# JORNADA STIC

CAPÍTULO COLOMBIA


# Acceso Seguro a Información Sensible

En colaboración con:

ccn-cert centro criptológico nacional

incibe_

ean

unad


## Jerónimo García Parra

**CEO - Sidertia Solutions**

**jgarcia@sidertia.com**




## Julián Blázquez García

**Gerente Técnico - Sidertia Solutions**

**jblazquez@sidertia.com**

# Evolución Tecnológica

Big Data

Transformación Digital

Inteligencia Artificial

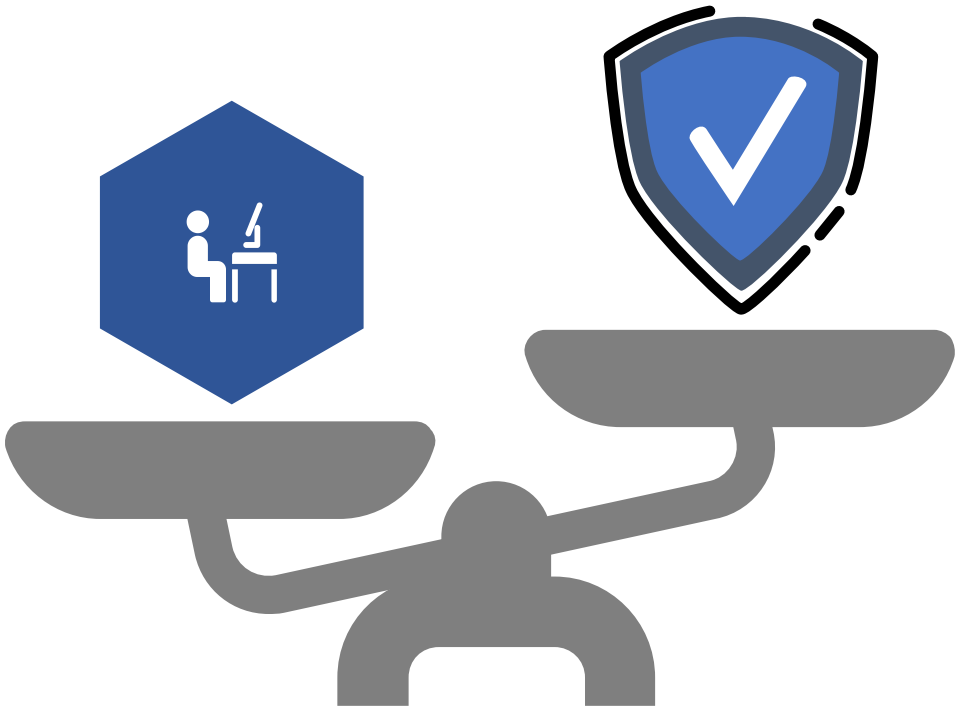
Seguridad

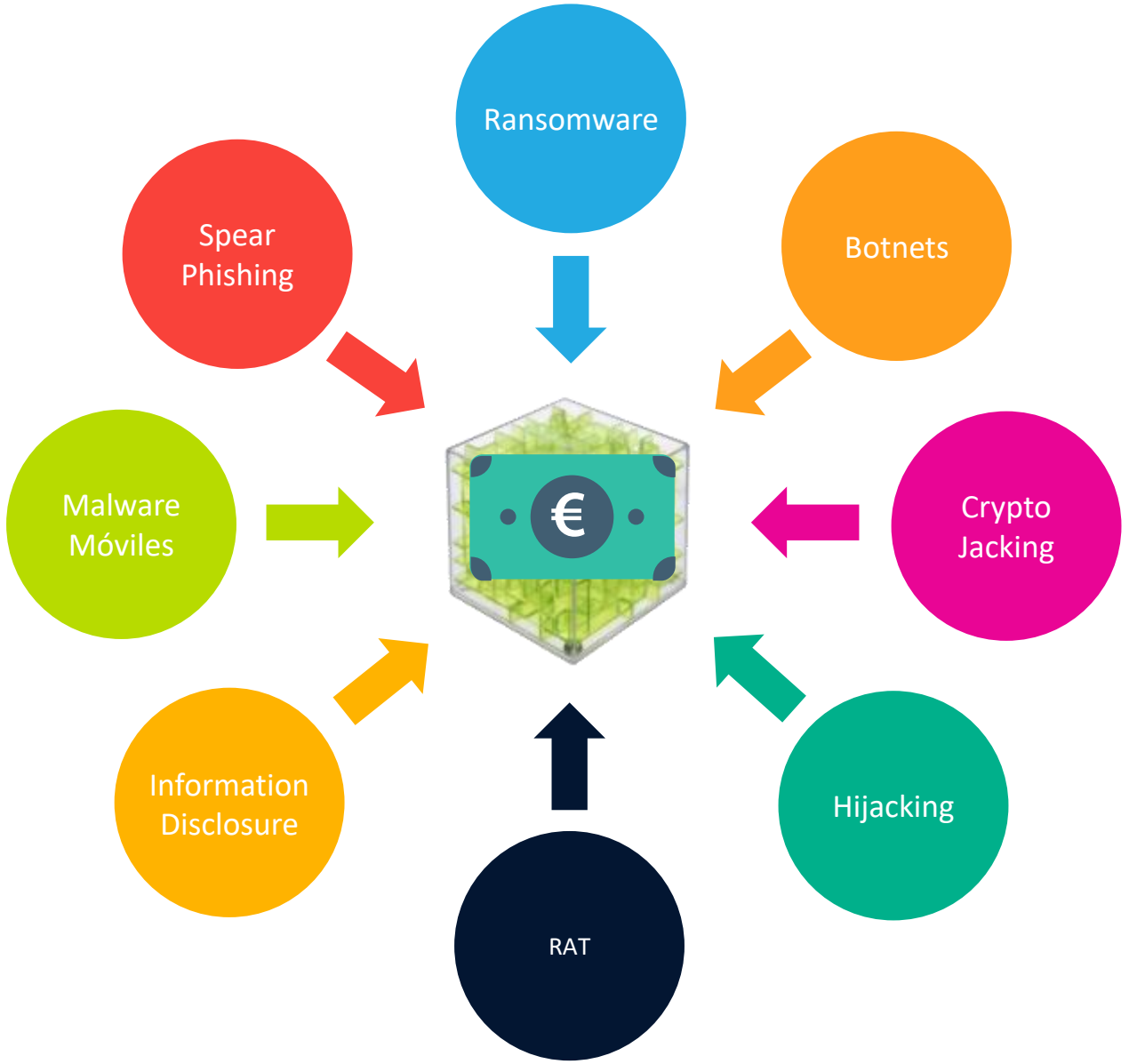
# Problemática

## *Línea Temporal de Proyectos*

# Protección del Dato

## *Amenazas*





# Superficie de Exposición

## Diversidad Usuarios

- Múltiples tipos de usuarios manejando información
- Usuarios Externos con baja confiabilidad
- Empleados con bajo nivel de concienciación
- Equipos no confiables

## Dispersión Geográfica

- Sedes geográficas
- Redes de baja seguridad
- Movilidad de los usuarios
- Teletrabajo
- Dispositivos no Corporativos

