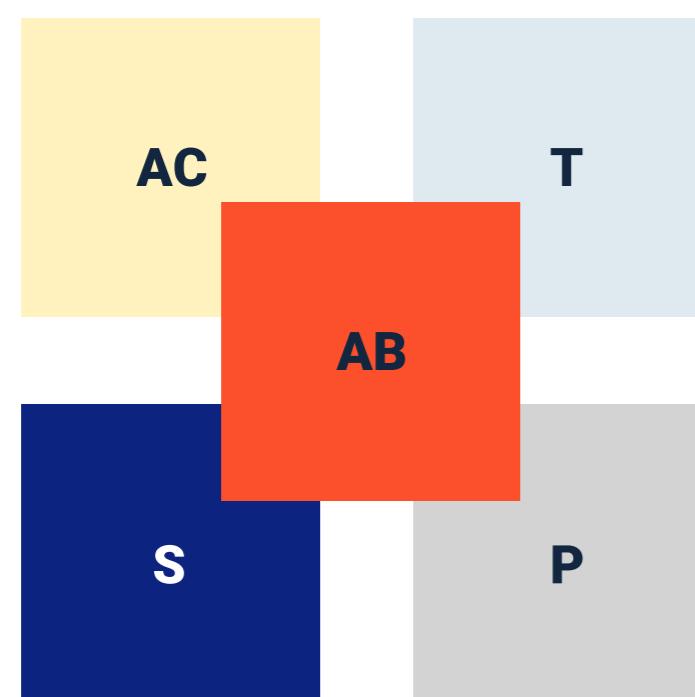


Ciberseguridad y documentación de incidentes

Las empresas pueden verse expuestas a eventos e incidentes de seguridad que arriesgan los activos digitales, una forma de minimizar estos riesgos, es mediante buenas prácticas organizacionales, que conlleve a la creación de estándares y modelos de referencia que permitan documentar procesos dentro del sistema de gestión de seguridad de la información, realizar auditorías y trazabilidad de seguridad informática.

[Iniciar >](#)

	PRIMARIO #D3D3D3		ACENTO CONTENIDO #FFF2BF		CB
	SECUNDARIO #0D2380		ACENTO BOTONES #FC502D		
	NEUTRAL 1 #EFEFEF		NEUTRAL 2 #F9F7EC		



Introducción



Estimado Aprendiz, bienvenido a este componente formativo que presenta los requerimientos asociados a la documentación de incidentes en la ciberseguridad, necesaria para registrar las operaciones de redes de datos y obtener la información para generar informes y reportes de operación en relación con las herramientas de protección y minimizar riesgos a los que puede verse expuesta la información.

Con diferentes contenidos audiovisuales puede apropiarse de la valiosa información que está aquí dispuesta, como parte del proceso de aprendizaje que adelanta y para continuar con los demás temas de estudio venideros.

Le invitamos a explorar el contenido y estudie a detalle todos los temas y al final realice la actividad de repaso.



VIDEO

1 Documentación de incidentes en la Ciberseguridad

Los procesos que permiten gestionar y dar tratamiento a los incidentes de la ciberseguridad se rigen bajo la familia de las normas ISO/IEC 27000. Estas normas describen lineamientos para el seguimiento de eventos, incidentes y acciones que lleguen a impactar en el desempeño de los sistemas de seguridad de la información en las empresas.

En Colombia, está contemplado dentro del marco de gobierno digital el Modelo de Seguridad y Privacidad de la Información – MSPI. Este modelo está basado en un ciclo de operación que incluye 5 fases:

- ✓ Diagnóstico
- ✓ Planificación
- ✓ Implementación
- ✓ Evaluación de desempeño
- ✓ Mejora continua

