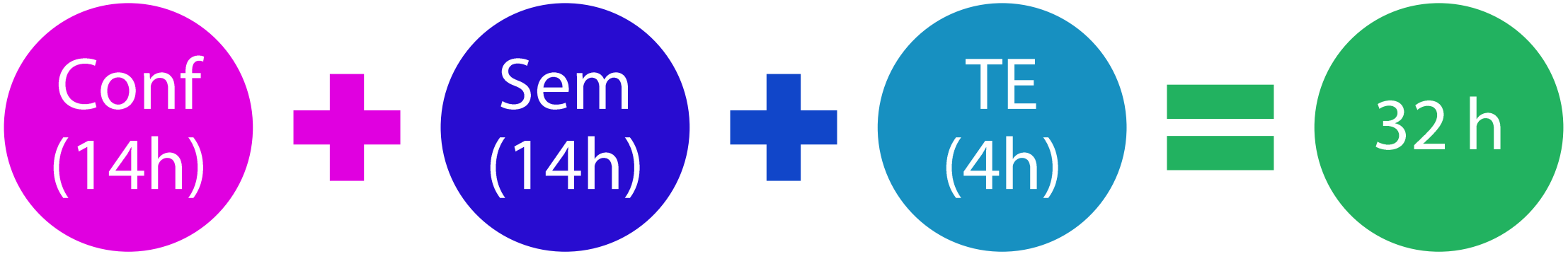
Universidad de las Ciencias Informáticas

Práctica Profesional

Gestión de la Ciberseguridad

2024

Organización de la asignatura



Tema 1

- Describir los estándares y metodologías para la gestión de la ciberseguridad
- Explicar el proceso de planificación del SGSI
- Caracterización del sistema informático.
- Identificación de las amenazas

Tema 2

- Caracterización de metodologías para la gestión de riesgos
- Estimación de riesgos
- Selección de controles de seguridad informática
- Diseño de Políticas de Seguridad Informática
- Elaboración de planes de seguridad informática
- Medición y evaluación de indicadores de seguridad informática

Objetivo del año

- **Diseñar** un **sistema de ciberseguridad** mediante la realización de **análisis de riesgos**, la **aplicación de controles técnicos de seguridad**, el uso de técnicas para el desarrollo seguro de software y la evaluación de vulnerabilidades; todo ello sustentado en el uso de técnicas de inteligencia artificial como apoyo a la toma de decisiones y utilizando criterios eficientes para racionalizar los procesos y recursos.

Universidad de las Ciencias Informáticas

Práctica Profesional

Gestión de la Ciberseguridad

Tema 1: Introducción a la gestión de la ciberseguridad

A1C1: "Fundamentos de la gestión de la ciberseguridad"

Ing. Victor Alejandro Roque Dominguez

varoque@uci.cu

2024

Objetivo

- Caracterizar la gestión de la ciberseguridad atendiendo a las bases conceptuales, alcance, dominios y metodologías para comprender su enfoque sistémico e incremental que impacta en la materialización de la seguridad de la información.

Bibliografía consultada

[1] ISO 27032:2015 Information technology — Security techniques — Guidelines for cybersecurity

[2] Decreto 360 de 2019 de Consejo de Ministros, (2019). https://www.gacetaoficial.gob.cu/es/decreto-360-de-2019-de-consejo-de-ministros

[3] NC ISO 27000:2023 Information technology — Security techniques — Information security management systems — Overview and vocabulary

¿Qué es el ciberespacio?

" … es el ambiente virtual y dinámico, definido por tecnologías, equipos, procesos y sistemas de información, control y comunicaciones, que interactúan entre sí y con las personas, y en el que la información se crea, procesa, almacena y transmite".

Artículo 4, Decreto 360 de 2019 de Consejo de Ministros, (2019).

¿Qué es el ciberespacio?

"Es el entorno resultante de la interacción de **personas, software y servicios en Internet**, el cuál está **respaldado por las tecnologías de la información y las comunicaciones"** [1].

En este entorno, como en otros, existe gran cantidad de amenazas.