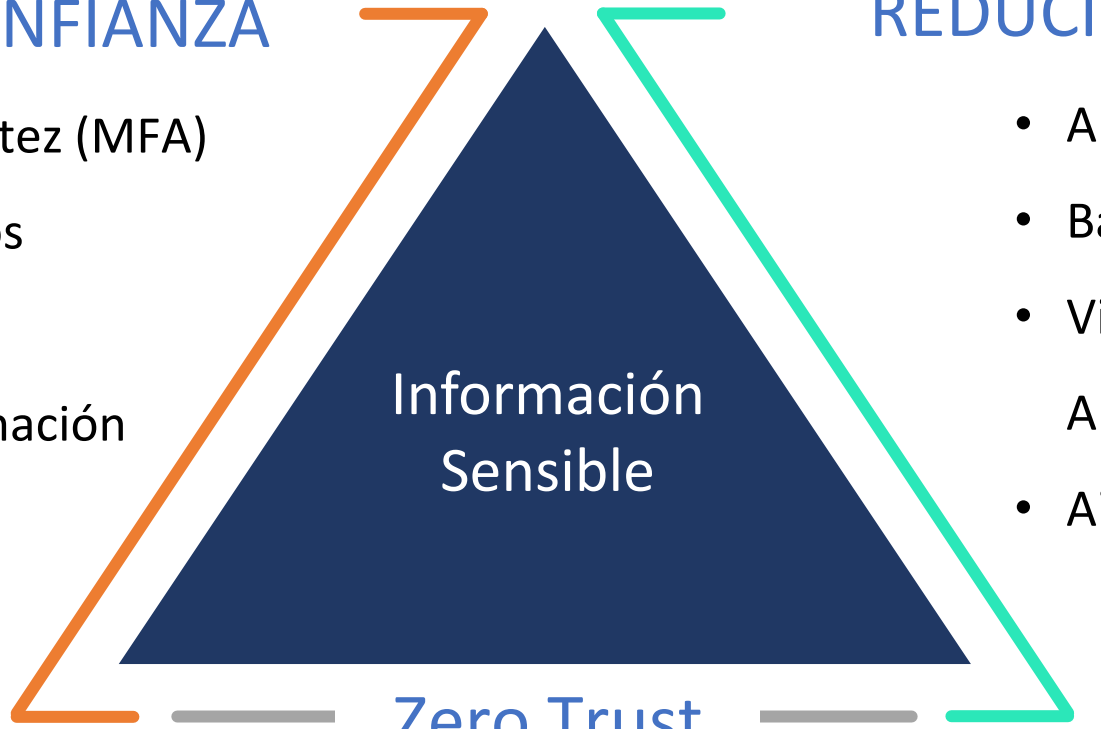
## Servicios Críticos

- Integración de Servicios Potenciales en Organización
- Servicios imprescindibles pero altamente inseguros
- Correo
- Navegación Web

# Reducir Perímetro Seguridad

## INCREMENTAR CONFIANZA

- Identificación y Robustez (MFA)
- Evaluación Dispositivos
- Acceso Contextual
- Trazabilidad de Información




## REDUCIR RIESGO

- Alineamiento Normativo
- Bastionado en profundidad
- Vigilancia (Monitorización y Analítica)
- Aislamiento Servicios Críticos:
  - Correo
  - Navegación