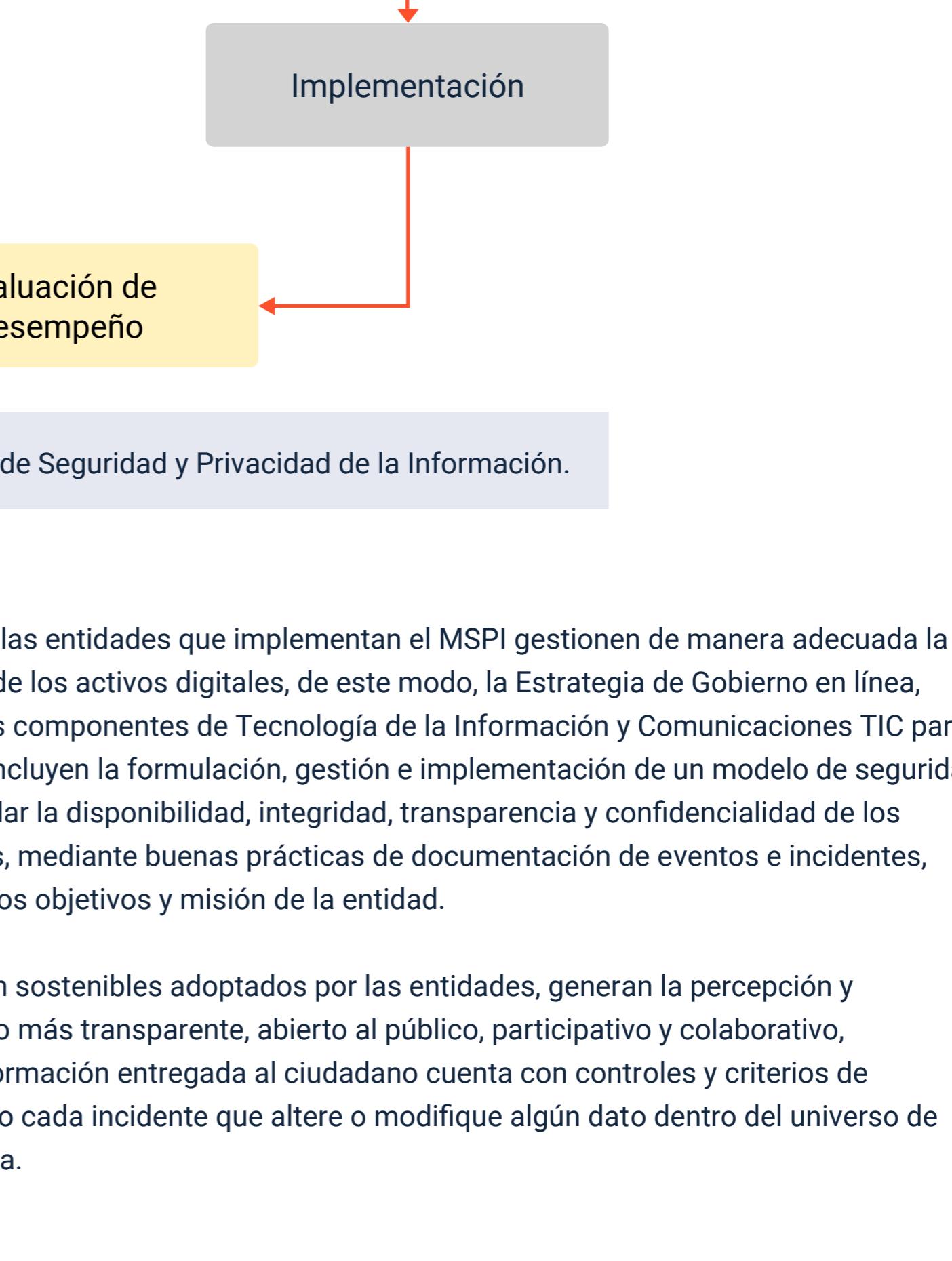
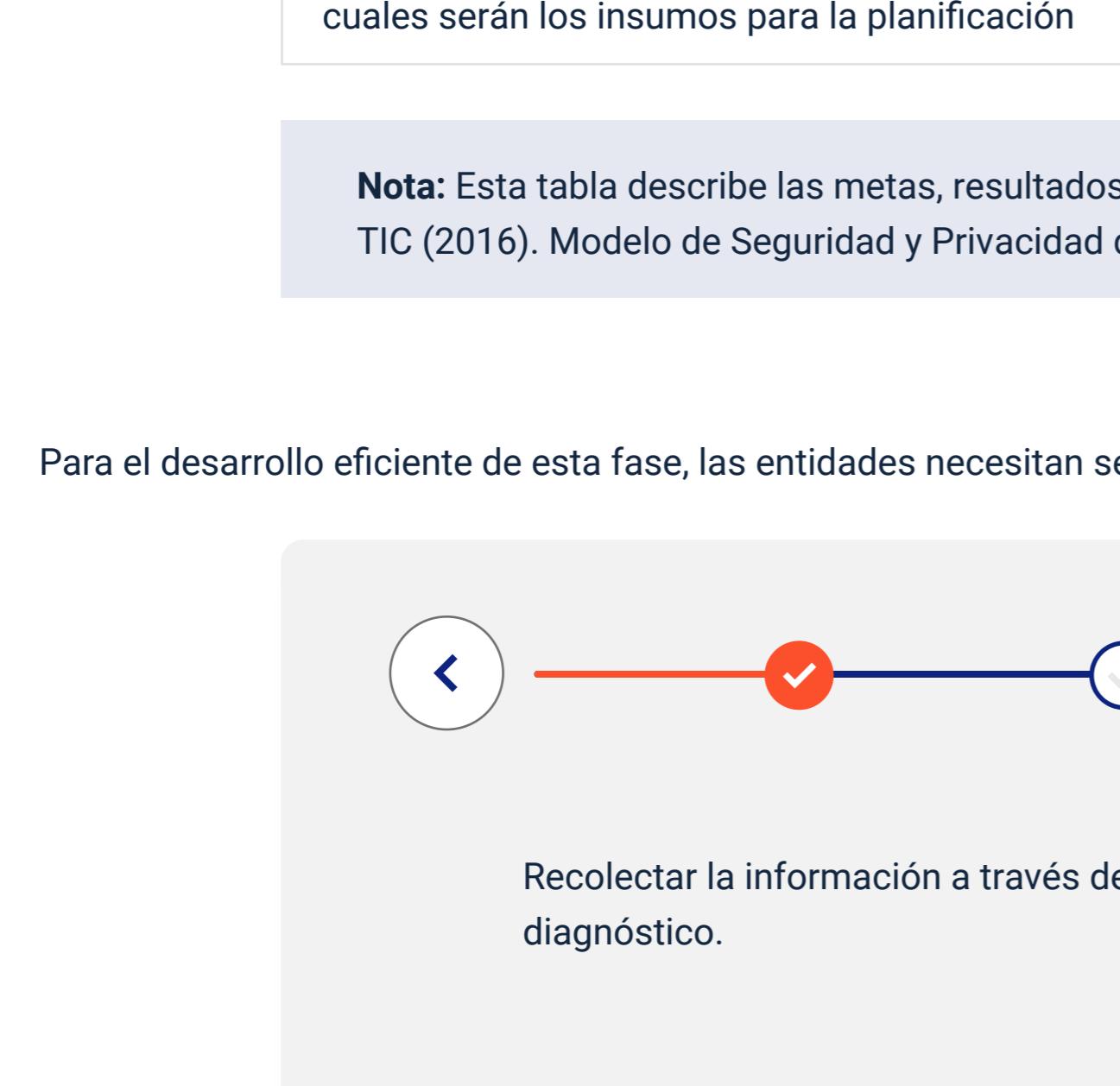


Figura 1 Ciclo de operación del Modelo de Seguridad y Privacidad de la Información



Nota: tomada y adaptada de Ministerio de las TIC (2016). Modelo de Seguridad y Privacidad de la Información.



Estas fases, logran que las entidades que implementan el MSPI gestionen de manera adecuada la seguridad y privacidad de los activos digitales, de este modo, la Estrategia de Gobierno en línea, permite centrarse en los componentes de Tecnología de la Información y Comunicaciones TIC para gestionar aportes que incluyen la formulación, gestión e implementación de un modelo de seguridad enfocado en salvaguardar la disponibilidad, integridad, transparencia y confidencialidad de los activos y datos digitales, mediante buenas prácticas de documentación de eventos e incidentes, dando cumplimiento a los objetivos y misión de la entidad.

