se pueden utilizar varias metodologías.
La más conocida es **Magerit**.

- **Impacto** que generaría el incidente
- **Probabilidad** de que ocurra el incidente

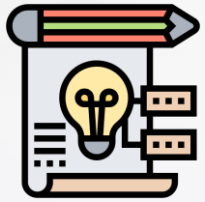
magerit
METHODOLOGY FOR INFORMATION SYSTEMS RISK ANALYSIS AND MANAGEMENT

| Impacto \ Probabilidad | MUY BAJA | BAJA | MEDIA | ALTA | MUY ALTA |
|---|---|---|---|---|---|
| MUY ALTA | MEDIO | MEDIO | ALTO | ALTO | EXTREMO |
| ALTA | MEDIO | MEDIO | ALTO | ALTO | ALTO |
| MEDIA | BAJO | MEDIO | MEDIO | ALTO | ALTO |
| BAJA | BAJO | BAJO | MEDIO | MEDIO | ALTO |
| MUY BAJA | MUY BAJO | BAJO | BAJO | MEDIO | MEDIO |

# Proceso de Adecuación al ENS

Plan de Tratamiento de riesgos

El plan de tratamiento del riesgo (PTR) contiene las medidas necesarias para tratar los riesgos identificados y evaluados durante el AGR con el objetivo de **reducir la probabilidad y el impacto de los riesgos**.



## Contenido

El plan debe **abordar todos los riesgos** identificados en el análisis de riesgos, asegurando que se tomen decisiones informadas.

## Características

1. Identificación de Riesgos
2. Medidas de Mitigación
3. Responsabilidades
4. Cronograma
5. Coste-Beneficio
6. Seguimiento y Revisión

# Proceso de Adecuación al ENS

Auditorías de seguridad y Certificación de Conformidad

Las auditorías del ENS son fundamentales para:

- **Verificar el cumplimiento** de las medidas de seguridad.
- **Identificar áreas de mejora** en los dominios de control del ENS.

**La certificación de ENS se renueva cada 2 años,**
pero se deben realizar auditorías frecuentemente.

**El proceso de adecuación es cíclico**
Hay que volver a empezar para asegurar la seguridad.


En una auditoría de una universidad, podría descubrirse que los servidores que almacenan calificaciones no tienen las medidas de seguridad adecuadas, lo que podría exponer los datos de los estudiantes a ataques externos. La auditoría recomendaría la implementación de controles de acceso más estrictos y cifrado de datos.

# Glosario, fuentes y referencias

# Glosario, fuentes y referencias web

Fuentes principales

## ¿QUÉ SON LAS GUÍAS DE SEGURIDAD?

Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el **Centro Criptológico Nacional** (CCN), en el ejercicio de sus competencias, elabora y difunde guías de seguridad de las tecnologías de la información y las comunicaciones.

Con esta finalidad, las series de **documentos CCN-STIC,** elaborados por el CCN ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el ENS.


## ¿CUÁLES SON LOS OBJETIVOS DE LAS GUÍAS DE SEGURIDAD?

- **Establecer pautas de carácter general**, que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares.
- **Particularización por cada organización**, a su entorno singular en función de lo que se tenga ya hecho, de los recursos disponibles, del tipo de organización, de la idiosincrasia de los responsables

# Glosario, fuentes y referencias web

Fuentes principales

Las fuentes y referencias web utilizadas para elaborar esta sesión formativa son:


## Legislación

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.


## Guías de seguridad

- CCN-STIC 800 - Glosario de términos y abreviaturas del ENS
- CCN-STIC 801 - Esquema Nacional de Seguridad responsabilidades y funciones
- CCN-STIC 804 - ENS. Guía de implantación
- CCN-STIC 805 - Política de Seguridad de la Información
- CCN-STIC 105 - Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación


## Referencias webs

- https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html
- https://www.boe.es/eli/es/res/2016/10/13/(4)/dof/spa/pdf

# Situación Actual de FGUCM

- Organigrama y roles
- Marco normativo
- Auditoría y certificación

# Organigrama de la FGUCM en materia de ENS

FUNDACIÓN COMPLUTENSE

## ROLES

**REPRESENTANTE DE LA FGUCM**
Dª María Paz García Vera

**DELEGADA DE PROTECCIÓN DE DATOS**
Dª Loyola Martín Fraiz

**SEGURIDAD DE LA INFORMACIÓN**
Dª Irene García González-posada

**SISTEMA DE LA INFORMACIÓN**
Dª Ana María Sanz Fernández

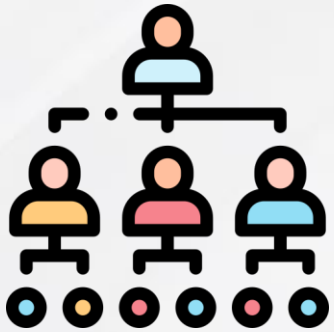
**COMITÉ DE SEGURIDAD DE LA INFORMACIÓN**

**RESPONSABLES DE SERVICIO/INFORMACIÓN**

| Dª. Sonia Olmeda García | D. Ignacio Fernández Arias | D. Luis Zuloaga Uría | Dª. Ángeles Andrés Gómez | D. Javier Tejedor Bordegaray | D. Alejandro Cabero Alonso | Dª. Patricia Lanzaco Corbalán | Dª. Isabel Torres Gallego | Dª. Concepción Aragoneses Arranz | Dª. Almudena Pedrazuela Yuste | Dª. Myriam Crespo Garrido |
|---|---|---|---|---|---|---|---|---|---|---|
| GESTIÓN DE LA INVESTIGACIÓN | GESTIÓN DE ACTIVIDADES CULTURALES | PORTAL INSTITUCIONAL | ACTIVIDADES QUE CONTRIBUYAN A LA MEJOR ATENCIÓN A LA COMUNIDAD UNIVERSITARIA | ECONÓMICO FINANCIERO | GESTIÓN DE CONGRESOS | RELACIONES INSTITUCIONALES Y MECENAZGO | JURÍDICO | EMPLEO Y FORMACIÓN BONIFICADA | RECURSOS HUMANOS | COMUNICACIÓN |
| PULSA | GESTIÓN DE BECAS Y AYUDAS | PORTAL DE TRANSPARENCIA | | | | | PERFIL DEL CONTRATANTE | | | |
| | GESTIÓN DE ACTIVIDADES FORMATIVAS Y EVENTOS | | | | | | | | | |

# Situación Actual de FGUCM

Organigrama y roles



## Representante de FGUCM

Representa a toda la organización.

## Delegada de Protección de Datos (DPD)

Responsable de garantizar el cumplimiento sobre protección de datos personales.

## Responsable de Seguridad

Implementa, gestiona y mantiene las medidas de seguridad necesarias.