## Zero Trust

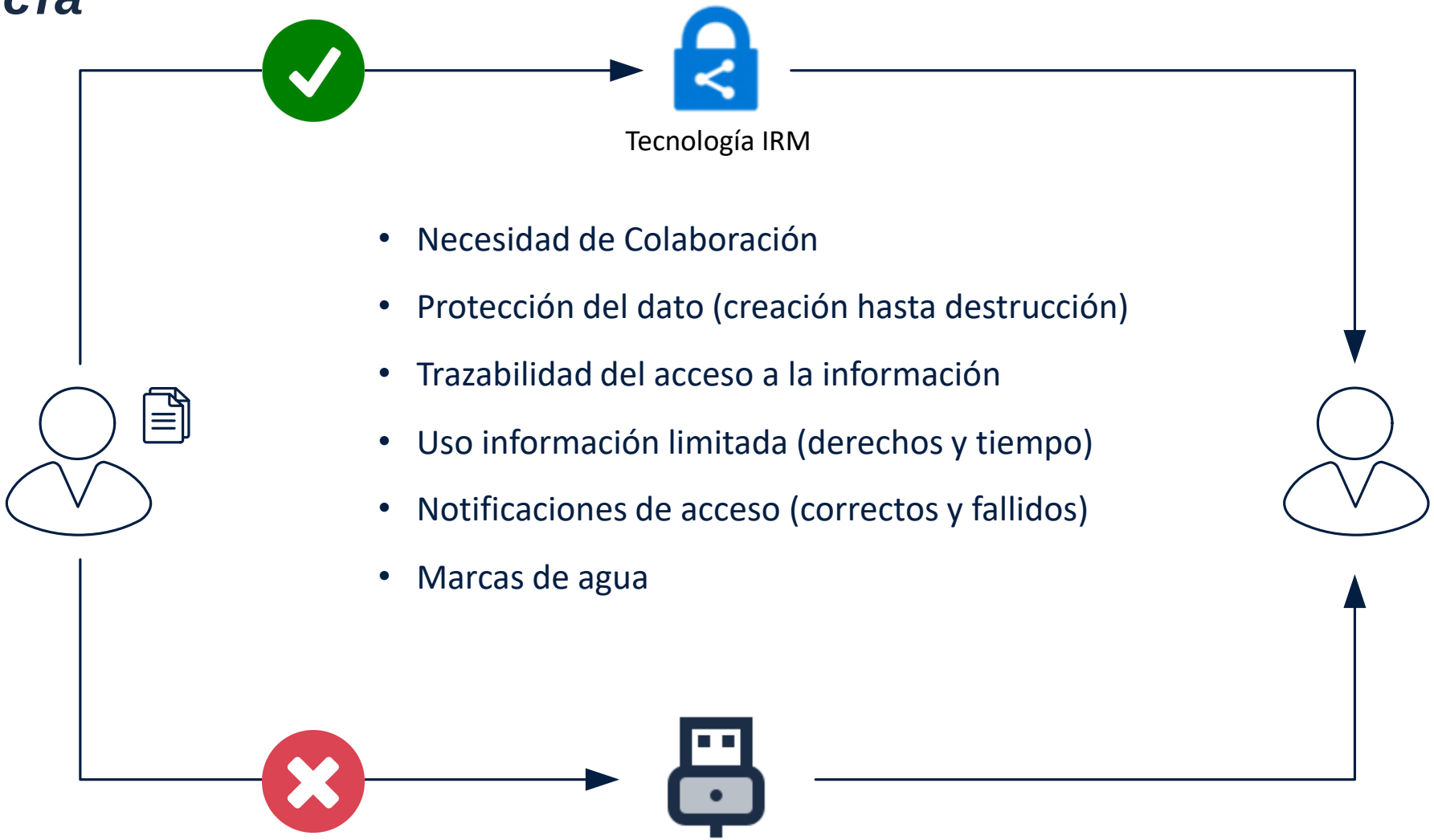
**Usuario Interno:**
- Concienciación

**Administrador:**
- Multi-propósito

**Usuario Externo:**
- Sin Control