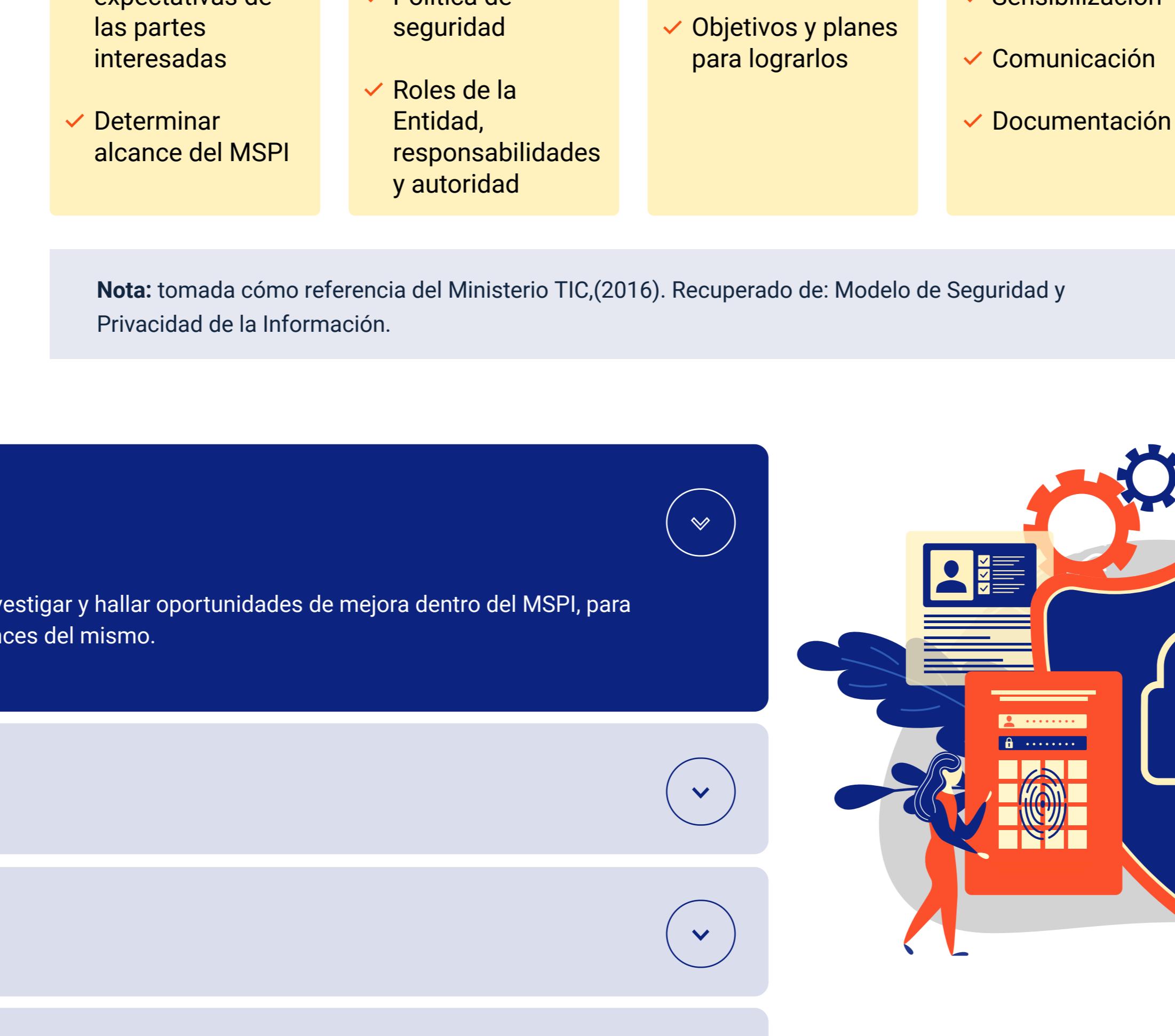
Los sistemas de gestión sostenibles adoptados por las entidades, generan la percepción y aceptación de un estado más transparente, abierto al público, participativo y colaborativo, garantizando que la información entregada al ciudadano cuenta con controles y criterios de seguridad, documentado cada incidente que altere o modifique algún dato dentro del universo de información almacenada.

1.1 Informes de operación de red de datos

De acuerdo a las etapas del MSPI en su fase de diagnóstico se identifica la operatividad de la red de datos según procedimientos técnicos y marcos de referencia; Es así que se describe el estado de la entidad, el nivel de madurez y el levantamiento de información, teniendo en cuenta los requerimientos, metas y resultados.

En esta etapa, al generar los informes de operación de la red de datos, se debe describir las metas, los resultados e instrumentos utilizados, tal como se describe en la siguiente en la figura 2 y la tabla 1:

Figura 2 Fase de diagnóstico MSPI.



Nota: tomada y adaptada de Ministerio TIC (2016). Modelo de Seguridad y Privacidad de la Información.

Tabla 1 Fase de diagnóstico

Metas	Resultado	INSTRUMENTOS MSPI
Establecer el estado actual de la entidad en la gestión de seguridad y privacidad de la información – SPI	Herramienta diligenciada y documentada	Herramienta de diagnóstico
Identificar el nivel de madurez de SPI en la Entidad	Herramienta diligenciada y nivel de madurez identificado	Herramienta de diagnóstico
Identificar vulnerabilidades técnicas y administrativas, las cuales serán los insumos para la planificación	Informe con los hallazgos obtenidos de las pruebas de vulnerabilidad	Herramienta de diagnóstico

Nota: Esta tabla describe las metas, resultados y instrumentos de la fase de diagnóstico del MSPI. Tomada y adaptada de Ministerio TIC (2016). Modelo de Seguridad y Privacidad de la Información.

