OFICINA Acelera pyme

CON PASO SEGURO EN CIBERSEGURIDAD

01/02/2024

Fondo Europeo de Desarrollo Regional

"Europa se siente"

JORNADAS DE CIBERSEGURIDAD

REQUISITOS LEGALES Y TÉCNICOS PARA CUMPLIR CON LA NORMATIVA ESPAÑOLA Y EUROPEA

Normativa Y Estándares

NORMATIVA Y ESTÁNDARES

ISO/IEC
Serie
27000+

Esquema
Nacional de
Seguridad

GDPR
LOPDGDD

Directiva NIS
Y NIS 2

Código Penal
(Prevención
de Delitos en
la Empresa)

NORMATIVA Y ESTÁNDARES

ISO 27001 – 114 controles en 14 secciones

ISO/IEC
Serie
27000+

- Políticas
- Organización
- Seguridad en los recursos humanos
- Gestión de activos
- Controles de acceso
- Criptografía
- Seguridad física y del entorno
- Seguridad operacional
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento del sistema
- Relación con proveedores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información para la gestión de la continuidad del negocio
- Cumplimiento

NORMATIVA Y ESTÁNDARES

ISO 27001 – Declaración de Aplicabilidad

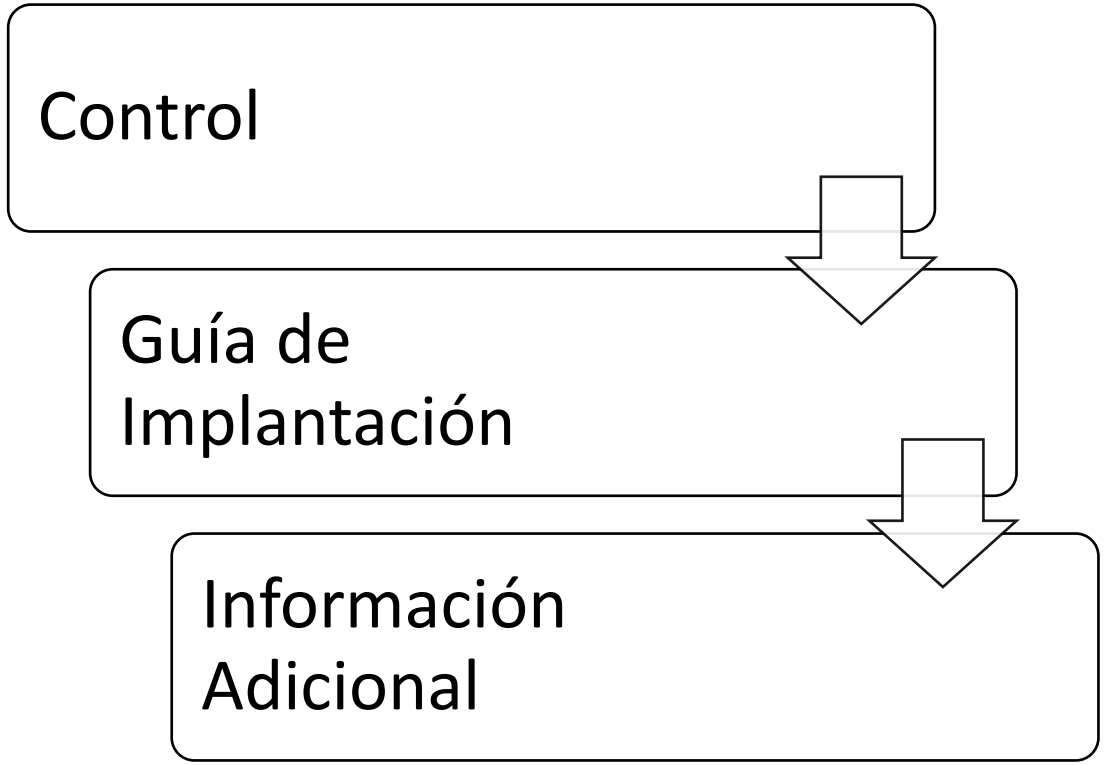
ISO/IEC Serie 27000+

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/ BP	RRA	
Cláusula	**Sección**	**Objetivo de control / control**							
5 Políticas de Seguridad	5,1	Dirección de la alta gerencia para la seguridad de la información							
	5.1.1	Políticas de seguridad de la información							
	5.1.2	Revisión de las políticas de seguridad de la información							
6 Organización de la Seguridad de la Información	6,1	Organización interna							
	6.1.1	Roles y responsabilidad de seguridad de la información							
	6.1.2	Segregación de deberes							
	6.1.3	Contacto con autoridades							
	6.1.4	Contacto con grupos de interés especial							
	6.1.5	Seguridad de la información en la gestión de proyectos							
	6,2	Dispositivos móviles y teletrabajo							
	6.2.1	Política de dispositivos móviles							
	6.2.2	Teletrabajo							
7 Seguridad en los Recursos Humanos	7,1	Previo al empleo							
	7.1.1	Verificación de antecedentes							
	7.1.2	Términos y condiciones del empleo							
	7,2	Durante el empleo							
	7.2.1	Responsabilidades de la Alta Gerencia							
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información							
	7.2.3	Proceso disciplinario							
	7,3	Terminación y cambio de empleo							
	7.3.1	Termino de responsabilidades o cambio de empleo							