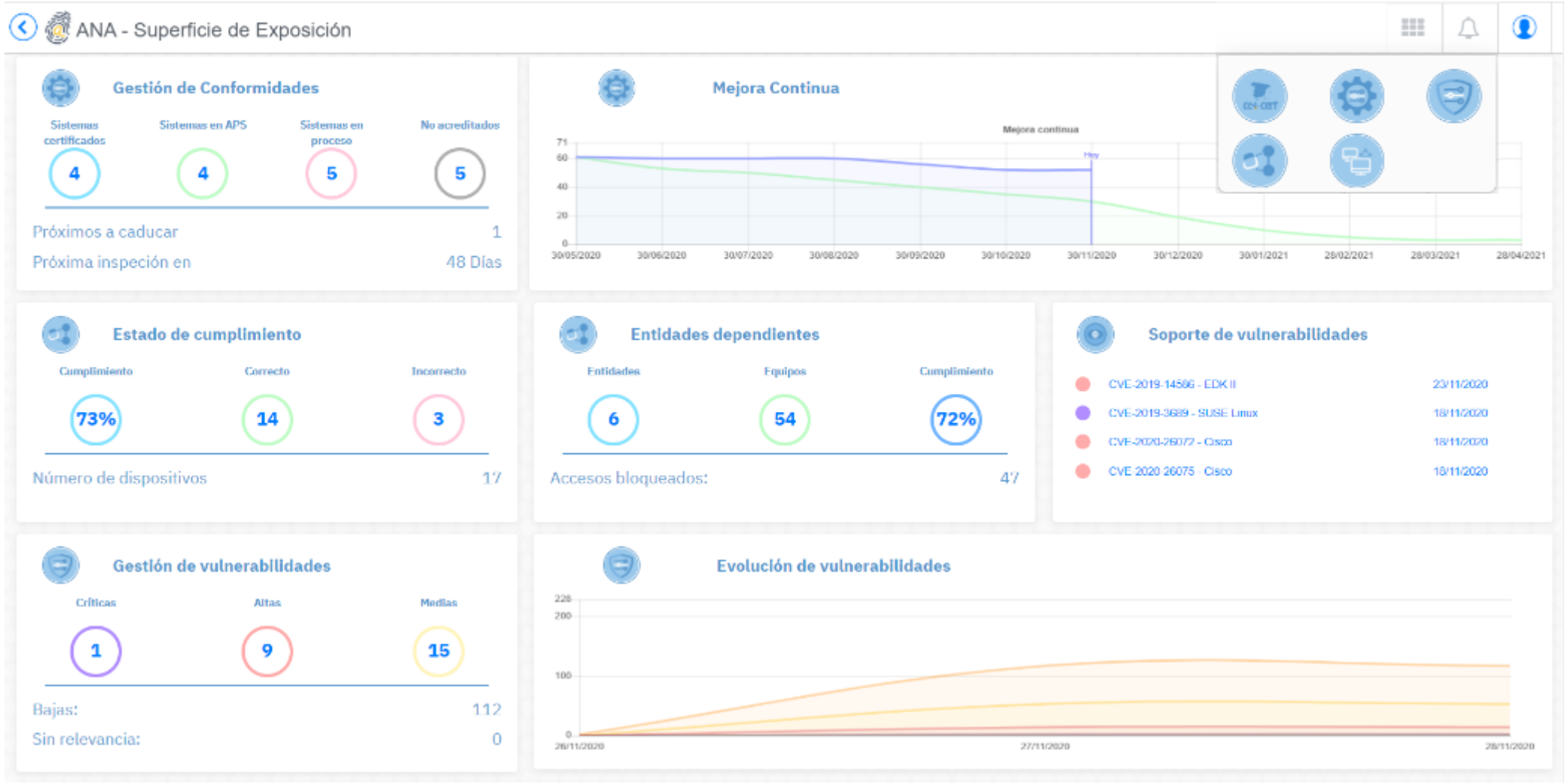
# Trazabilidad Información

## *Vigilancia*

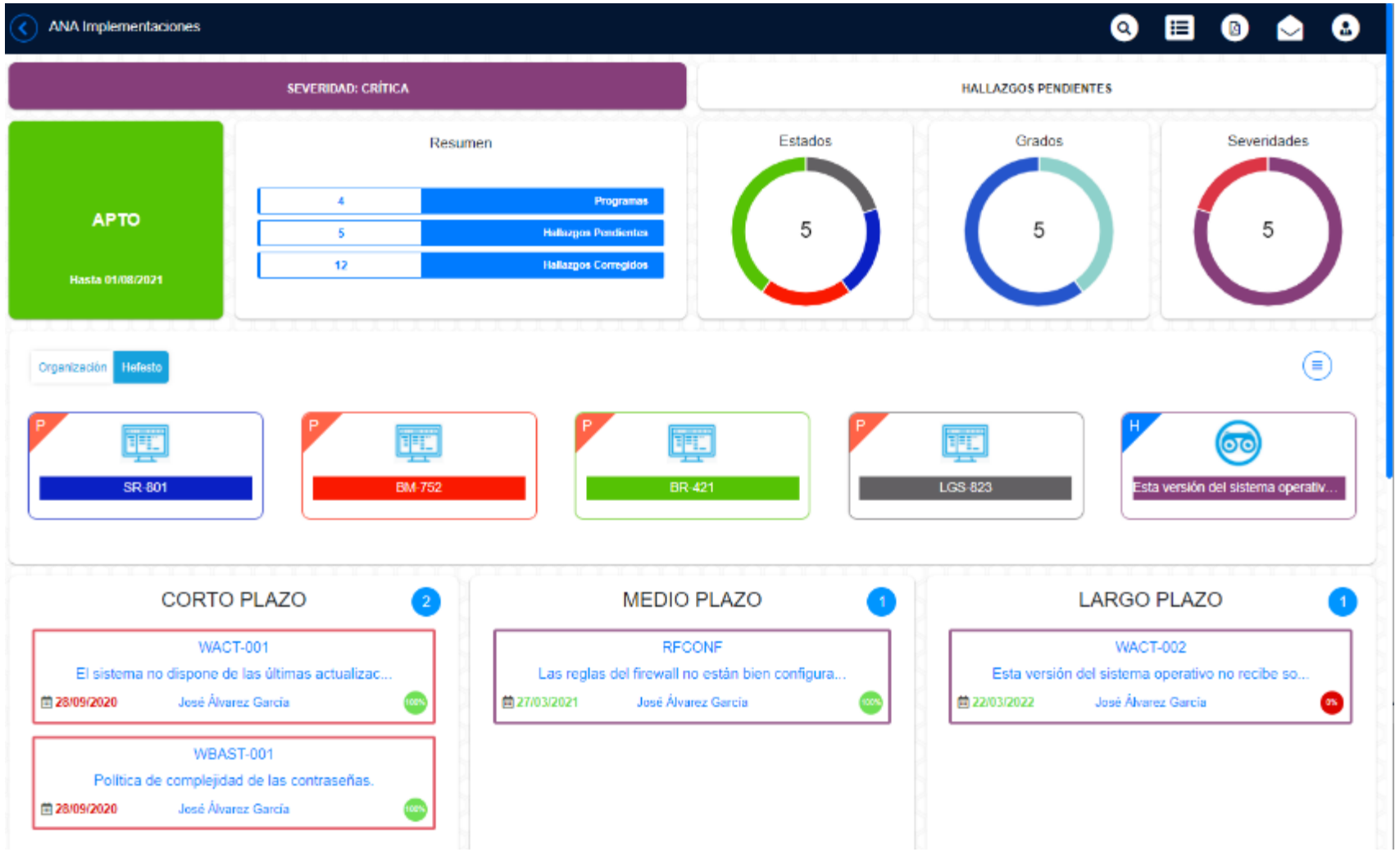



- Necesidad de Colaboración
- Protección del dato (creación hasta destrucción)
- Trazabilidad del acceso a la información
- Uso información limitada (derechos y tiempo)
- Notificaciones de acceso (correctos y fallidos)
- Marcas de agua