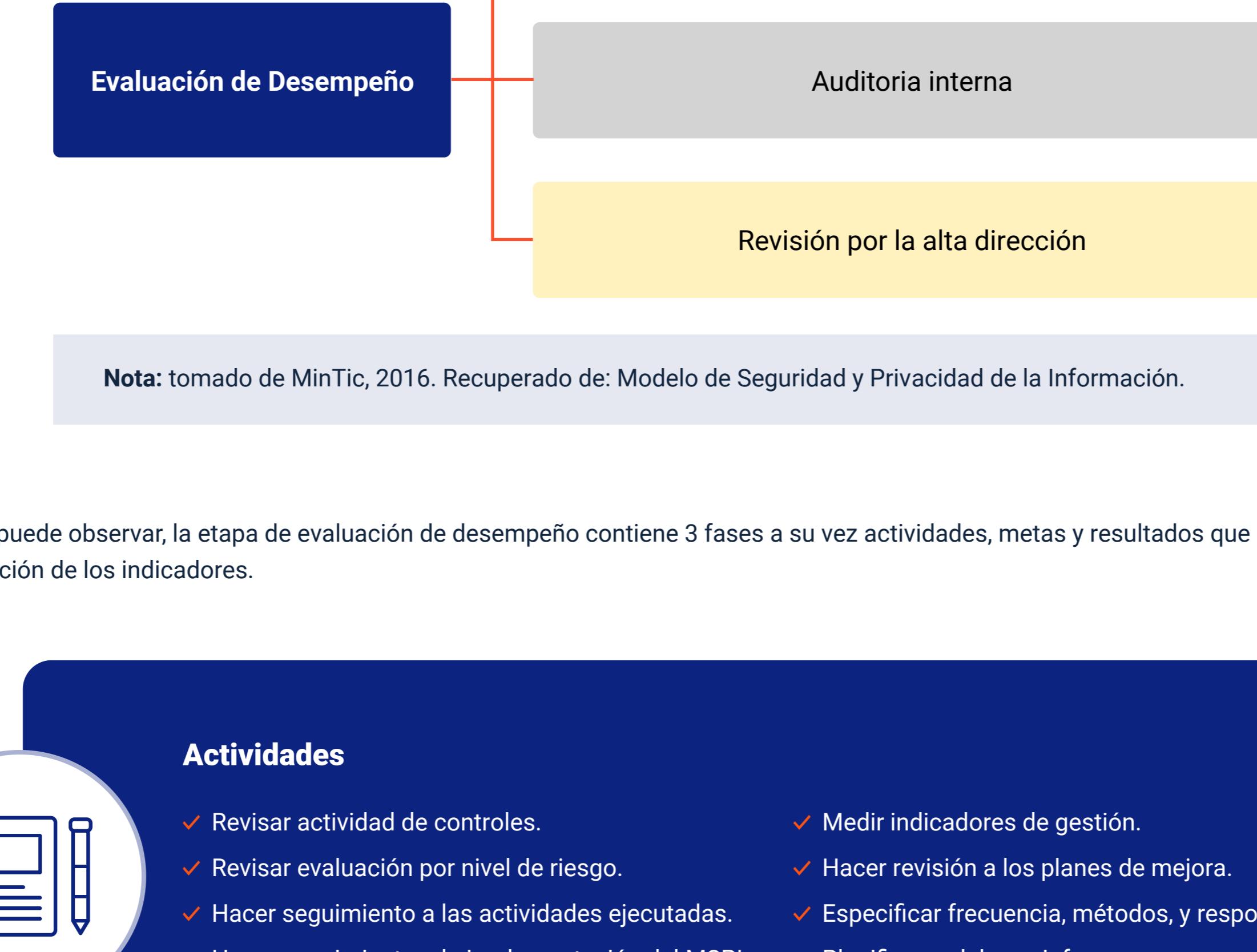
Para el desarrollo eficiente de esta fase, las entidades necesitan seguir estos pasos:



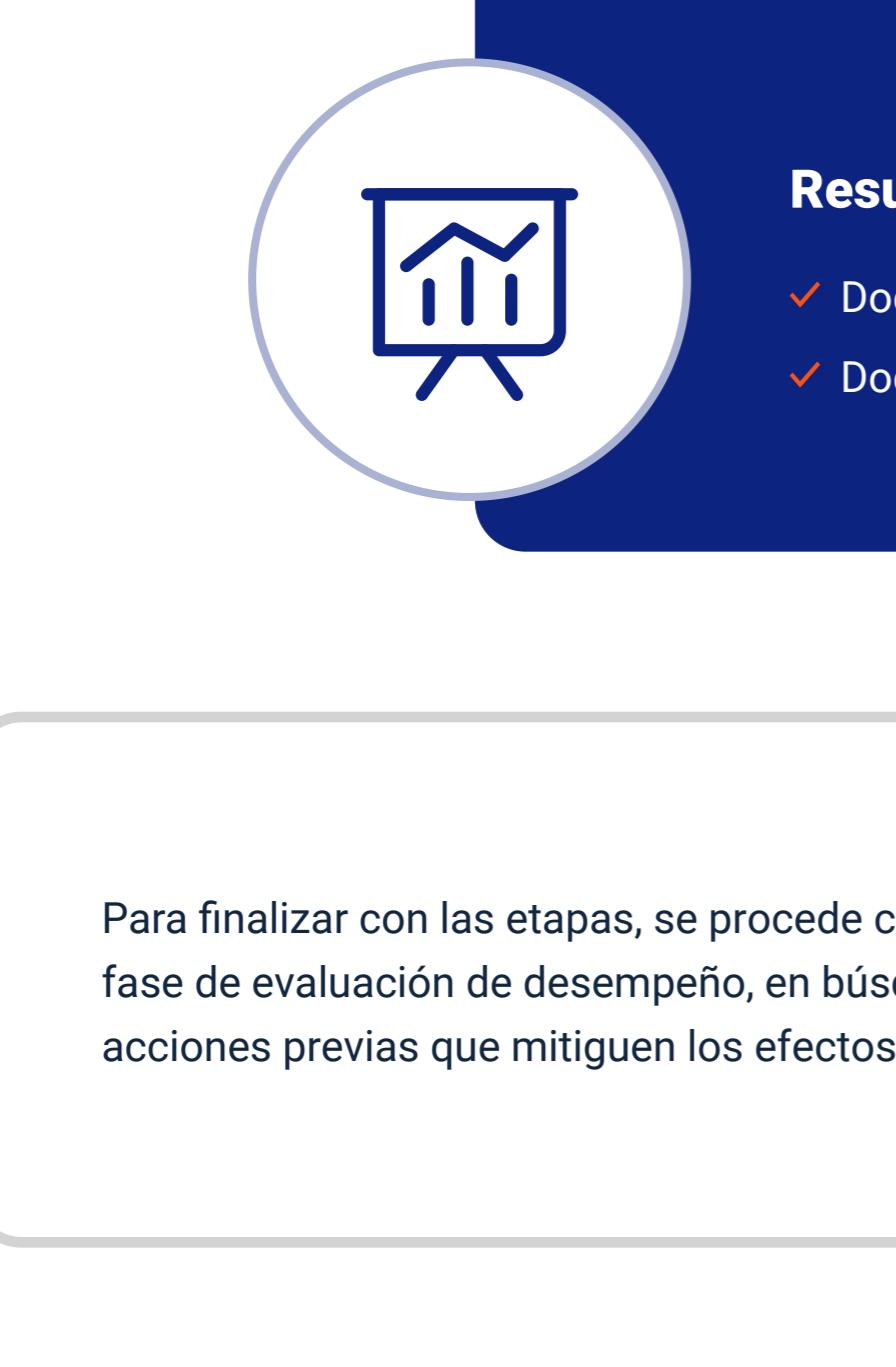
A continuación, se detalla el proceso de la etapa de planificación y las partes que debe contener un informe de gestión, junto con sus metas, resultados e instrumentos para el MSPI en una entidad.