NORMATIVA Y ESTÁNDARES

ISO 27002 – Guía de Implantación de Controles

ISO/IEC
Serie
27000+



NORMATIVA Y ESTÁNDARES

Esquema Nacional de Seguridad

El sistema será de categoría	¿Cuándo?
ALTA	Si alguna de sus dimensiones de seguridad alcanza el nivel ALTO
MEDIA	Si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO y ninguna el nivel ALTO
BÁSICA	Si alguna de sus dimensiones de seguridad alcanza el nivel BAJO y ninguna el nivel medio o alto

NORMATIVA Y ESTÁNDARES

Esquema Nacional de Seguridad

2. Las medidas de seguridad se dividen en tres grupos:
   a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
   b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
   c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (Anexo II)

https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

DARKNET systems SKYNET SYSTEMS INTPIRE

NORMATIVA Y ESTÁNDARES

Esquema Nacional de Seguridad

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad BAJO Categoría de seguridad del sistema BÁSICA	MEDIO MEDIA	ALTO ALTA
org	**Marco organizativo**				
org.1	Política de seguridad	Categoría	aplica	aplica	aplica
org.2	Normativa de seguridad	Categoría	aplica	aplica	aplica
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica

https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

NORMATIVA Y ESTÁNDARES

Esquema Nacional de Seguridad

op	Marco operacional				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento /gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica

https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

NORMATIVA Y ESTÁNDARES

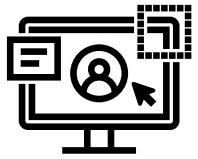
Esquema Nacional de Seguridad

mp	Medidas de protección				
mp.if	Protección de las instalaciones e infraestructuras				
mp.if.1	Áreas separadas y con control de acceso	Categoría	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Categoría	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Categoría	aplica	aplica	aplica
mp.if.4	Energía eléctrica	D	aplica	+ R1	+ R1
mp.if.5	Protección frente a incendios	D	aplica	aplica	aplica

https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

NORMATIVA Y ESTÁNDARES

Derechos del Usuario

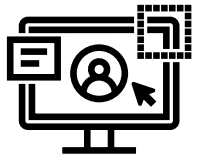


GDPR
LOPDGDD

- Derecho de acceso
- Derecho de rectificación
- Derecho de oposición
- Derecho de supresión ("al olvido")
- Derecho a la limitación del tratamiento
- Derecho a la portabilidad
- Derecho a no ser objeto de decisiones individuales automatizadas
- Derecho de información

https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

NORMATIVA Y ESTÁNDARES



GDPR
LOPDGDD

Deberes del Responsable

- Registro de actividades de tratamiento
- Inventario de actividades de tratamiento
- Designación de un delegado de protección de datos
- Evaluación del riesgo que, para los derechos y libertades de los interesados, podría suponer un tratamiento de datos personales
- Realización de evaluaciones de impacto para la protección de datos
- Consulta previa
- Protección de datos desde el diseño
- Protección de datos por defecto
- Seguridad de los tratamientos de datos
- Notificación de brechas de datos personales a la Autoridad de Control
- Comunicación de brechas de datos personales a los interesados
- Códigos de conducta
- Establecimiento de garantías para las transferencias de datos personales a terceros países u organizaciones internacionales

https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

DarkNet Systems SkyNet Systems INTPIRE

NORMATIVA Y ESTÁNDARES

Directiva NIS

Sectores Críticos / Esenciales

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Obligatoria

Entidades en el listado del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)

- Proveedor de servicios digitales
- Administración
- Espacio
- Industria nuclear
- Industria química
- Instalaciones de investigación
- Agua
- Energía
- Salud
- Tecnologías de la Información y las Comunicaciones (TIC)
- Transporte
- Alimentación
- Sistema financiero y tributario

https://www.boe.es/buscar/pdf/2018/BOE-A-2018-12257-consolidado.pdf

NORMATIVA Y ESTÁNDARES

Directiva NIS

Sectores Críticos / Esenciales

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Obligaciones de seguridad

- **Designación de un Responsable de Seguridad de la Información**
- Establecer una Política de Seguridad con atención al menos a los siguientes puntos:
  - Análisis y gestión de riesgos.
  - Gestión de riesgos de terceros o proveedores.
  - Catálogo de medidas de seguridad, organizativas, tecnológicas y físicas.
  - Gestión del personal y profesionalidad.
  - Adquisición de productos o servicios de seguridad.
  - Detección y gestión de incidentes.
  - Planes de recuperación y aseguramiento de la continuidad de las operaciones.
  - Mejora continua.
  - Interconexión de sistemas.
  - Registro de la actividad de los usuarios.
- Notificar incidentes
- Supervisión por la autoridad

CSIRT de Referencia

- CCN-CERT
- INCIBE-CERT
- ESPDEF-CERT

https://www.boe.es/buscar/pdf/2018/BOE-A-2018-12257-consolidado.pdf

DARKNET systems SKYNET SYSTEMS INTPIRE

NORMATIVA Y ESTÁNDARES

Directiva NIS 2

Sectores Críticos / Esenciales

27 de diciembre de 2022 → 17 de octubre de 2024

Obligatoria

- 250+ empleados
- Facturación anual 50M+ €
- Balance anual 43M+ €
- Sectores críticos

Medidas de seguridad

- Análisis de riesgos
- Políticas de seguridad
- Formación y concienciación
- Respuesta a incidentes
- Continuidad del negocio
- Gestión de crisis
- Encriptación
- Seguridad de la cadena de suministro
- Métricas en gestión de riesgos
- Divulgación de vulnerabilidades

https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

DARKNET systems SKYNET SYSTEMS INTPIRE

NORMATIVA Y ESTÁNDARES

Directiva NIS 2

Sectores Críticos / Esenciales

27 de diciembre de 2022 → 17 de octubre de 2024

Notificaciones de Incidentes

- 24 h > Inicial
- 1 mes > Actualización

Multas por Incumplimiento

- 2% Facturación anual
- 10M €

https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

NORMATIVA Y ESTÁNDARES

Código Penal (Prevención de Delitos en la Empresa)

Artículo 31 bis. (Código Penal)

1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables:

a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.

b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.

https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

DARKNET systems SKYNET SYSTEMS INTPIRE

NORMATIVA Y ESTÁNDARES

Código Penal (Prevención de Delitos en la Empresa)

Artículo 33. (Código Penal)

...