Componentes del ciberespacio

Partes interesadas

- Entes que interactúan en el ciberespacio

Activos

- Componentes que tienen valor para una de las Partes interesadas

Clasificación de las **Partes Interesadas**

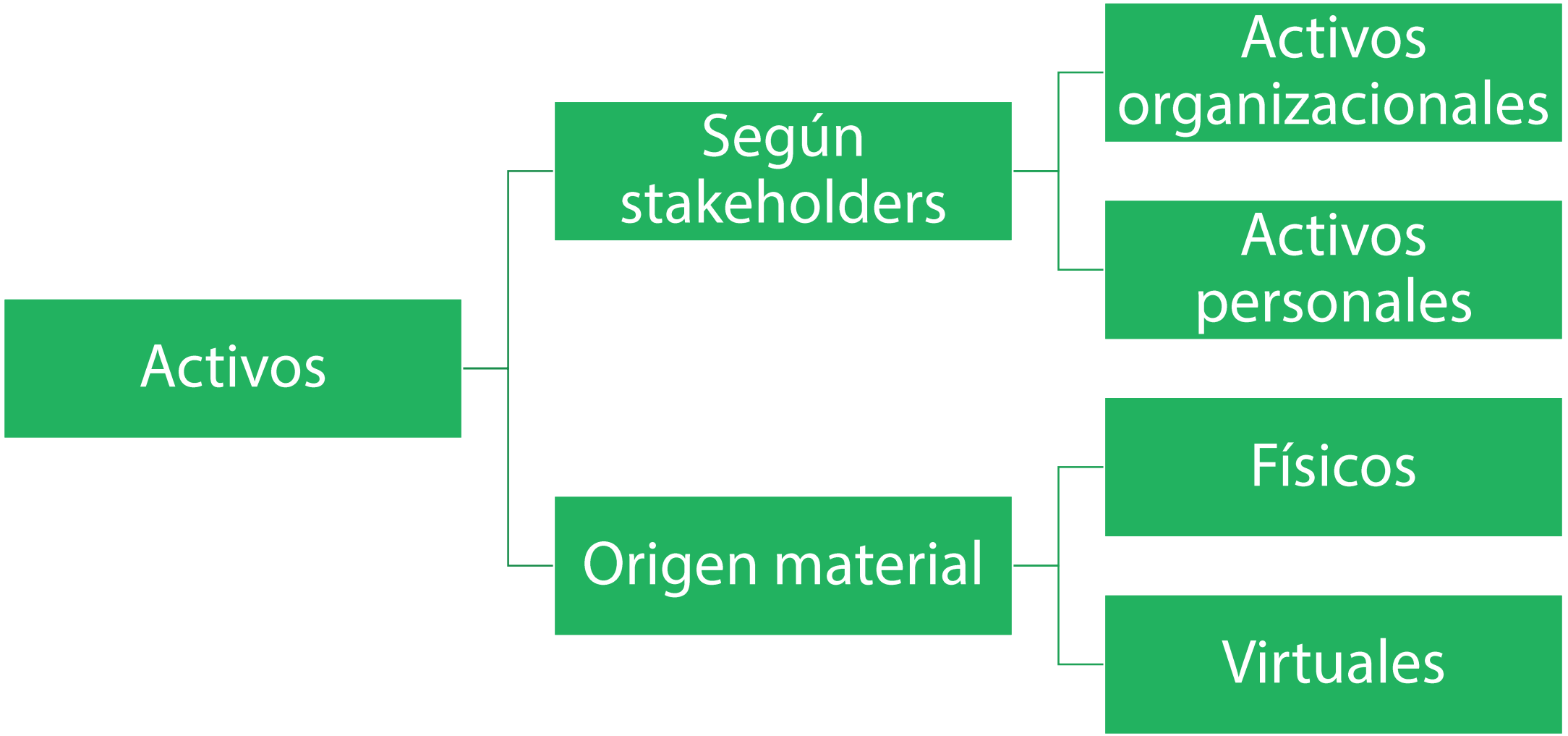
Consumidores

- Hacen uso de servicios dispuestos en el ciberespacio. Ej: personas naturales y personas jurídicas.

Proveedores

- Ponen a disposición servicios para ser utilizados por los consumidores, como servicios de conectividad y de acceso.

Clasificación de los **Activos**



Conceptos asociados. Decreto 360

Artículo 6. La situación o acontecimiento que puede causar daños a los bienes informáticos, sea una persona, un programa maligno o un suceso natural o de otra índole y representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema se denomina **amenaza**.

Artículo 7. Se denomina **ataque** al intento de acceso o acceso a un sistema o una red informática o terminal mediante la explotación de vulnerabilidades existentes en su seguridad.