## Responsable del Sistema de Información

Administra toda la infraestructura TI.

## Responsables del Servicio

Gestionan la prestación de servicios, verificando que cumplan los requisitos de seguridad.

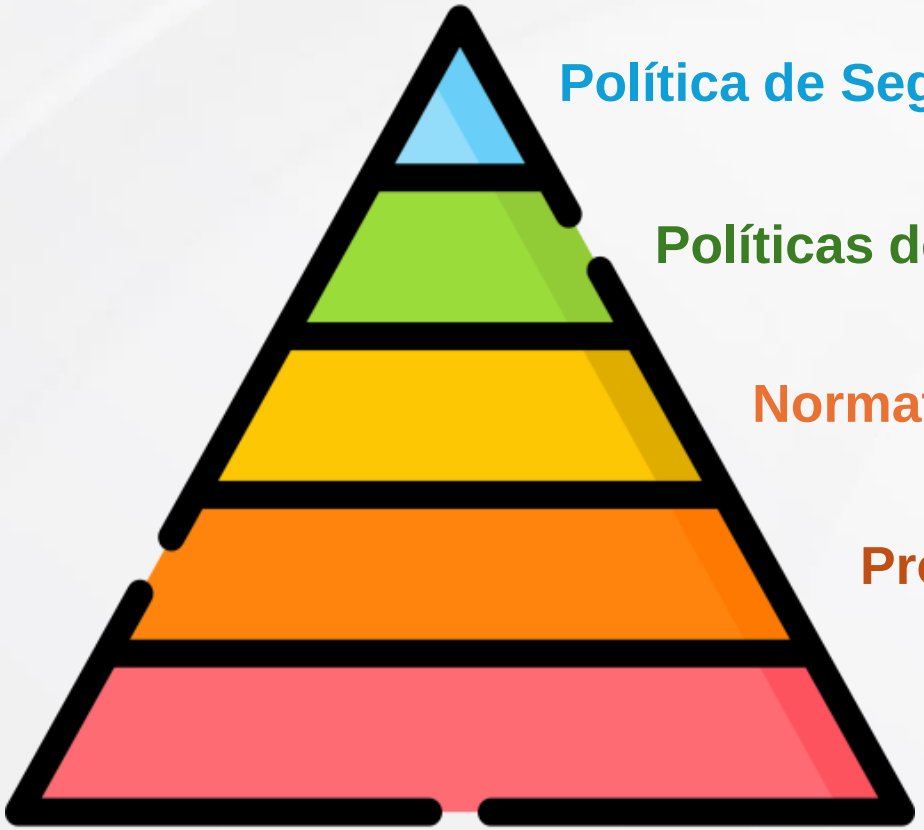
## Responsables de la Información

Controlan los datos y otros activos que se manejan, garantizando su protección y accesibilidad.

# Situación Actual de FGUCM

Marco normativo

FGUCM posee un marco normativo adecuado a las exigencias del ENS.



**Política de Seguridad de la Información**

**Políticas de seguridad específicas**

**Normativas de seguridad**

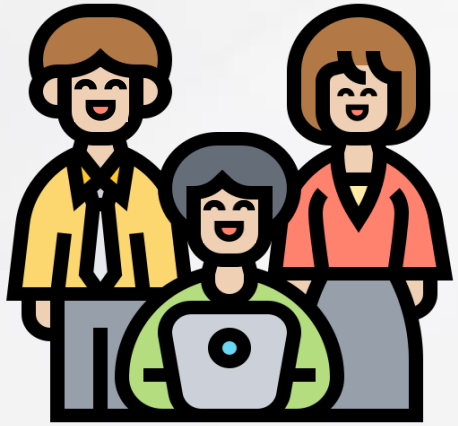
**Procedimientos de seguridad**

**Guías e Instrucciones técnicas**

# Directrices Principales del ENS en FGUCM

Marco normativo

Todos los usuarios de FGUCM deben:



- **Leer**
- **Comprender**
- **Aceptar**
- **Aplicar**

Política de Seguridad de la Información (PSI).

Políticas específicas, normativas y procedimientos que apliquen a su actividad diaria en FGUCM.

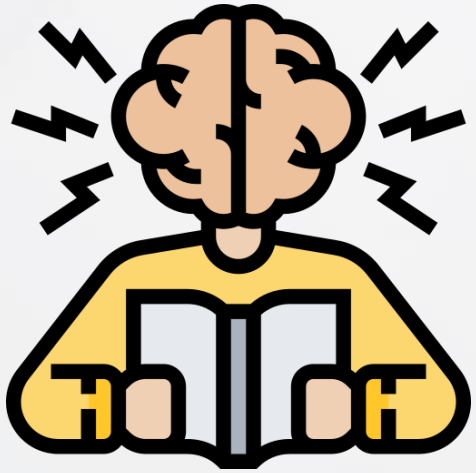
Cláusulas de seguridad de la información.

# Directrices Principales del ENS en FGUCM

Marco normativo

**FGUCM está aplicando medidas** para la mejora de la seguridad y sus usuarios, realizando actividades como:

- Formaciones.
- Gestión documental.
- Establecimiento de pautas de buen uso de recursos.
- Etc.

## ¡Recordad!

La seguridad de FGUCM es la seguridad de todos sus usuarios.

# Directrices Principales del ENS en FGUCM

Auditoría y certificación

FGUCM realizó una **auditoría interna** en 2024 para evaluar el estado actual de seguridad.
Las no conformidades encontradas se subsanarán a lo largo de este año y del que viene, ya que la **auditoría externa** para la certificación ENS se realizará en 2025.


**sept 2024** → **Subsanación de no conformidades** → **2025**

# Buenas Prácticas propias de la FGUCM

- Normativa de Gestión de la clasificación y tratamiento de la Información
- Normativa de Gestión de Soportes
- Normativa de uso aceptable de activos
- Protección frente ataques
- Otros ataques
- Normativa de puesto de trabajo y escritorios despejados
- Contraseñas Robustas
- Normativa de bloqueo del puesto de trabajo
- Gestión de incidentes

# Normativa de Gestión de la clasificación y tratamiento de la Información

Clasificación de la información


El sistema de **clasificación** de datos de la FGUCM utiliza el principio de “Necesita conocer”. La información no se divulgará a nadie que no tenga la necesidad legítima y demostrable de recibir la información.