7. Las penas aplicables a las personas jurídicas, que tienen todas la consideración de graves, son las siguientes:

a) Multa por cuotas o proporcional.

b) Disolución de la persona jurídica. La disolución producirá la pérdida definitiva de su personalidad jurídica, así como la de su capacidad de actuar de cualquier modo en el tráfico jurídico, o llevar a cabo cualquier clase de actividad, aunque sea lícita.

c) Suspensión de sus actividades por un plazo que no podrá exceder de cinco años.

d) Clausura de sus locales y establecimientos por un plazo que no podrá exceder de cinco años.

e) Prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito. Esta prohibición podrá ser temporal o definitiva. Si fuere temporal, el plazo no podrá exceder de quince años.

f) Inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social, por un plazo que no podrá exceder de quince años.

g) Intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario, que no podrá exceder de cinco años.

https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

NORMATIVA Y ESTÁNDARES

Código Penal (Prevención de Delitos en la Empresa)

Delitos especialmente relevantes en materia de Ciberseguridad

- Descubrimiento y Revelación de Secretos
- Allanamiento Informático
- Daños Informáticos
- Revelación de Secretos de Empresa (Contra la Propiedad Intelectual e Industrial)
- Producción o tenencia de Pornografía Infantil
- Odio y Enaltecimiento

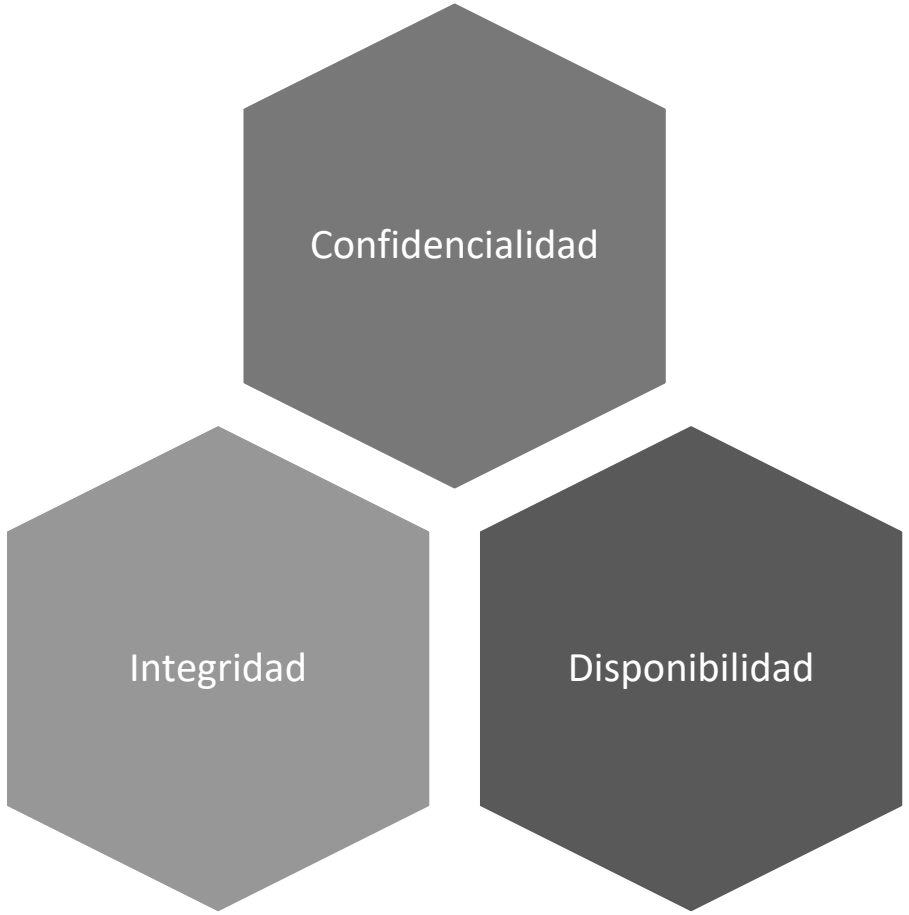
https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