Como se puede observar, la fase de planificación contiene 4 subprocessos: Contexto, liderazgo, planeación y soporte.

Figura 3 Fase de planificación MSPI



Nota: tomada como referencia del Ministerio TIC,(2016). Recuperado de: Modelo de Seguridad y Privacidad de la Información.



Control y planeación operacional:

La entidad planifica, implementa y controla todos los procesos indispensables que permitan cumplir con todas las condiciones necesarias de SPI. Es indispensable, que toda esta información sea documentada para llevar un control de acciones en búsqueda de la mitigación de riesgos que puedan presentarse.

Plan de tratamiento de riesgos de SPI:

Definición de indicadores de gestión:

Para otro lado, es importante definir las actividades a realizar para la migración de los protocolos IPv4 a IPv6, cabe recordar que las IPv son las conexiones de internet, siendo la IPv4 más antigua y vulnerable, a partir del 2020 se migró a la IPv6. En esta fase se realizan actividades de direccionamiento, diseño, montaje, ejecución y corrección de pruebas, activación de políticas de SPI, validación de funcionalidad, a continuación, se describen metas, entregables e instrumentos para la migración de IPv4 a IPv6.

Tabla 2 Migración IPv4-IPv6

Metas	Resultado	INSTRUMENTOS MSPI
Implementar la estrategia de migración IPv4 a IPv6.	Informe para implementar la estrategia de migración de IPv4 a IPv6	Guía Transición de IPv4 a IPv6 para Colombia

Nota: Esta tabla describe las metas, resultados e instrumentos de la migración de IPv4 a IPv6.

1.2 Documentación de implementación

En este ítem se aborda la etapa de implementación del MSPI, donde se logrará llevar a cabo la implementación de lo planificado en los informes de operación de red de datos. Esta etapa contiene 3 subprocessos como son: Control y planeación operacional, plan de tratamiento de riesgos de seguridad y privacidad de la información, y la definición de indicadores de gestión.

Figura 4 Fase de implementación MSPI

Nota: tomado de MinTic, 2016. Recuperado de: Modelo de Seguridad y Privacidad de la Información.

Como se puede observar, la etapa de implementación contiene 3 fases a su vez actividades, metas y resultados que permite la consolidación de los indicadores.

Tabla 3 Mejoramiento continuo

Metas	Resultado	INSTRUMENTOS MSPI
Realizar el plan de mejora. Analizar los resultados del seguimiento. Analizar los resultados de las auditorías.	Informe con plan de mejora. Informe con plan de divulgación	Guía de mejora continua

Nota: Esta tabla describe las metas, resultados e instrumentos de la fase de mejoramiento continuo.

1.3 Informes de operación de herramientas de protección

Existen herramientas de protección que permiten la operación continua de la entidad, es indispensable documentar cada etapa del proceso y generar informes, este aspecto hace parte del MSPI en las etapas de evaluación de desempeño y mejora continua.

En la etapa de evaluación de desempeño se realiza el seguimiento al MSPI, de acuerdo a los resultados obtenidos en la etapa de implementación. Este proceso permite verificar la eficiencia de todas las acciones que se implementan.

Figura 5 Fase de evaluación de desempeño MSPI

Nota: tomado de MinTic, 2016. Recuperado de: Modelo de Seguridad y Privacidad de la Información.

Como se puede observar, la etapa de evaluación de desempeño contiene 3 fases a su vez actividades, metas y resultados que permite la consolidación de los indicadores.

Tabla 4 Fase de mejoramiento continuo

Metas	Resultado	INSTRUMENTOS MSPI
Realizar el plan de mejora. Analizar los resultados del seguimiento. Analizar los resultados de las auditorías.	Informe con plan de mejora. Informe con plan de divulgación	Guía de mejora continua

Nota: Esta tabla describe las metas, resultados e instrumentos de la fase de mejoramiento continuo.

Como se puede observar, la etapa de mejoramiento continuo consta de 2 fases que son: Acciones correctivas y mejora continua; cada una de estas fases contiene metas, resultados e instrumentos.

Tabla 5 Fase de mejoramiento continuo

Metas	Resultado	INSTRUMENTOS MSPI
Realizar el plan de mejora. Analizar los resultados del seguimiento. Analizar los resultados de las auditorías.	Informe con plan de mejora. Informe con plan de divulgación	Guía de mejora continua

Nota: Esta tabla describe las metas, resultados e instrumentos de la fase de mejoramiento continuo.

2 Reportes de incidente de la ciberseguridad

Los reportes de incidentes permiten identificar, evaluar, y responder a eventos del sistema de información. Éstos manejan un nivel de madurez que busca establecer criterios de valoración y determina el estado de la SI en las entidades. Existen 6 niveles de madurez y abarca desde la inexistencia hasta la optimización.

Figura 7
Nivel de madurez

Nivel 0 - Inexistente
Desconoce o no tiene en cuenta el tema de seguridad de la información
Nivel 1 - Inicial
Reconoce que tiene problemas de seguridad y que estos necesitan ser resueltos
Nivel 2 - Repetible
Tiene procedimientos no formales de seguridad
Nivel 3 - Definido
En este nivel se realizan las fases de diagnóstico, planificación e implementación
Nivel 4 - Administrativo
Ha realizado las fases de evaluación de desempeño y mejora continua
Nivel 5 - Optimizado
Encuentra en la seguridad de la información, un valor agregado para la Entidad

Nota: tomado de MinTic, (2016). Recuperado de: Modelo de Seguridad y Privacidad de la Información.