Criterios para clasificar la información de FGUCM

| | |
|---|---|
| **Confidencial** | Información, sensible o muy sensible, cuyo tratamiento por personal no autorizado puede causar un daño grave o irreparable, a FGUCM o a terceros, o puede causar pérdidas económicas significativas. |
| **Uso interno** | Información cuyo acceso, revelación o modificación por parte de personal no autorizado puede causar un daño leve a la FGUCM o terceros. |
| **Pública** | Toda información que no encaja en ninguna de las clasificaciones anteriores y cuya divulgación no supone un peligro. |

Se tiene previsto el cambio de clasificación de:

- **Confidencial** → USO OFICIAL - Acceso restringido
- **Uso interno** → USO OFICIAL

Para más información, leer la Normativa de Gestión de la clasificación y Tratamiento de la Información.

# Normativa de Gestión de la clasificación y tratamiento de la Información

Etiquetado de la información y los soportes

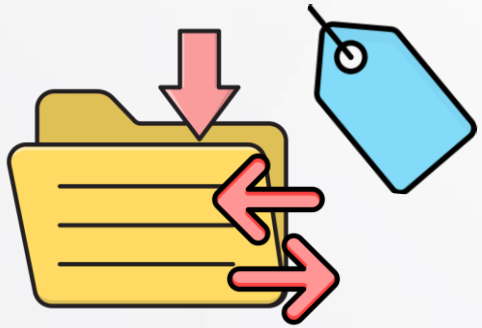
Se **etiquetarán** los documentos electrónicos, en papel y cualquier otro soporte.

- La etiqueta deberá describir un código que permita al usuario identificar dicha información sin que se pueda deducir a simple vista por un tercero.
- La etiqueta deberá permanecer durante todo el ciclo de vida de la información.

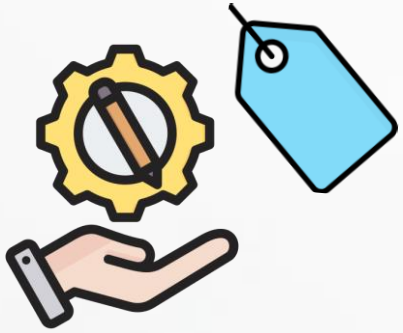
**Ciclo de vida de la Información**

**Creación**

**Almacenamiento y traslado**



**Modificación**



**Eliminación o borrado seguro**

Para más información, leer la Normativa de Gestión de la clasificación y Tratamiento de la Información y la Normativa de Gestión de Soportes.

# Normativa de Gestión de la clasificación y tratamiento de la Información

Intercambio de Información

La información **circulará** dependiendo de su clasificación.

- Red interna de FGUCM.
- Red pública (internet).
- Soportes sólidos (fotocopias, memorias y discos duros externos, etc.).

| | |
|---|---|
| **Uso oficial**<br>**Uso restringido** | Puede circular por la organización personal autorizado si se hace de manera segura. Se incluyen datos personales. Para envíos por fax, concertar un momento exacto con el receptor. |
| **Uso oficial** | Puede circular libremente dentro de FGUCM. Su circulación fuera de la organización será solo por y para personal autorizado. |
| **Pública** | Puede circular libremente dentro y fuera de FGUCM |

## Con respecto a terceros…

- Podrán tratar información (o los soportes que la contenga) Pública y de Uso interno (*autorizados*).
- Solo podrán tratar información confidencial si se firma el **acuerdo de confidencialidad.**

Para más información, leer la Normativa de Gestión de la clasificación y Tratamiento de la Información, la Normativa de contratación y relaciones con terceros y la normativa de Gestión de Soportes.

# Normativa de Gestión de la clasificación y tratamiento de la Información

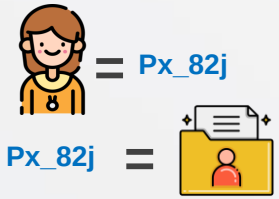
Datos Personales

| | |
|---|---|
| **Datos personales** | "Toda información sobre una persona física **identificada o identificable**". |

| | |
|---|---|
| **Persona física**<br>**identificada o identificable** | Toda persona cuya **identidad pueda determinarse** mediante un identificador, como un nombre, datos de localización, imagen, voz, etc. |

| | | |
|---|---|---|
| **Tratamiento** | **Operaciones** realizadas sobre datos personales. | **Ejemplos de tratamiento:**<br>• Elaboración de expedientes.<br>• Destrucción de documentación.<br>• Mantenimiento de los equipos. |

| | |
|---|---|
| **Limitación**<br>**del tratamiento** | **Restricción** el uso de los datos para ciertos fines. |




| | |
|---|---|
| **Seudonimización** | Los datos se almacenan **sin estar directamente asociados** al interesado, pero pueden ser reidentificables. |

Para más información, leer la Normativa de Gestión de la clasificación y Tratamiento de la Información y Normativa de contratación y relaciones con terceros

# Normativa de Gestión de la clasificación y tratamiento de la Información

Datos Personales

## Categorías especiales de datos

Datos cuyo tratamiento podría entrañar importantes **riesgos** para los derechos y las libertades fundamentales.

En Europa se definen hasta 51 datos sensibles.

En el artículo 9 del RGPD se definen las **“Categorías especiales de datos”.**


Para más información, leer la Normativa de Gestión de la clasificación y Tratamiento de la Información y Normativa de contratación y relaciones con terceros

# Normativa de Gestión de la clasificación y tratamiento de la Información

Almacenamiento

Los soportes de información deberán ser **custodiados** según su nivel de calificación, garantizando:

- Su disponibilidad y control de quien accede.
- Respeto a las exigencias de mantenimiento del fabricante: temperatura, humedad...
- Para los soportes almacenados por largos periodos de tiempo, comprobar su tiempo medio de vida.

Durante su almacenamiento, se deberá registrar el historial de uso de cada soporte.

En caso de que proveedores necesiten tener acceso recurrente a información de uso oficial se recomienda establecer un repositorio seguro (Teams, Google Drive) al que accedan los proveedores vía doble factor, conectándose a la red interna de FGUCM.

INCIBE recomienda algunas herramientas de cifrado:
https://www.incibe.es/ciudadania/filtro/herramientas?tid=303602&tid_1=All&tid_2=All&tid_3=All

Para más información, leer la Normativa de Gestión de la clasificación y Tratamiento de la Información y la Normativa de Gestión de Soportes.