Activos

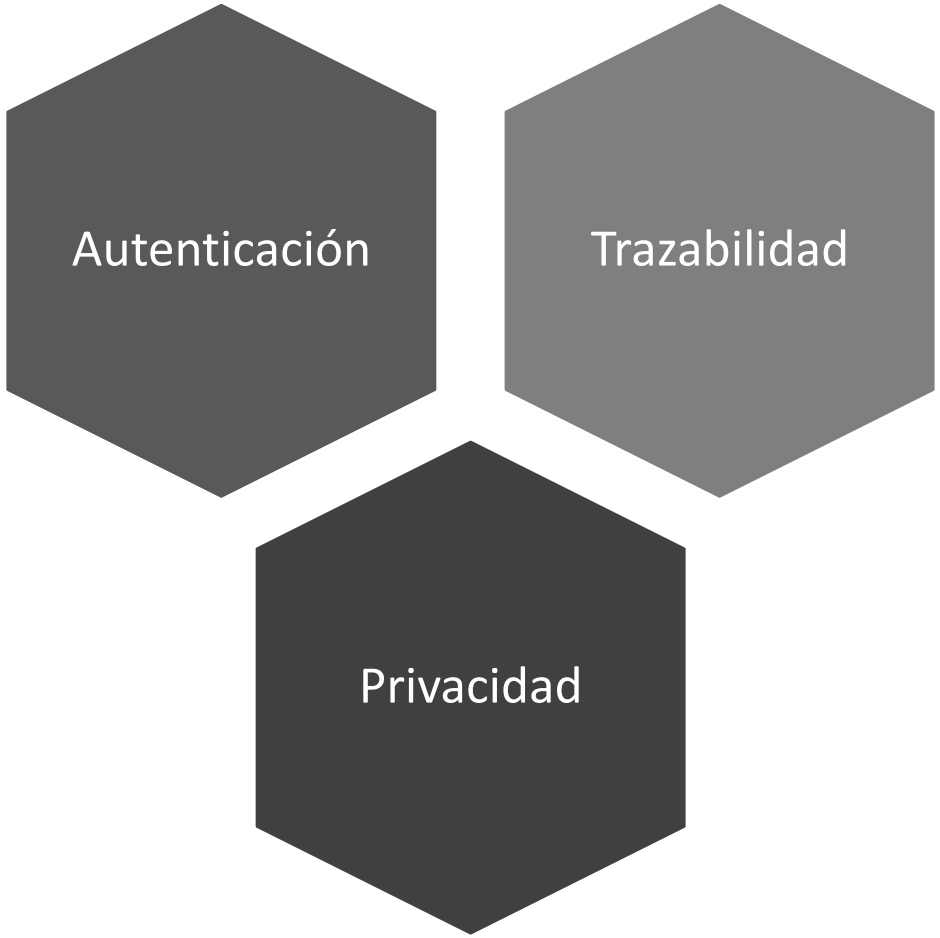
TIPOS DE ACTIVOS

Sistemas	Servicios
Personal	**Información**
Dispositivos de seguridad	**Redes y Comunicaciones**
Servicios Auxiliares	**Instalaciones**