Inexistencia

- ✓ No se implementa control de infraestructura de TI, física, y recursos humanos.
- ✓ No se reconoce la información como un activo digital sensible e importante.

Inicio

Repetición

Definición

Administración

Optimización

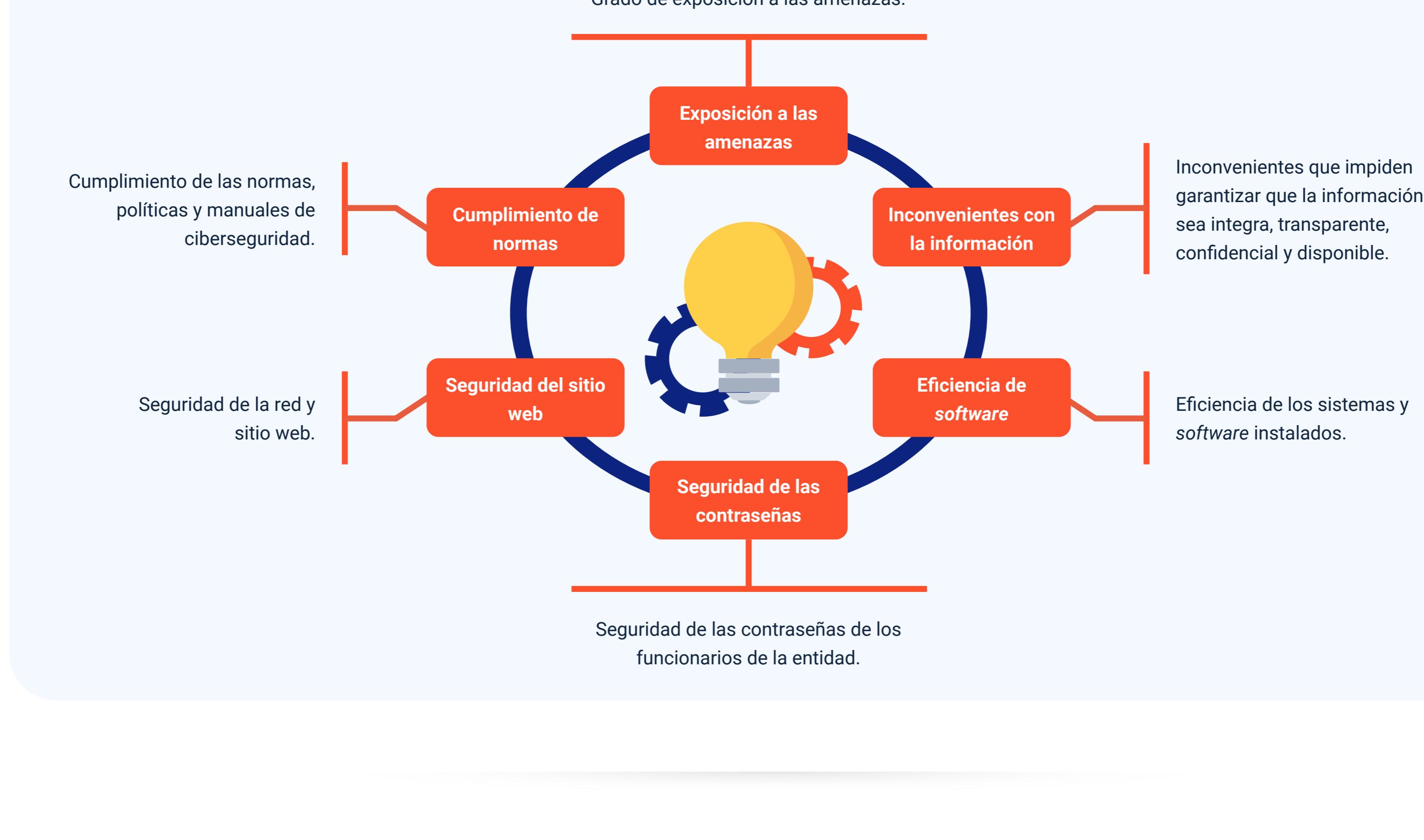
2.1 Auditorías



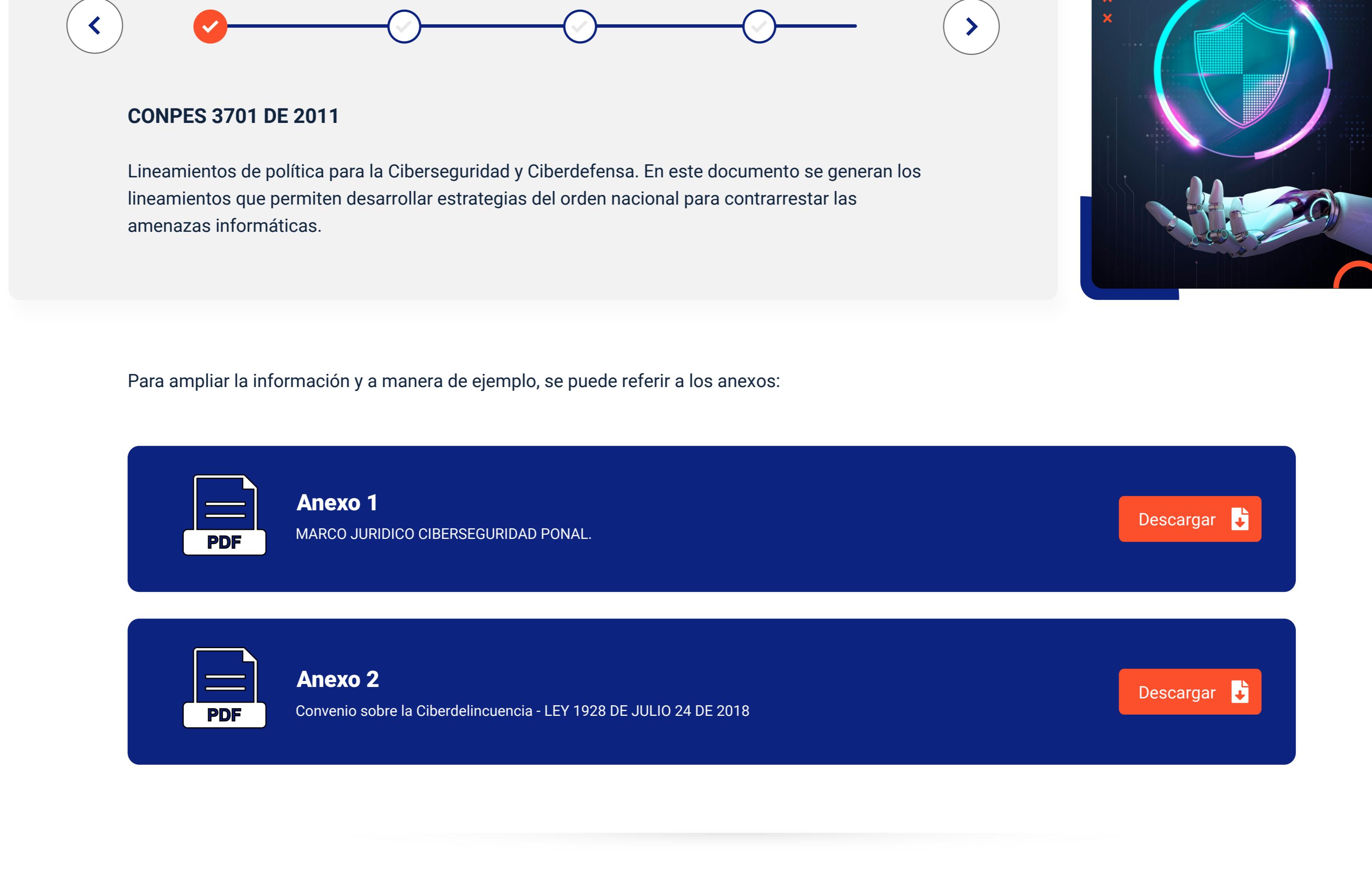
En muchas oportunidades no se aprecia el alto grado de exposición a vulnerabilidades en ciberseguridad que enfrentan las entidades día tras día, es por ello, que lo más idóneo es realizar una auditoría. Estas acciones que van enmarcadas a través de buenas prácticas normalizadas por ISO 27000, permite detectar, enlistar y documentar aquellas incidencias y vulnerabilidades en la infraestructura TIC de la entidad. Los objetivos de las auditorías son:

- ✓ Analizar situación actual de la entidad y rendimiento de la productividad.
- ✓ Realizar una propuesta de seguridad física perimetral.
- ✓ Analizar y planea la mejora técnica de la red interna.
- ✓ Analizar el hardware, software, y comunicaciones que ayude a generar las políticas de actualización y vulnerabilidades de la entidad.
- ✓ Enlistar las recomendaciones de mejora continua y buenas prácticas en la configuración y acceso al hardware.
- ✓ Realizar pruebas de huella externa (Fase External Footprinting - FEF).
- ✓ Realizar pruebas de ficheros remotos RFI.
- ✓ Probar los servidores, firewall y PC's, mediante escáner y pruebas manuales de autenticación.
- ✓ Analizar red inalámbrica (Wireless) con el fin de saber, que operación realiza una persona que acceda a esta red.