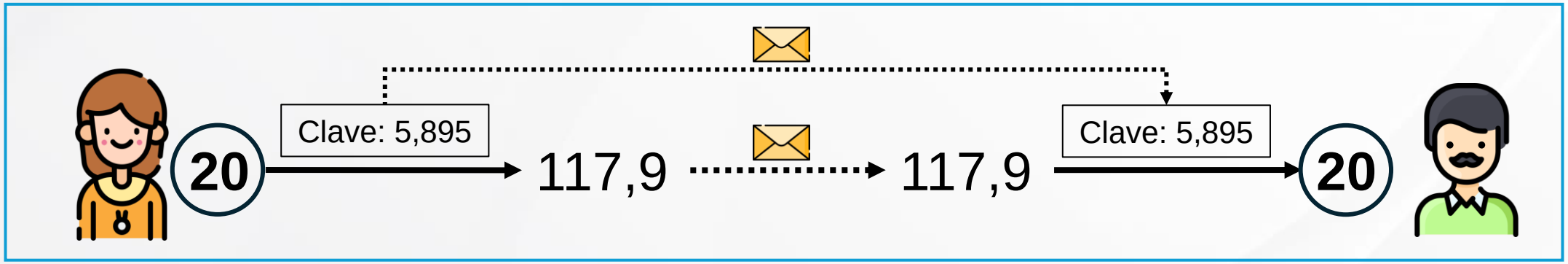
# Normativa de Gestión de la clasificación y tratamiento de la Información

Cifrado

Los soportes podrán trasladarse fuera de FGUCM cuando estén **cifrados**. Dentro serán cifrados cuando la información del soporte sea de extrema criticidad.

Se utilizarán los medios de protección criptográfica dependiendo del nivel de calificación de la información.

Cifrando un documento **cambiamos su código para que sea ilegible**, a no ser que se decodifique con el mismo código.




INCIBE recomienda algunas herramientas de cifrado:
https://www.incibe.es/ciudadania/filtro/herramientas?tid=303602&tid_1=All&tid_2=All&tid_3=All

Para más información, leer la Normativa de Gestión de la clasificación y Tratamiento de la Información y la Normativa de Gestión de Soportes.

# Normativa de Gestión de la clasificación y tratamiento de la Información

Limpieza de documentos

Antes de compartir un documento (pdf, texto, hoja de cálculo, imagen, audio, etc.) de la FGUCM, es obligatorio **retirar toda información adicional** contenida en él.

- Campos ocultos.
- Metadatos.
- Comentarios.
- Versiones anteriores.

El **incumplimiento** puede perjudicar:

- La confidencialidad de la información y sus fuentes.
- La buena imagen de la FGUCM.

Para más información sobre como eliminar metadatos, visitar:
https://www.incibe.es/empresas/blog/son-los-metadatos-y-eliminarlos

Para más información, leer la Normativa de Gestión de la clasificación y Tratamiento de la Información y el Procedimiento de limpieza de documentos

# Normativa de Gestión de Soportes

Borrado y destrucción

El último momento del ciclo de vida de la Información es su **borrado o destrucción.**

Si se va a reutilizar un soporte, se debe aplicar un mecanismo de borrado seguro (permanente e irrecuperable).

El mecanismo de borrado dependerá de la clasificación de la información.

**Uso oficial**
**Uso restringido**

**Uso oficial**

**Pública**

## Borrado

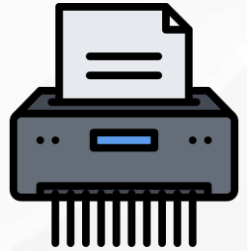
Cuando se desee (y se pueda) reutilizar el soporte.

- Sobreescritura
- Desmagnetización, etc.


## Destrucción

Cuando no se quiere (o no se puede) reutilizar el soporte.

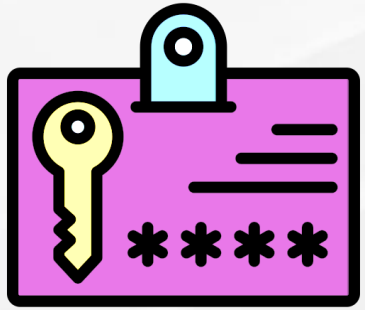
- Desintegración
- Incineración
- Trituración, etc.



Para más información, leer la Normativa de Gestión de soportes

# Normativa de uso aceptable de activos

Uso general de los medios tecnológicos




**Acceso restringido por privilegios**. Los usuarios tienen autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones

Se **prohíbe** el uso de los medios tecnológicos cuando:

- Se viole la legislación vigente (protección de datos, licencias de programas, derechos de autor, etc.).
- Se realice con fines privados con ánimo de lucro.
- Pueda dañar la reputación y buen nombre de la FGUCM.
- Se atente contra la seguridad o eficiencia de la FGUCM.

Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Normativa de uso aceptable de activos

Ordenadores de puesto de trabajo y periféricos

**Los usuarios de los equipos, físicos y portátiles, se responsabilizarán de:**

- La protección frente a uso indebido por terceros
- No realizar modificaciones a nivel de administrador sin tener privilegios para ello.
- Devolver los equipos cuando FGUCM obligue a ello (ej. finalización contrato).

## Uso aceptable

Utilizar los equipos para tareas relacionadas con FGUCM.

Bloquear el PC cuando no se esté utilizando y apagar al terminar la jornada.

Notificar, sin demora, cualquier incidente.

## Uso NO aceptable

Modificación de la configuración sin autorización.


Instalar software no autorizado.

Uso abusivo del teléfono para llamadas particulares.

Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información y la Normativa de Uso y Protección de Portátiles

# Normativa de uso aceptable de activos

Repositorios de información / Carpetas de red

**Los usuarios tienen acceso a:**

- Repositorio general de la FGUCM
- Repositorio personal (si procede), del cual son responsables

## Uso aceptable

Almacenar la información de la FGUCM.
Debe cumplir con las directrices dispuestas en la Normativa de clasificación y tratamiento de la información

Uso responsable de los recursos compartidos.

## Uso NO aceptable

Almacenar información sin clasificar que contenga datos personales.

Almacenar información de uso personal.

Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Normativa de uso aceptable de activos

Memorias extraíbles / Discos duros

En función de las necesidades, es posible que desde la FGUCM se facilite un **dispositivo extraíble** con capacidad de almacenamiento

## Uso aceptable

Almacenar la información no clasificada.

Cuando un dispositivo cumpla su función se entregará al responsable oportuno para su borrado seguro y reordenación.

## Uso NO aceptable

Almacenar información clasificada sin supervisión ni autorización.

Almacenar información de uso personal.

Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Normativa de uso aceptable de activos

Impresoras

Deberán utilizarse las **impresoras** de red y las fotocopiadoras corporativas, a no ser que exista autorización para la instalación y uso de impresoras locales.

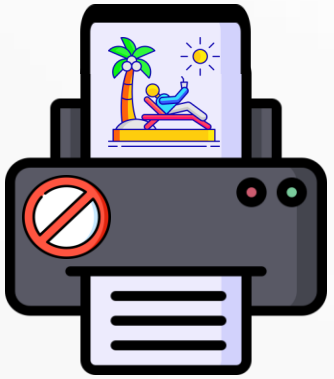
## Uso aceptable

Recoger la información impresa lo antes posible.

En caso de encontrar documentación en la impresora, avisar al propietario.