Dimensiones de Seguridad



DIMENSIONES DE SEGURIDAD

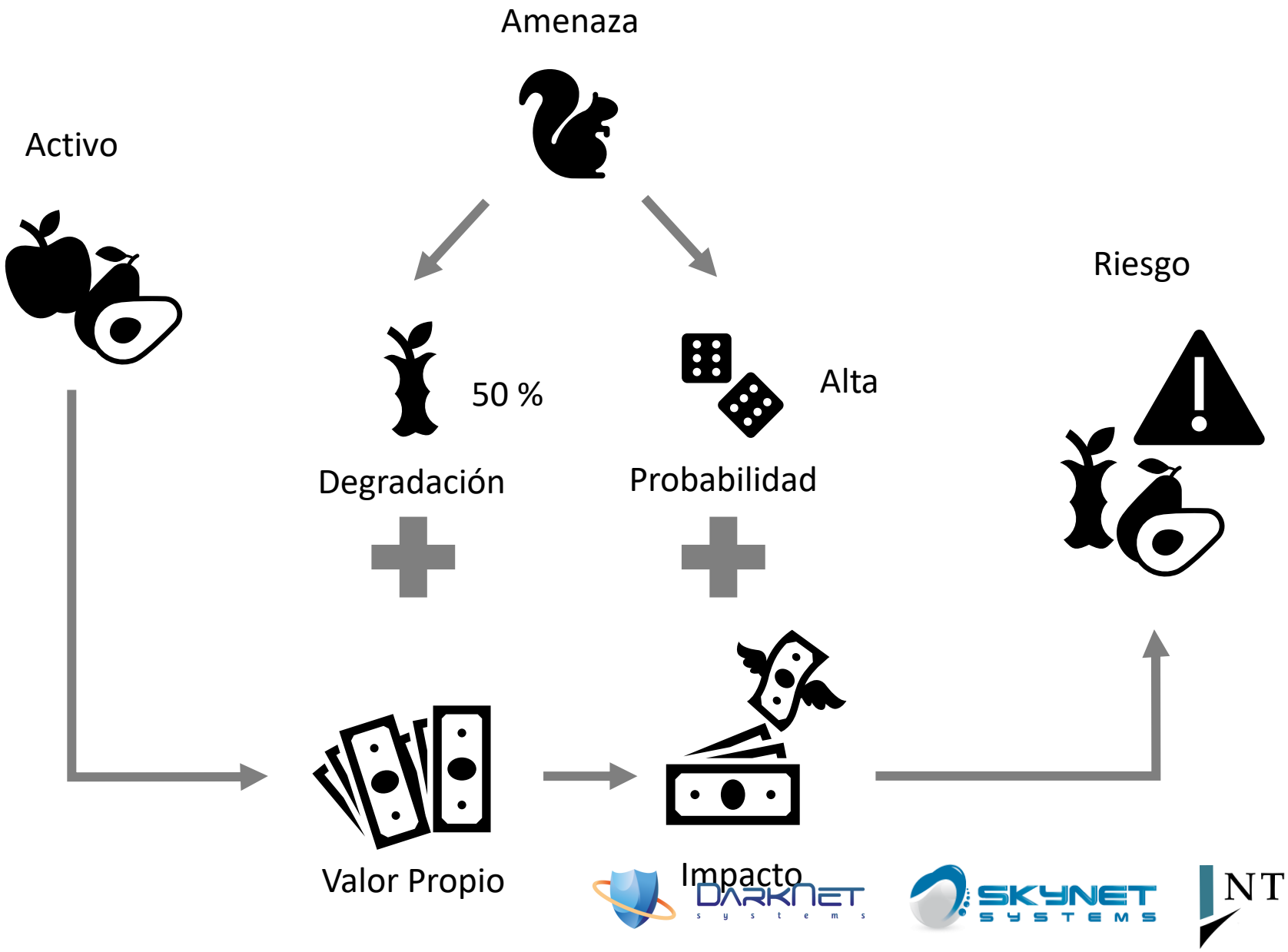


DIMENSIONES DE SEGURIDAD

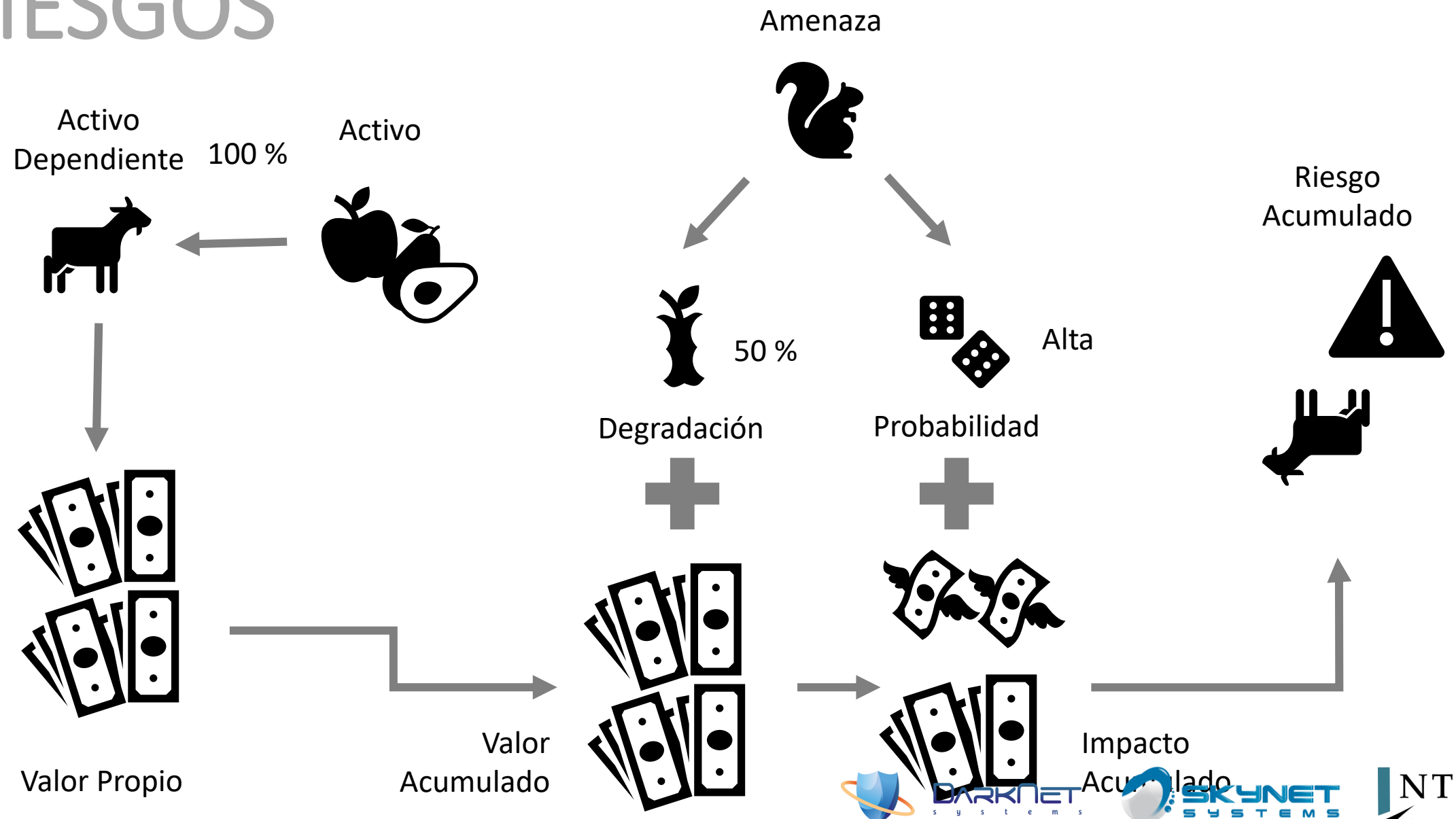
DarkNet Systems SKYNET SYSTEMS INTPIRE

Riesgos

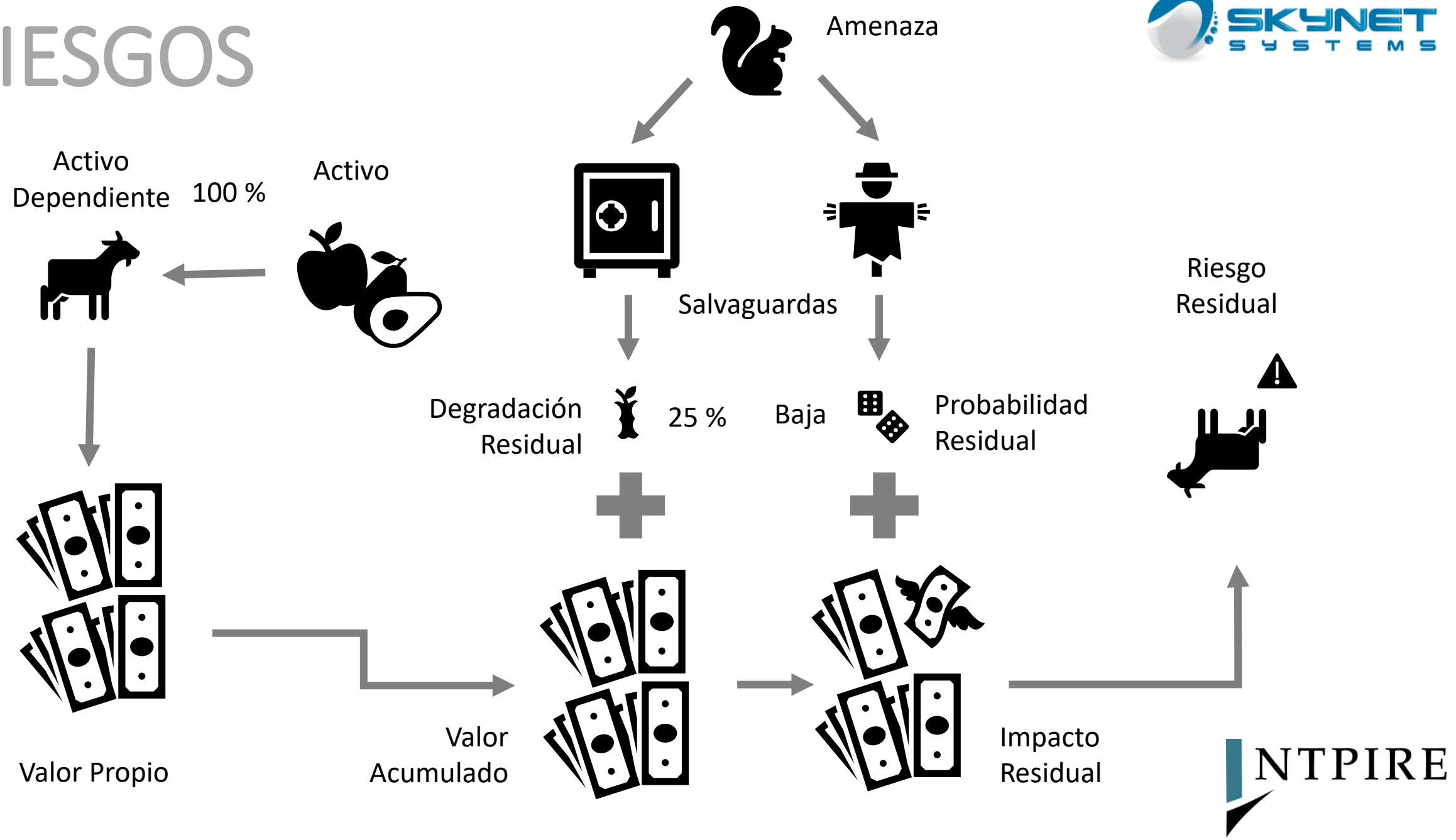
RIESGOS


Amenaza
Activo
50 %
Alta
Riesgo
Degradación
Probabilidad
Valor Propio
Impacto

RIESGOS


Amenaza
Activo
Dependiente
100 %
Activo
Riesgo
Acumulado
50 %
Alta
Degradación
Probabilidad
Valor Propio
Valor
Acumulado
Impacto
Acumulado

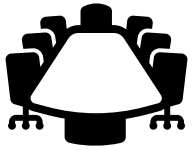
RIESGOS


Amenaza
Activo
Dependiente
100 %
Activo
Salvaguardas
Riesgo
Residual
Degradación
Residual
25 %
Baja
Probabilidad
Residual
Valor Propio
Valor
Acumulado
Impacto
Residual