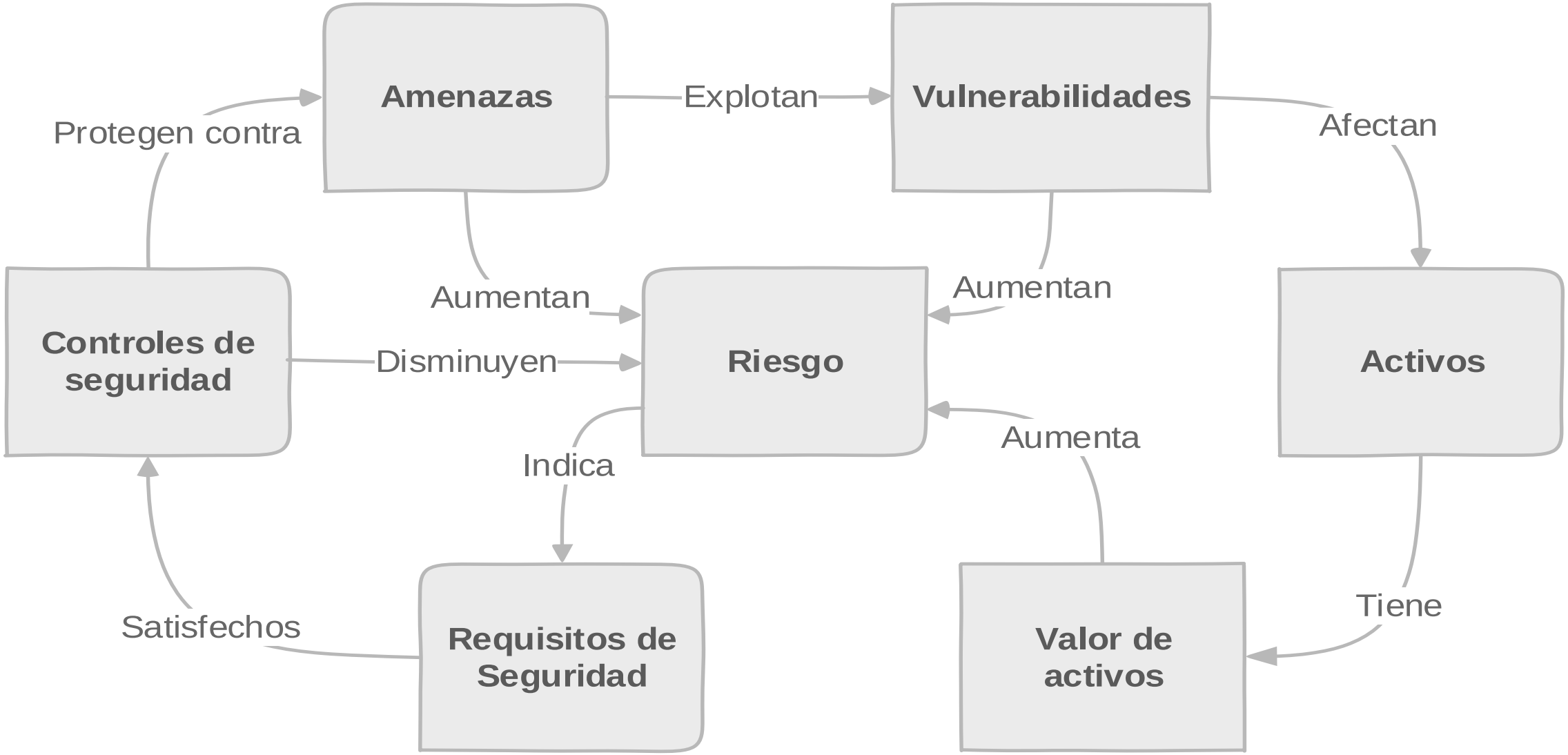
Conceptos asociados. Decreto 360

Artículo 8. Se identifica como **riesgo** a la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático y cause un impacto negativo en la organización.

Artículo 9. La **vulnerabilidad** se identifica como el punto o aspecto del sistema que muestra debilidad al ser atacado o que puede ser dañada su seguridad; representa los aspectos falibles o atacables en el sistema informático y califica el nivel de riesgo de un sistema.

Relación entre los conceptos

Relación entre los conceptos



Ciberseguridad

- **Artículo 5.** La Ciberseguridad es el estado que se alcanza mediante la aplicación de un sistema de medidas (organizativas, normativas, técnicas, educativas, políticas y diplomáticas), destinado a garantizar la protección y el uso legal del ciberespacio.
- En la protección del ciberespacio se incluye la reducción de riesgos y vulnerabilidades, la creación de capacidades para detectar y gestionar eventos e incidentes y el fortalecimiento de la resiliencia.