Los documentos clasificados que se envíen por fax deberán eliminarse del equipo.

## Uso NO aceptable



Imprimir documentos personales.

Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Normativa de uso aceptable de activos

Correo electrónico

Los usuarios de FGUCM tienen, al menos, una cuenta de **correo electrónico**. Los usuarios deberán hacerse responsable del buen uso de su correo y sus cuentas.

## Información relevante

El correo podrá ser **monitorizado o inspeccionado** cuando así lo requiera una acción judicial o las herramientas de seguridad.

Se realizarán **copias de seguridad** de los buzones con el fin de garantizar su **disponibilidad** en caso de incidentes.

Se **filtrarán, detendrán y estudiarán** automáticamente **correos entrantes o salientes** que puedan representar algún **peligro**.

- Por su contenido.
- Por procedencia o destino considerado peligroso.

Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Normativa de uso aceptable de activos

Correo electrónico

## Uso aceptable

Considerar la clasificación de la información antes de enviarla.

- Información Pública
- Información de Uso Interno
- Información Confidencial
- Información Extremadamente Confidencial

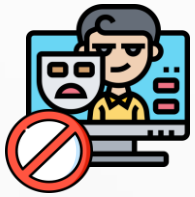
Comunicar y eliminar cualquier correo sospechoso.

Pasar el antivirus antes de abrir cualquier archivo recibido por correo.

Ocultar la dirección de correo de los destinatarios (Copia oculta - CCO).

## Uso NO aceptable

Facilitar el acceso a la cuenta de usuario a otras personas.



Suplantar la identidad de otro usuario.

Con fines personales que interfieran con el rendimiento del servicio, las labores del trabajador, o suponga un alto coste para la FGUCM.

Difundir contenido inadecuado o ilegal.

Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Normativa de uso aceptable de activos

Uso de la red, internet y de la navegación


Los usuarios son los únicos responsables del uso que le dan a **Internet**.

- La navegación es monitorizada, quedando registrados los sitios concretos a los que se accede.
- Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por la FGUCM.

## Uso aceptable

Acceder a información relacionada con el desempeño de las funciones del empleado.

Acceder a información con fines particulares solamente de forma puntual y no abusiva.

## Uso NO aceptable

Alterar la configuración del navegador o utilizar uno distinto sin autorización.


Escuchas del tráfico de red.

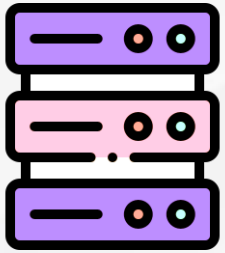
Descarga de contenido ilegal y de ocio.

Uso de programas “peer-to-peer” para compartir archivos (Torrent).

Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Normativa de uso aceptable de activos

Uso de servidores



Los **servidores** de la FGUCM no tendrán permitida la conexión a Internet, salvo que sea estrictamente necesario para el funcionamiento del servicio ofrecido.

Tampoco se podrán utilizar para actividades típicas de usuarios finales.

## Uso aceptable

Generación e intercambio de información relacionada con funciones de:

- Administración
- Operaciones
- Desarrollo
- Servicios y actividades de la FGUCM

## Uso NO aceptable

Uso de herramientas ofimáticas.

Almacenamiento de archivos no relacionados con los servicios prestados.

Uso de Internet: páginas Web, Chat, descarga, etc.

Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Protección frente ataques

Los (ciber) delincuentes llevan a cabo sus ataques a través de todo tipo de medios. Muchos de estos ataques van dirigidos a todo **tipo de ususarios**, por lo que necesitamos conocer cómo se realizan estos ataques para poder defendernos.

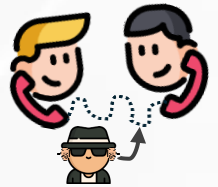
Algunos de los **ataques a través de la red** más comunes son:

**Phising**

**Suplantación de identidad**

**Ransomware**

**Malware**



**Man in the middle**

# Protección frente ataques

Phising

El **phising** es un ataque muy común que busca hacernos clicar en algún enlace o descargar algún archivo para:

- Robar dinero
- Robar credenciales
- Obtener información
- Infectar tu equipo, etc.

El phising puede ser **genérico** (campaña) o **dirigido**, suplantando la identidad de una persona u organización para engañarnos.

## ¡Recuerda!

- **Sospecha**
- **Pregunta**
- **Nunca pinches enlaces**
- **Nunca descargues contenido desconocido**
- **Comunica**

Se puede lanzar a través de **distintos medios:**

**Whatsapp**


**SMS**

**Email**


**Publicidad**

# Protección frente ataques

Suplantación de identidad

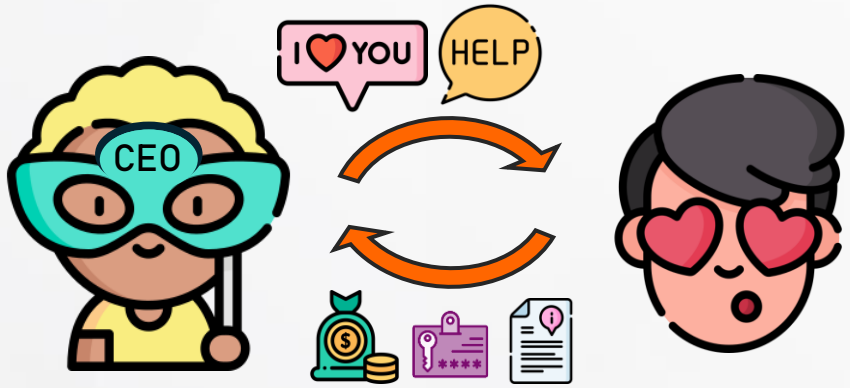
La **suplantación de identidad** es una forma de ciberataque en el que los estafadores se hacen pasar por otras personas para engañarnos y manipularlos para pedir:

- Dinero
- Privilegios de acceso
- Información, etc.

## ¡Recuerda!

- **Sospecha**
- **Pregunta**
- **Nunca pinches enlaces**
- **Nunca descargues contenido desconocido**
- **Comunica**

Un ataque muy típico es el denominado **Fraude del CEO**, por el cual se hacen pasar por altos cargos de la organización para pedir lo que desean.



# Protección frente ataques

Malware

**Software malicioso** diseñado para dañar o acceder sin autorización a sistemas.

Incluye virus, troyanos, ransomware, spyware, etc.