Medidas de Seguridad Organizativas

MEDIDAS DE SEGURIDAD ORGANIZATIVAS

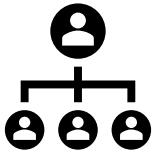
Redacción de Políticas y Protocolos



Asignación de Responsabilidades

Clasificación de la Información

Segregación de Tareas



Asignación de Permisos

Control de Recursos Humanos

Planes de Concienciación

Plan de Recuperación de Desastres

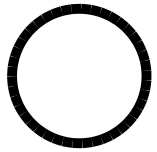
Control de Cadenas de Suministro

Auditorías y Revisiones

Estrategias y Posturas de Ciberseguridad

ESTRATEGIAS Y POSTURAS DE CIBERSEGURIDAD

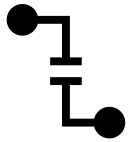
Mínimo Privilegio Necesario



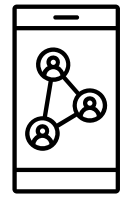
Zero Trust

Cebolla

Alcachofa



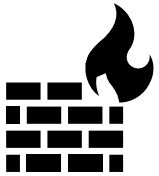
Air Gapping



Modelos de Movilidad BYOD vs COBO

Medidas de Seguridad Técnicas

MEDIDAS DE SEGURIDAD TÉCNICAS



Firewalls

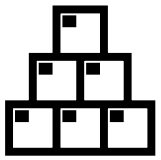
Antivirus / Antimalware

IDS/IPS

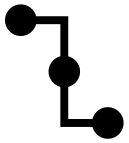
EDR / XDR

Sandbox / Virtualización

Bastionado de Sistemas



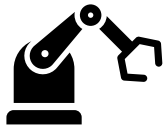
Inventarios



VPN

Honeypots / Honeyfiles

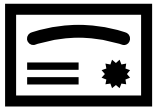