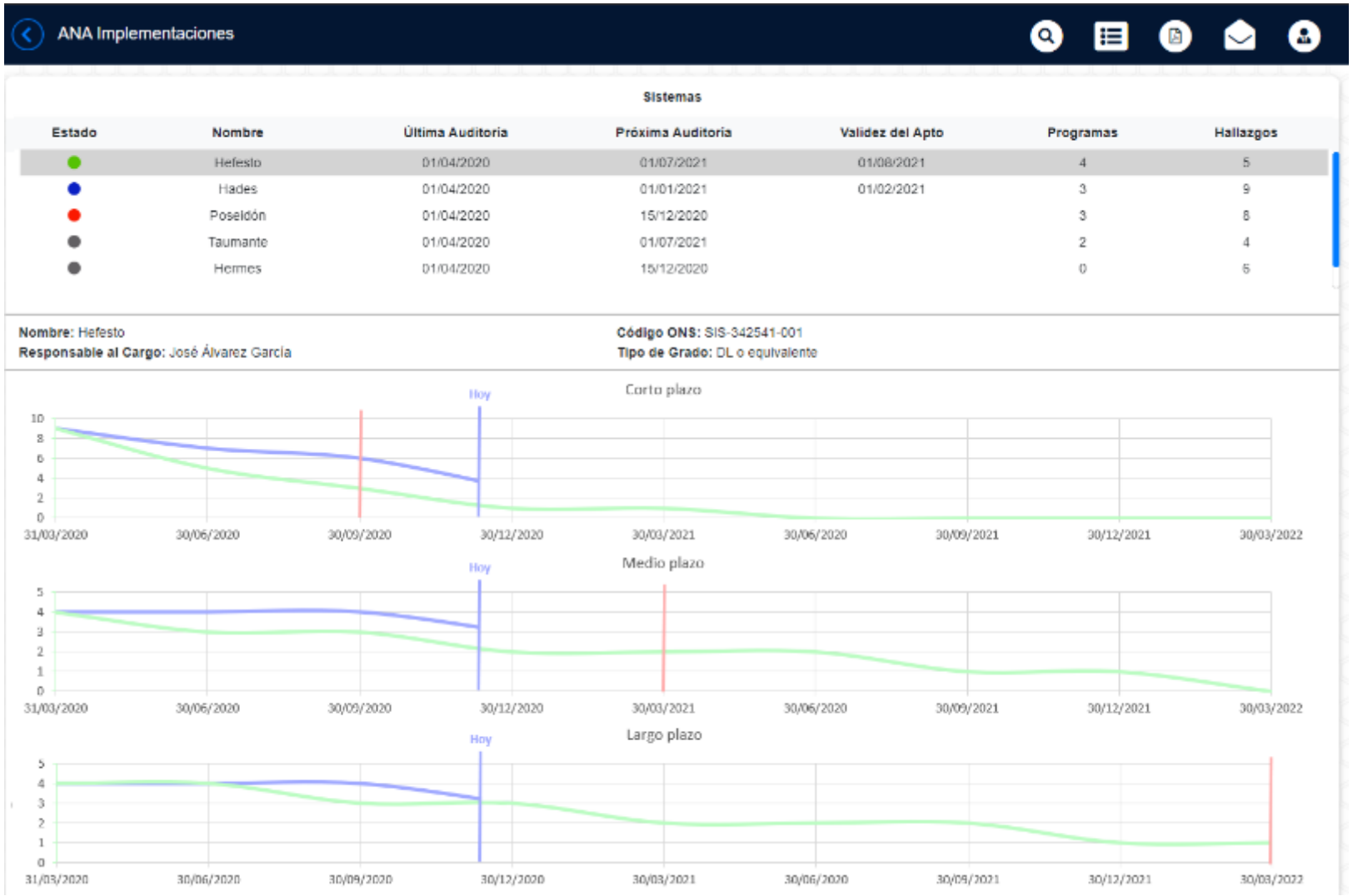
# ANA


ANA - Superficie de Exposición
Gestión de Conformidades
Sistemas certificados
4
Sistemas en APS
4
Sistemas en proceso
5
No acreditados
5
Próximos a caducar
1
Próxima inspeción en
48 Días
Mejora Continua
Mejora continua
Hoy
30/05/2020
30/06/2020
30/07/2020
30/08/2020
30/09/2020
30/10/2020
30/11/2020
30/12/2020
30/01/2021
28/02/2021
28/03/2021
28/04/2021
Estado de cumplimiento
Cumplimiento
73%
Correcto
14
Incorrecto
3
Número de dispositivos
17
Entidades dependientes
Entidades
6
Equipos
54
Cumplimiento
72%
Accesos bloqueados:
47
Soporte de vulnerabilidades
CVE-2019-14586 - EDK II
23/11/2020
CVE-2019-3689 - SUSE Linux
18/11/2020
CVE-2020-26072 - Cisco
18/11/2020
CVE-2020-26075 - Cisco
18/11/2020
Gestión de vulnerabilidades
Críticas
1
Altas
9
Medias
15
Bajas:
112
Sin relevancia:
0
Evolución de vulnerabilidades
26/11/2020
27/11/2020
28/11/2020