## ¡Recuerda!

- **Sospecha**
- **Pregunta**
- **Nunca pinches enlaces**
- **Nunca descargues contenido desconocido**
- **Comunica**

El malware puede **afectar** de distintas maneras:

**Robo, modificación o borrado** de información

**Bloqueo o destrucción** de equipos y aplicaciones

**Encriptado** de información

**Desplazarse** para infectar otros equipos

**Modificar la configuración** de seguridad

**Seguimiento** de la actividad de los usuarios, etc.

# Protección frente ataques

Ransomware

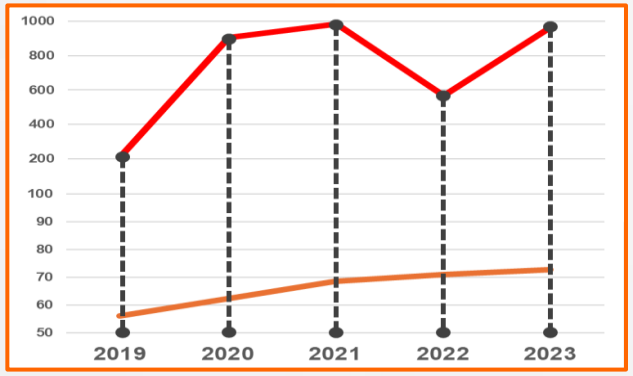
El **ransomware** es un ataque en el que "**secuestran**" nuestra información (mediante cifrado) o paralizan nuestros servicios, para después pedir un rescate.

El secuestro se realiza a partir de un malware que infecta los equipos.

Este tipo de ataques son un "**negocio redondo**" ya que, aunque paguemos el rescate (lo cual **nunca** es aconsejable), seguirán amenazándonos.

## ¡Recuerda!

- **Sospecha**
- **Pregunta**
- **Nunca pinches enlaces**
- **Nunca descargues contenido desconocido**
- **Comunica**




**Leyenda:**

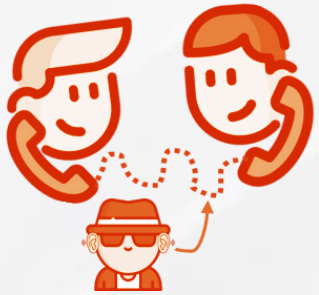
Volumen estimado (mill. €) en daños y perjuicios por ransomware. Casi 1000 millones en 2023.

Porcentaje de organizaciones afectadas, directa o indirectamente. 72% en 2023.

Datos obtenidos de statista y chainalysis:
https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/
https://www.chainalysis.com/blog/ransomware-2024/

# Protección frente ataques

Man in the middle



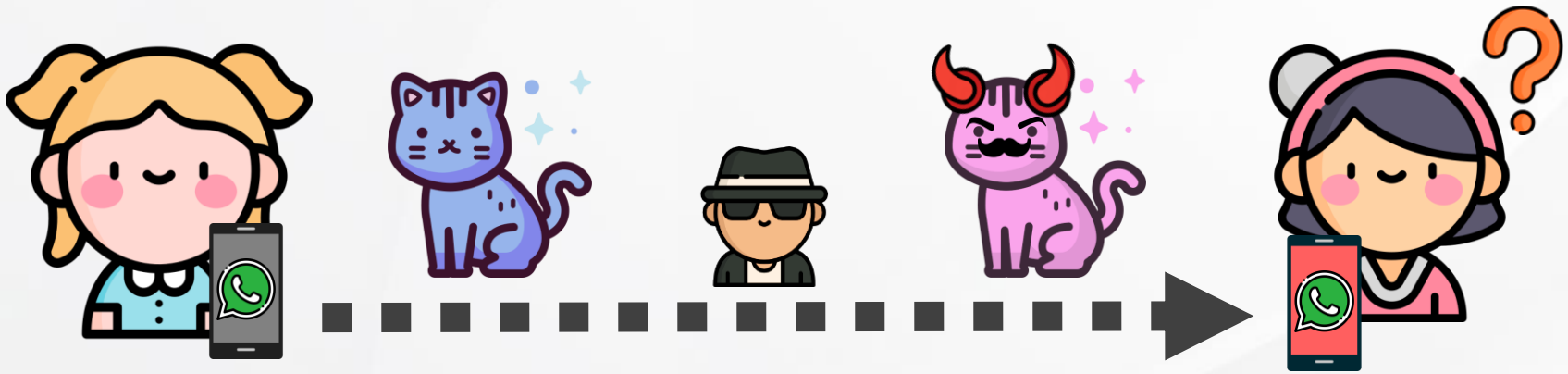
En el ataque **“Man in the Middle”,** el atacante intercepta y/o altera las comunicaciones entre dos partes sin que estas lo sepan.

Las comunicaciones se pueden dar por distintas vías:

- Telefónica
- SMS
- Correo electrónico
- WhatsApp, etc.

## ¡Recuerda!

- **Sospecha**
- **Pregunta**
- **Nunca pinches enlaces**
- **Nunca descargues contenido desconocido**
- **Comunica**



# Otros ataques

Hay otros ataques que pueden afectar a FGUCM cuyo **vector de entrada no son sus usuarios**, sino que se realizan sobre los servidores, las aplicaciones, la página web, etc.


## Ataque de Denegación de Servicio (DoS) y DDoS

Sobrecarga de un servidor con tráfico excesivo para dejarlo inaccesible.

## Ataques de fuerza bruta

Intentan adivinar contraseñas probando una gran cantidad de combinaciones.

## Exploits Zero-Day

Atacan vulnerabilidades desconocidas en software que no tienen parches de seguridad.


## Cross-Site Scripting (XSS)

Inyección de scripts maliciosos en sitios web que permiten robar cookies, sesiones y datos sensibles.

# Normativa de puesto de trabajo y escritorios despejados

**No todos los ataques se realizan a través de la red**, muchos son físicos.

Mantener las mesas de trabajo ordenadas y libres de documentos sensibles ayuda a proteger datos confidenciales de accesos no autorizados y minimiza el riesgo de fuga de información.

## Protección de información

Los equipos y la información sensible o crítica se guardarán bajo llave, evitando la fuga de datos.


## Contraseñas protegidas

Nunca dejar al alcance de terceros credenciales de acceso.

## Protección física de los equipos

Tener los puestos de trabajo despejados ayuda a mantener la integridad física de los equipos de trabajo, evitando ser golpeados, mojados, etc.

Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Normativa de puesto de trabajo y escritorios despejados

Respetar la normativa evita:


**Accesos no autorizados.**
A información o aplicaciones de FGUCM.

**Robo de Identidad.**
Pueden utilizar nuestras credenciales para hacerse pasar por nosotros.

**Daño a la reputación.**
Por la pérdida de información o incapacidad temporal de la actividad.

**Sanciones legales.**
Por falta de medidas de protección.

Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Normativa de bloqueo del puesto de trabajo

El equipo de usuario es el activo más valioso de los usuarios de FGUCM. Es necesario para trabajar y autenticarnos, por lo que es importante protegerlo.