SIEM



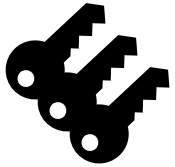
SOAR

Equipo DFIR

MEDIDAS DE SEGURIDAD TÉCNICAS



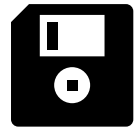
Certificados Digitales



MFA

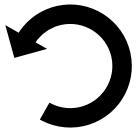
Balanceadores de Carga

Seguridad Física y Electrónica



Copias de Seguridad

Exposición y Huella Digital



Actualización y Parcheo

NAC

Filtros de Email

Criptografía Adecuada

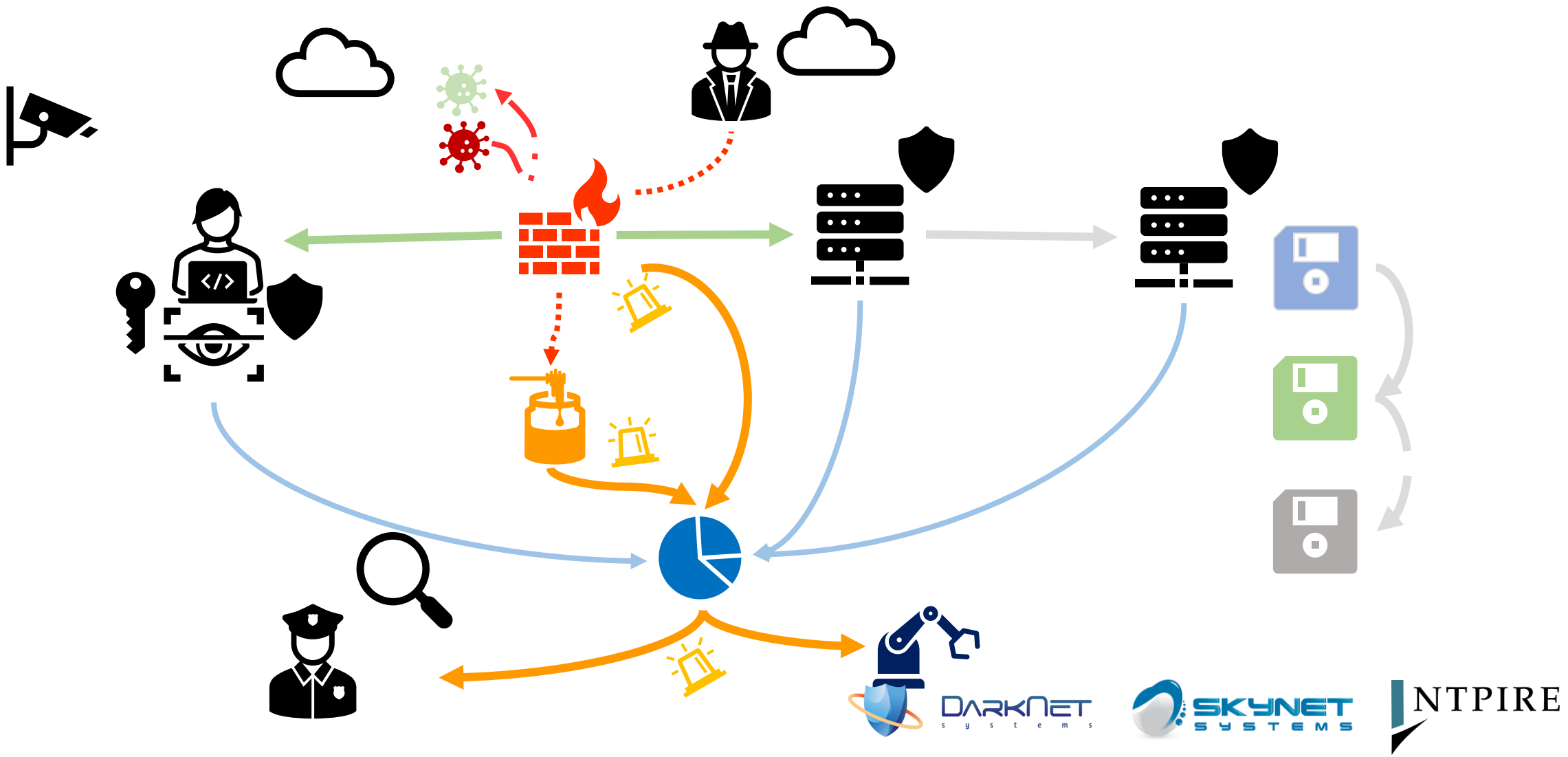
Alimentación y Servicios Auxiliares

Inteligencia de Amenazas

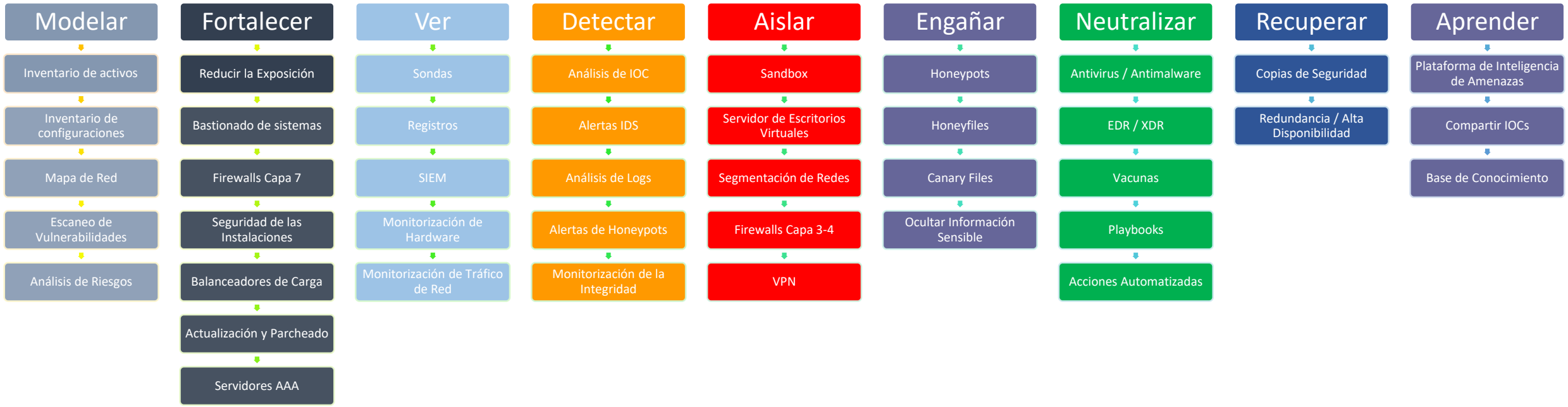
MEDIDAS DE SEGURIDAD TÉCNICAS

Y cada día más…

MEDIDAS DE SEGURIDAD TÉCNICAS



MEDIDAS DE SEGURIDAD TÉCNICAS



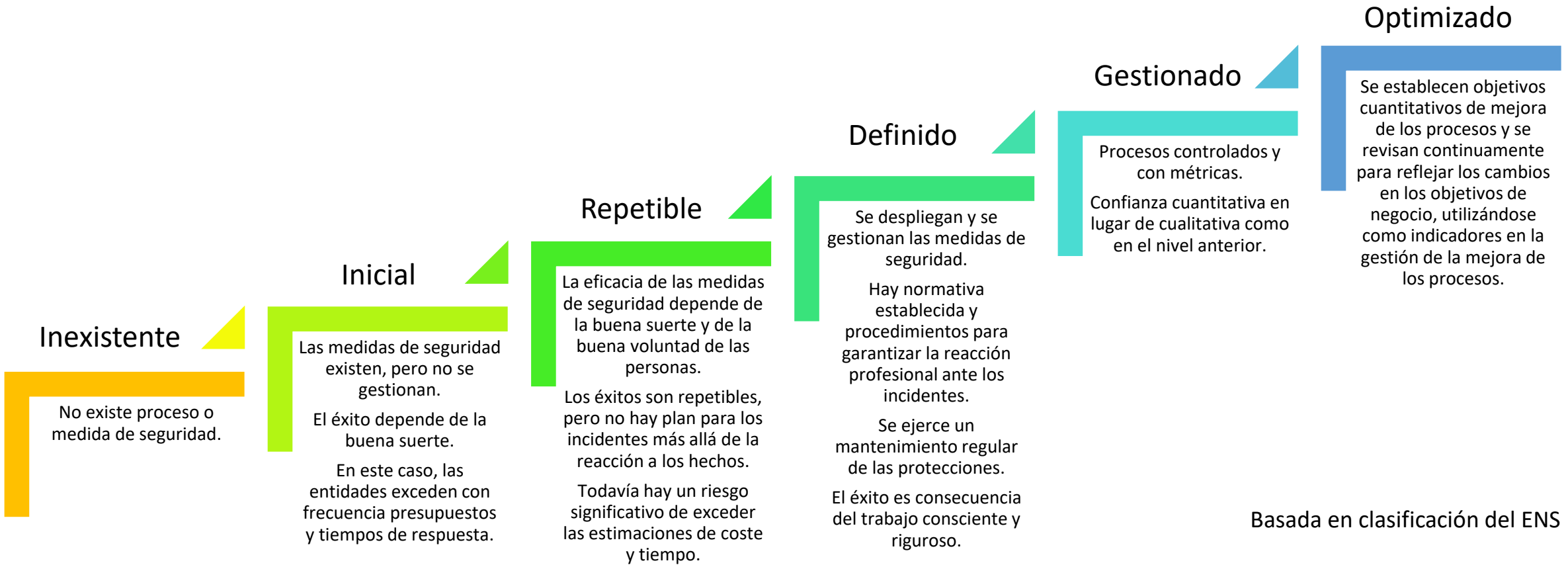
DARKNET systems

SKYNET SYSTEMS

INTPIRE

Madurez de los Sistemas

MADUREZ DE LOS SISTEMAS



Basada en clasificación del ENS

DarkNet Systems · Skynet Systems · Intpire

SKYNET SYSTEMS

INTPIRE

DARKNET systems

968 67 92 90

910 60 31 23

OFICINA Acelera pyme

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

Fondos Europeos

Financiado por la Unión Europea

Fondo Europeo de Desarrollo Regional

"Europa se siente"