- ✓ Realizar un documento que describa las medidas a implementar y las acciones preventivas de mantenimiento en hardware y software.

El objetivo de las auditorías no es el de realizar actividades puntuales, sino acciones continuas que logran disminuir, minimizar y bloquear las amenazas latentes que están en continua transformación. De este modo, la entidad estaría preparada para actuar o prevenir consecuencias que se puedan presentar y así mejorar continuamente la seguridad y privacidad de los datos. Entre los tipos de auditorías más populares encontramos:



Sin importar el tamaño de la entidad, todas requieren de auditorías de ciberseguridad; Mantener operativa y segura la infraestructura tecnológica, genera confianza en los usuarios y elevan los niveles de calidad y productividad al interior de ésta. A continuación, de presentan las acciones que no pueden faltar en las auditorías de ciberseguridad:



En conclusión, una auditoría en ciberseguridad sirve para tener conocimiento e identificar algunos factores al interior de la entidad, tales como:



2.2 Marco Jurídico y Marco Legal

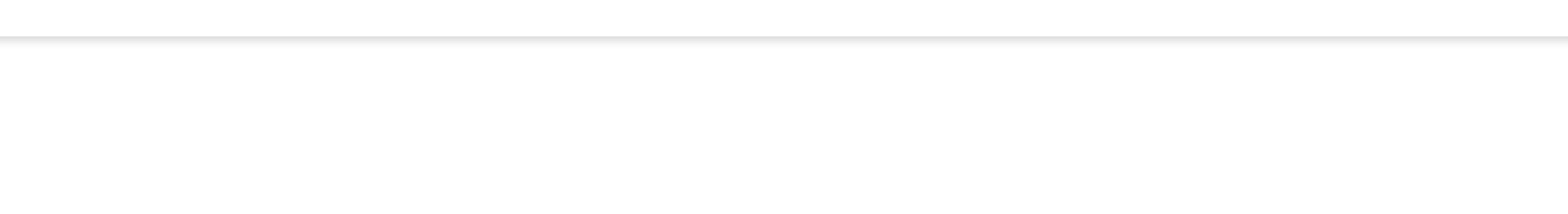
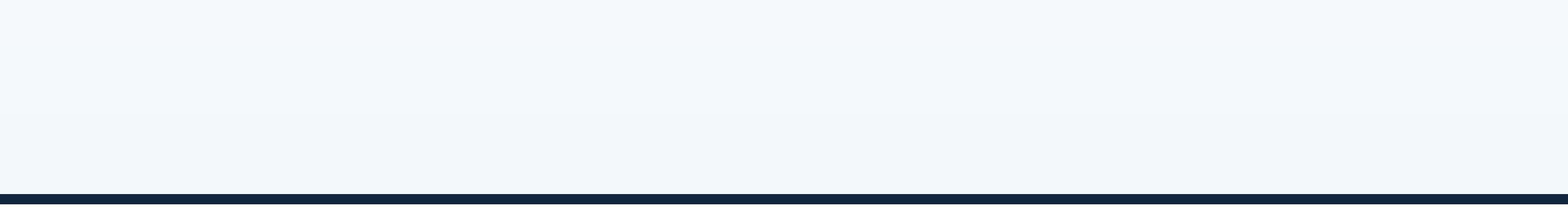
En la actualidad, existen diversos instrumentos Normativos de Ciberseguridad, con los cuales, el gobierno busca regular y controlar los ciberataques y los cibercriminales; Entre los decretos, leyes y artículos se destacan:



Lineamientos de política para la Ciberseguridad y Ciberdefensa. En este documento se generan los lineamientos que permiten desarrollar estrategias del orden nacional para contrarrestar las amenazas informáticas.