**Abandonar el puesto de trabajo con el equipo desbloqueado puede tener graves consecuencias.**

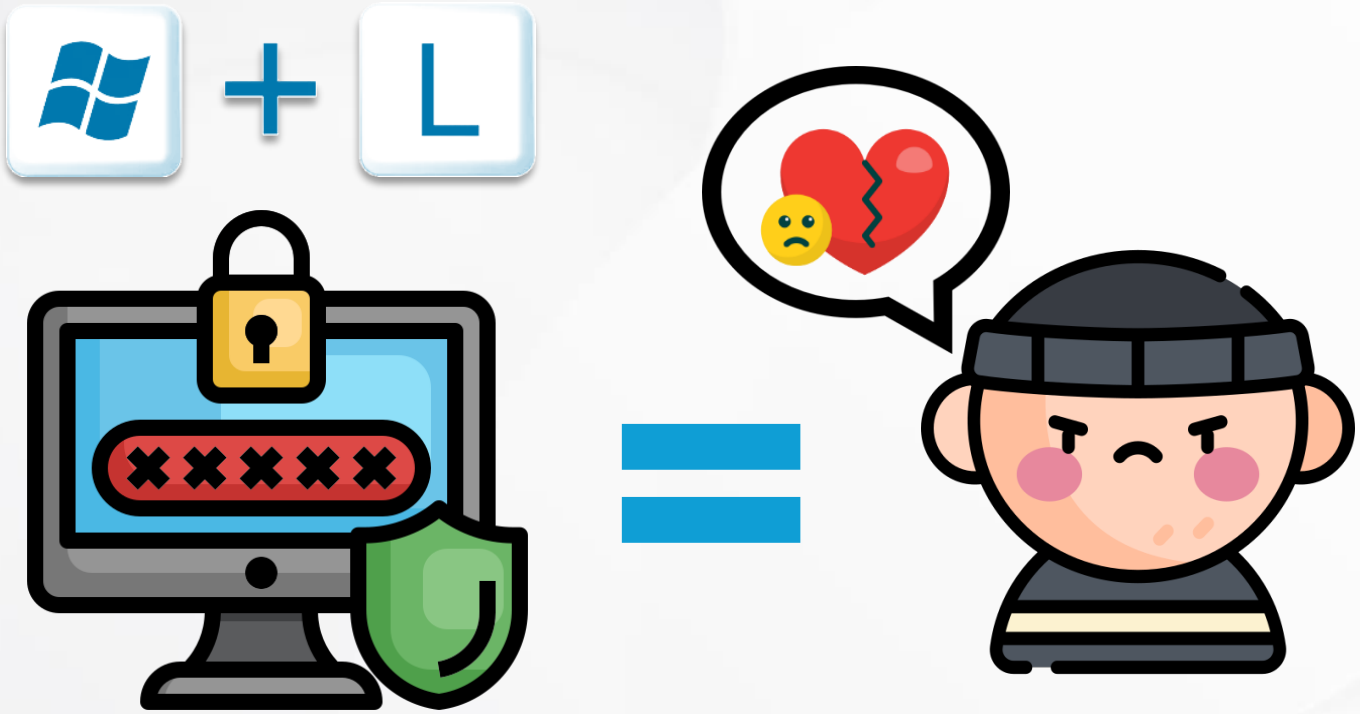
Cualquier otro usuario podría hacer un mal uso con nuestro equipo:

- Robar, borrar y modificar información.
- Utilizar nuestra cuenta de correo corporativo para hacerse pasar por nosotros.
- Robar credenciales.
- Pinchar una memoria USB y ejecutar un programa malicioso.
- Etc.


Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Normativa de bloqueo del puesto de trabajo

Recuerda **bloquear** siempre el equipo **cuando abandones** tu puesto de trabajo.




Para más información, leer la Normativa de Uso de Recursos y Accesos a Sistemas de Información

# Contraseñas Robustas

Las **contraseñas** son la primera línea de defensa contra accesos no autorizados.
Su complejidad determina cuánto tiempo y esfuerzo le llevará al atacante descifrarla.

## Contraseña insegura.

Simples, de poca longitud y solo un tipo de carácter.
Tiempo estimado de descifrado: segundos.

*123456*

## Contraseña moderada.

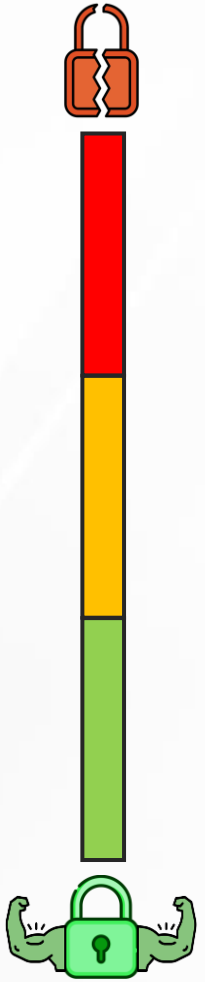
Dos caracteres diferentes.
Tiempo estimado de descifrado: min./horas.

*himan1990*

## Complejas.

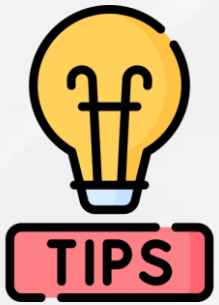
Mayor longitud. Mezclan mayúsculas, minúsculas, números y caracteres especiales.
Tiempo estimado de descifrado: años.

*K8_y0lMund!67*



# Contraseñas Robustas

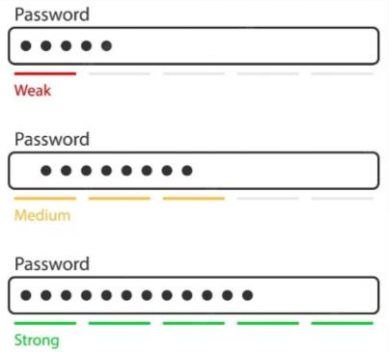
Buenas prácticas




## Utilizar siempre contraseñas complejas.

12 caracteres y mezclar los 4 tipos.
Una manera fácil de recordarla es inventar una frase y construirla a partir de ahí.
Por ejemplo:

*En 2005 fui a Paris y me comí 5 crepes.*
*En05_faP&mc_5C!*




## Nunca utilizar nombres o fechas

que sean fáciles de obtener por internet: nuestro nombre, el de un hijo, mascota, etc.

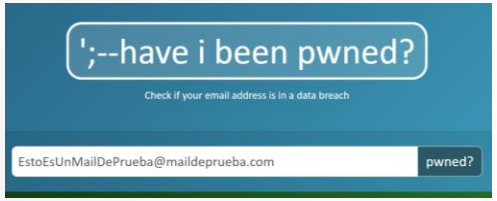

## Nunca reutilizar la misma contraseña en otras cuentas.

Si nos roban una nos las roban todas.