# ANA - Implementaciones



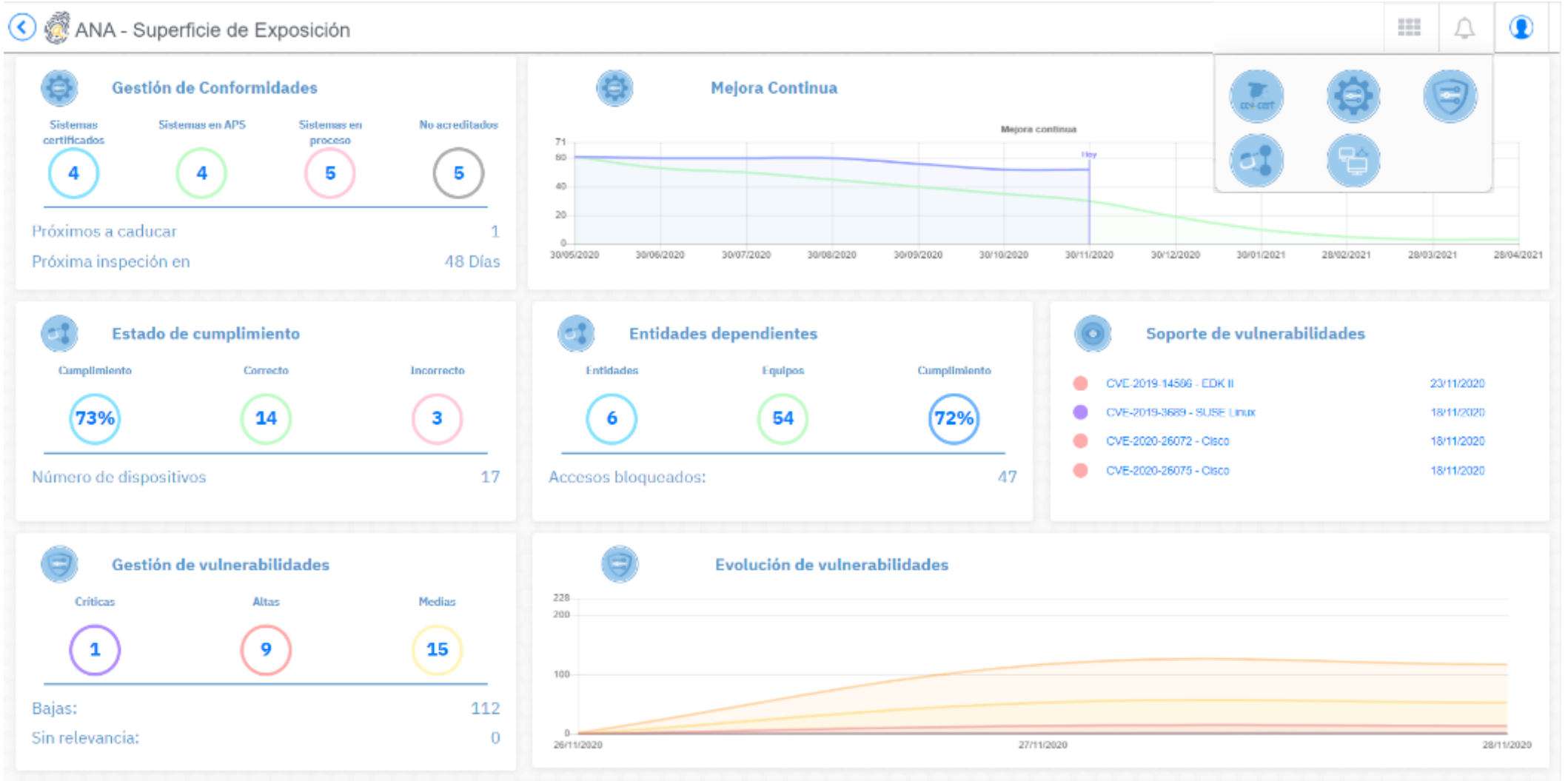
# ANA - Hoja de Ruta



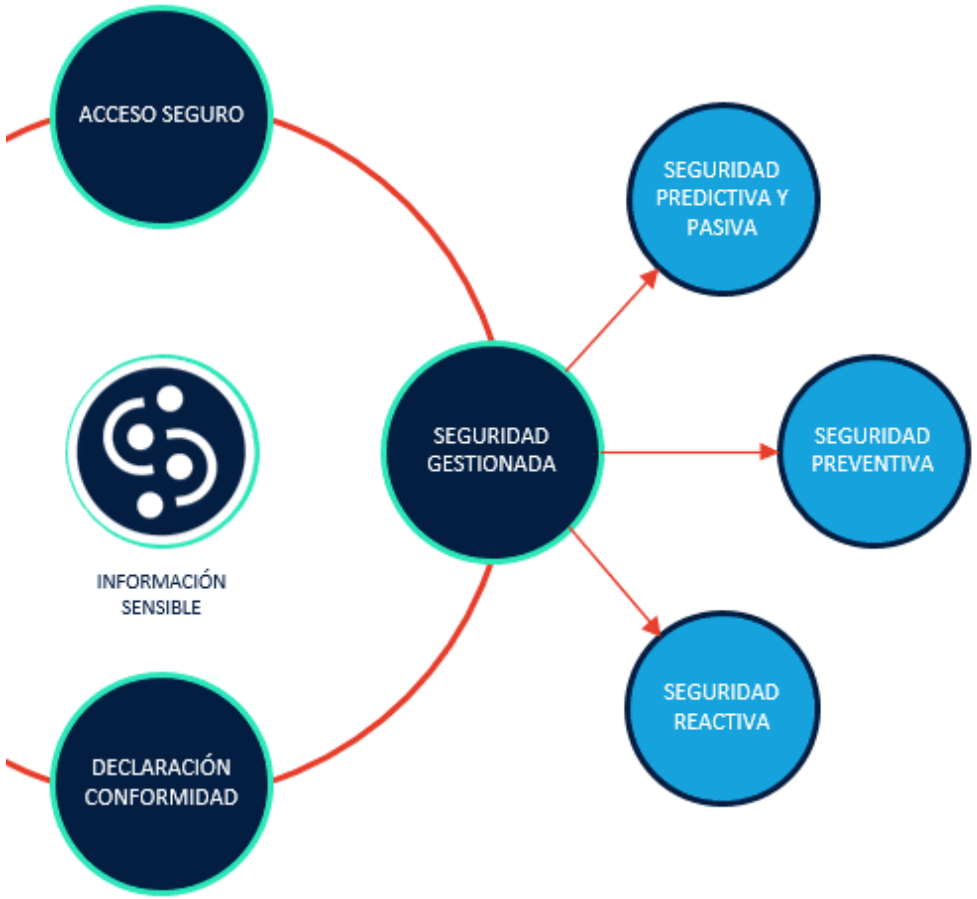
# ANA – Zero Trust


- Conocer el estado de cumplimiento normativo de seguridad de los activos tecnológicos que consumen datos
- Capacidad de medir el nivel de bastionado y confiabilidad de los equipos externos

# ANA


ANA - Superficie de Exposición
Gestión de Conformidades
Sistemas certificados
4
Sistemas en APS
4
Sistemas en proceso
5
No acreditados
5
Próximos a caducar
1
Próxima inspeción en
48 Días
Mejora Continua
Mejora continua
Hoy
71
60
40
20
0
30/05/2020
30/06/2020
30/07/2020
30/08/2020
30/09/2020
30/10/2020
30/11/2020
30/12/2020
30/01/2021
28/02/2021
28/03/2021
28/04/2021
Estado de cumplimiento
Cumplimiento
73%
Correcto
14
Incorrecto
3
Número de dispositivos
17
Entidades dependientes
Entidades
6
Equipos
54
Cumplimiento
72%
Accesos bloqueados:
47
Soporte de vulnerabilidades
CVE-2019-14596 - EDK II
23/11/2020
CVE-2019-3689 - SUSE Linux
18/11/2020
CVE-2020-26072 - Cisco
18/11/2020
CVE-2020-26075 - Cisco
18/11/2020
Gestión de vulnerabilidades
Críticas
1
Altas
9
Medias
15
Bajas:
112
Sin relevancia:
0
Evolución de vulnerabilidades
228
200
100
0
26/11/2020
27/11/2020
28/11/2020

# Sidertia




## Proteger

### Es garantizar la integridad digital del dato

Activo fundamental de una Organización.

Custodia y correcto manejo.

Factores diferenciadores que aportan prestigio y confianza.

Soluciones centralizadas basadas en microservicios.

## Securizar

### Es determinar el modelo de encapsulación del dato

Diseñar, implementar y aplicar las medidas requeridas por cada tipo de negocio o actividad, deriva en una capacidad preventiva ante ciberataques y fugas de información.

## Normativa

### Es concienciar para potenciar la experiencia del usuario

La evolución tecnológica deja en manos del fabricante la garantía de su producto. La fiabilidad de una solución debe exigir tanto  la aplicación de Medidas Técnicas como Medidas Organizativas.

JORNADA STIC

CAPÍTULO COLOMBIA

# GRACIAS


En colaboración con:

cn-cert centro criptológico nacional

incibe_

ean

unir