Para ampliar la información y a manera de ejemplo, se puede referir a los anexos:



2.3 Herramientas de gestión y manual de funcionamiento

Para que los sistemas no sufran consecuencias tras los ataques de ciberseguridad, es importante contar con herramientas de protección y, además, que los encargados de éstas cuenten con las habilidades y conocimientos para su óptimo funcionamiento:

Software antivirus, Firewall, Proxy, PKI - Public Key Infrastructure, MDR - Managed Detection and Response, y Pentesting.

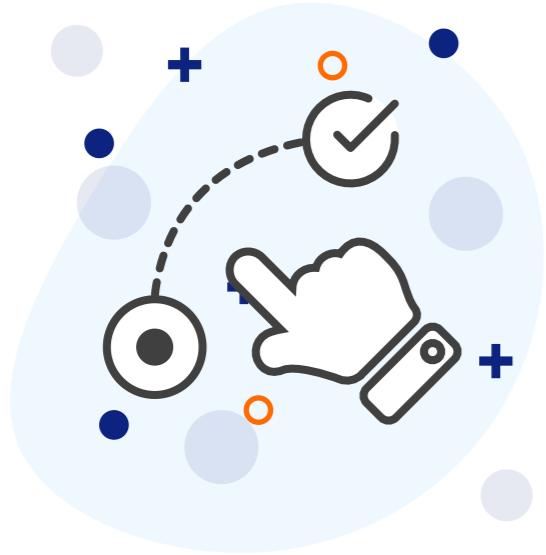
Para conocer la herramienta y su manual de funcionamiento, se puede remitir a <https://latam.kaspersky.com/antivirus>

VIDEO



Actividad didáctica

Arrastrar y soltar



Llegó el momento de validar los aprendizajes adquiridos con el estudio del componente formativo. Por favor relacionar cada término con la definición, arrastrando y soltando donde corresponda.

Arrastrar y soltar

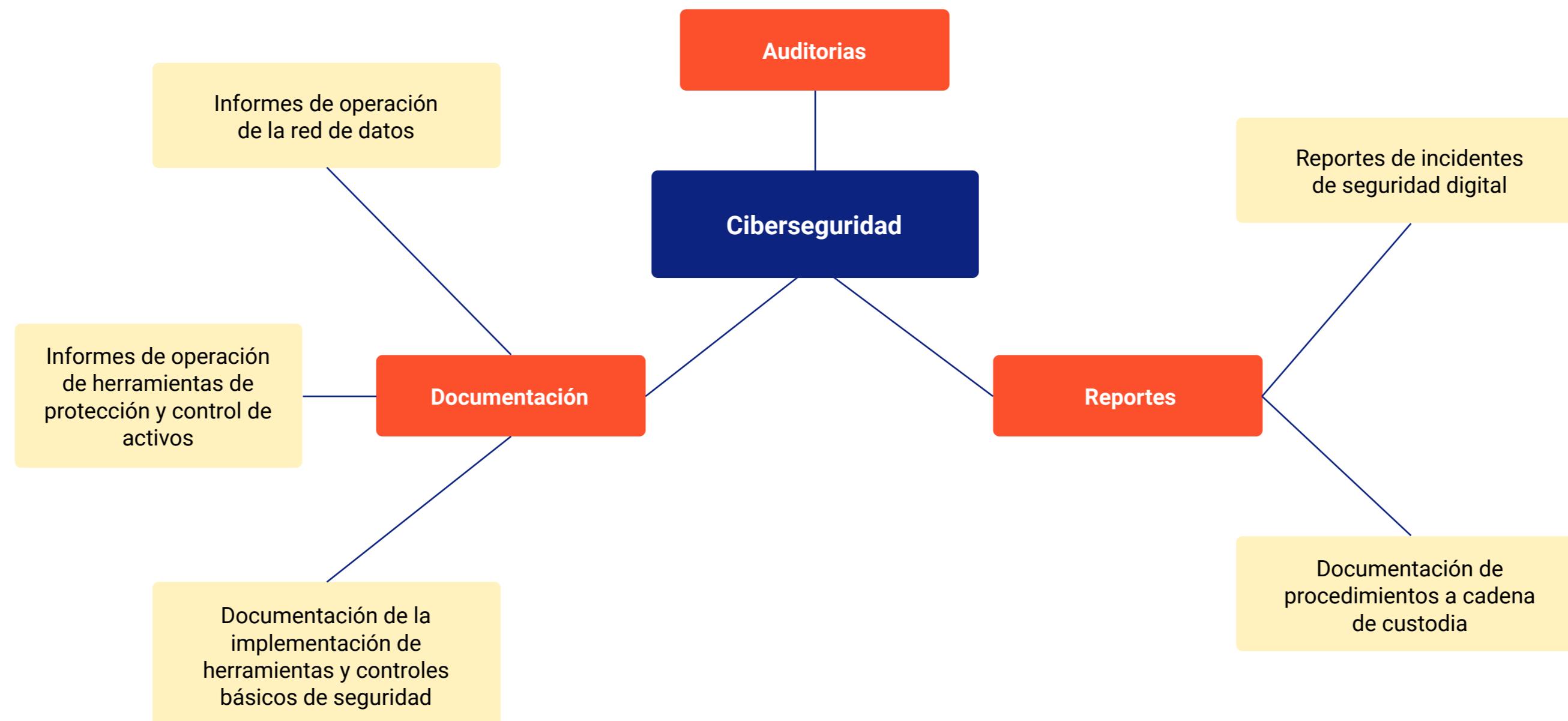
Realizar 

Control de la seguridad digital

Síntesis: Ciberseguridad y documentación de incidentes



En el siguiente diagrama encontrará un resumen de conceptos y palabras claves de los temas abordados en este contenido formativo.





Portada actividad

800 x 800



Portada actividad

800 x 800



Imagen acompañamiento Actividad

600 x 600



Imagen Resultado

900 x 600