## Cambiar la contraseña regularmente.

## Comprobar regularmente si nuestras han sido comprometidas

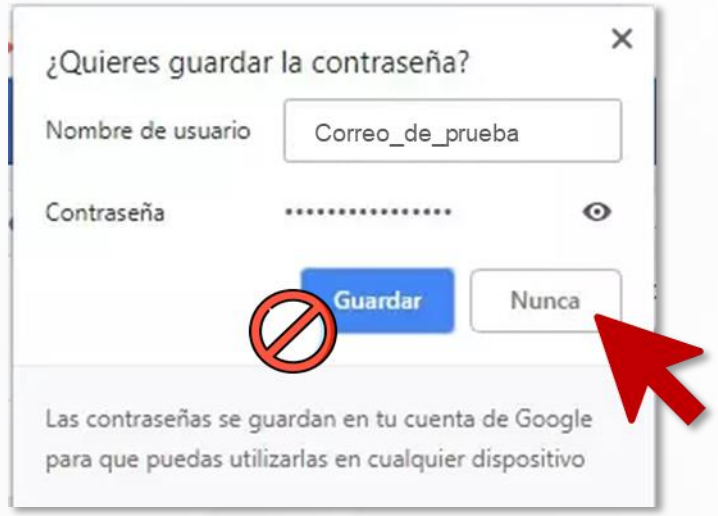
para cambiar la contraseña urgentemente en caso de que lo hayan sido (https://haveibeenpwned.com/).



# Contraseñas Robustas

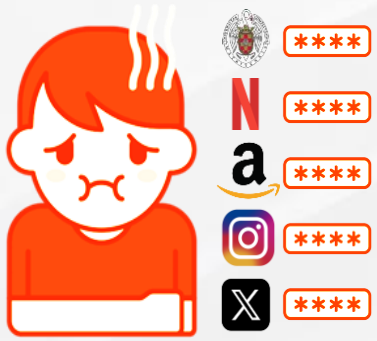
Buenas prácticas

**Nunca** aceptar el autocompletado del navegador.
Es muy fácil visualizar una contraseña desde el navegador.

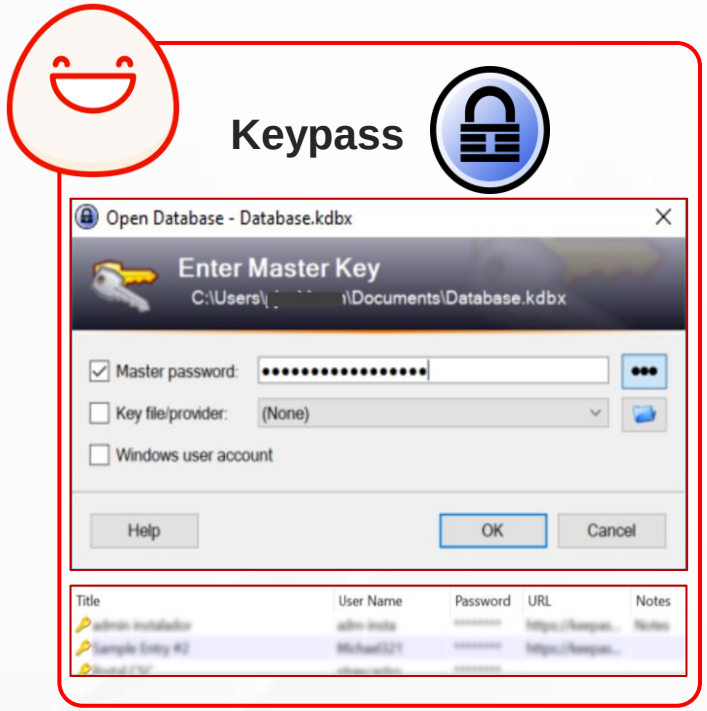
# Contraseñas Robustas

Buenas prácticas




¿Es difícil memorizar muchas contraseñas diferentes?
La solución: **utilizar gestores de contraseñas seguros.**

Los gestores de contraseñas producen y guardan credenciales de manera segura, permitiendo acceder a todos nuestros “USUARIO:CONTRASEÑA” a través de una **clave maestra**, la cual será la única que tengamos que memorizar.




Estos gestores pueden encontrarse para todos los tipos de equipos (PC, smartphone) y sistemas operativos (Windows, Android, IOS, macOS).

INCIBE - Gestores de contraseñas.
https://www.incibe.es/ciudadania/filtro/herramientas?tid=303607&tid_1=All&tid_2=All&tid_3=All

# Gestión de incidentes

Incluso siendo precavidos, pueden ocurrir incidentes. ¿Cómo los gestionamos?

## 1 Comunicación y detección de incidencias de seguridad

Por parte de todos los usuarios, detección y comunicación de actividades anómalas en FGUCM.

## 2 Identificación y registro de la incidencia

Evaluación de la incidencia para confirmar su existencia, naturaleza y amplitud.

## 3 Análisis de la incidencia

Obtener información para responder y describir la incidencia:

- Naturaleza
- Origen
- Sistemas y servicios afectados
- Intención (si se cree aleatorio o planificado)
- Efecto producido (información revelada, paro en servicios...)
- Si ha finalizado o continúa ocurriendo en ese momento.

Para más información, leer el Procedimiento de comunicación, gestión y respuesta ante incidentes

# Gestión de incidentes

Incluso siendo precavidos, pueden ocurrir incidentes. ¿Cómo los gestionamos?

## 4 Respuesta a la incidencia

Puesta en marcha el Plan de actuación para actuar frente a la incidencia.

- Contención
  (Limitación del alcance del incidente)
- Mitigación
  (Reducción del impacto del incidente)
- Recuperación
  (Reactivación de servicios paralizados)

## 5 Seguimiento y cierre de la incidencia

Una vez resuelto el incidente, los elementos afectados se someten a una monitorización para identificar posibles problemas se puedan reproducir.

## 6 Mejora continua de la seguridad

Impulsar la seguridad en base a las experiencias y lecciones aprendidas.
Las acciones de mejora deben contemplar dos ámbitos de aplicación:

- Mejora de la seguridad de la infraestructura física y tecnológica de la FGUCM.
- Mejora de la seguridad en la atención a usuarios de FGUCM y terceros.

Para más información, leer el Procedimiento de comunicación, gestión y respuesta ante incidentes

# Muchas gracias por su atención

# BABEL

**Antonia Pilar Farfán Madrid**
antonia.farfan@babelgroup.com

**Pablo Javier Trescastro Calderón**
pablojavier.tcastro@babelgroup.com