Seguridad de las TIC

- **Artículo 12.** La Seguridad de las TIC es el conjunto de medidas administrativas, organizativas, físicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las TIC; el empleo del término seguridad informática, tiene igual significado.

Incidente de seguridad

- **Artículo 16.** Se considera un incidente de seguridad cualquier evento que se produzca de forma accidental o intencional, que afecte o ponga en peligro las tecnologías de la información y la comunicación o los procesos que con ellas se realizan.

1

Gestión de la Ciberseguridad. ISO 27032

Sistema de gestión. ISO 27000

Conjunto de elementos interrelacionados o interactuantes de una *organización* (3.50) para establecer *políticas* (3.53), *objetivos* (3.49), así como los *procesos* (3.54) para lograrlos.

- Nota 1 a la entrada: Un sistema de gestión puede abordar una sola disciplina o varias.
- Nota 2 a la entrada: Los elementos del sistema incluyen la estructura, las funciones y responsabilidades, la planificación y la operación de la *organización* (3.50).
- Nota 3 a la entrada: El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones y secciones específicas e identificadas de la misma, o una o más funciones a través de un grupo de organizaciones.

Norma ISO 27001

Contexto de la organización

Liderazgo

Planificación

Soporte

Operación

Evaluación del desempeño

Mejora

Modelo para implementar un SGSI

El objetivo principal de esta fase es establecer el Sistema de Gestión de Seguridad de la Información. Concretamente, se establecerán en este paso los **objetivos, procedimientos y políticas relacionadas con la Seguridad de la Información**, y con la visión puesta en mejorar esta última.

Modelo para implementar un SGSI

Se implementará en este punto el SGSI establecido. Se llevarán a cabo los procedimientos establecidos en la anterior fase y se **implantarán los controles y operaciones necesarios** con el fin de gestionar la información de la organización de una manera segura y eficaz.

Modelo para implementar un SGSI

En esta fase que corresponde a la letra "C" del ciclo PDCA se evaluará y revisará la efectividad del Sistema de Gestión de Seguridad de la Información planificado e implantado en anteriores fases. Para ello, se comprobará que se cumplen aspectos tales como la **política de seguridad**, los objetivos o los diferentes procedimientos implementados.

Modelo para implementar un SGSI

En esta última fase del ciclo se mantendrá y mejorará el SGSI. Es decir, se llevarán a cabo a**cciones y planes tanto correctivos como preventivos** para mejorar los resultados obtenidos e implementar y conseguir así una mejora continua del Sistema de Gestión de la Seguridad de la Información.

Dominios de trabajo. ISO 27032

Proceso descrito en la ISO 27032 para un proyecto de CS

Fase I: Entendimiento de la Organización

En esta primera fase se realiza un trabajo importante de inmersión en los procesos de la empresa para conocer el funcionamiento de éstos y que uso realizan del Ciberespacio sus servicios. Para llevar a cabo esta tarea será necesario:

- Revisar productos y servicios
- Revisar el marco normativo de seguridad en uso
- Recopilar y revisar documentación de seguridad
- Conocer los flujos de información en los procesos
- Conocer las medidas técnicas de seguridad implementadas, etc

Esta fase permitirá también disponer de un inventario de activos de los servicios en el alcance.

Fase II: Análisis de Riesgos

La toma de decisiones en cuanto a los controles y medidas de seguridad que se van a implementar debe estar basada en la gestión de los riesgos y el alineamiento con las necesidades de la empresa. Es por ello que, en esta fase, se llevará a cabo esta evaluación considerando, entre otros, aspectos como:

- Activos críticos
- Amenazas
- Vulnerabilidades
- Impacto y riesgo
- Responsabilidades

Esta tarea se lleva a cabo con alineamientos a normas reconocidas a nivel internacional, que permiten su mantenimiento y gestión en el tiempo.

Fase III: Plan de Acción

En esta fase, y gracias al trabajo realizado en las fases anteriores, se redactará el plan que permita conocer la priorización y medidas que deberán desarrollarse para la consecución de los alineamientos de la ISO/IEC 27032:2012 en base a las exigencias del negocio.

Este Plan afrontará diferentes estrategias que incluirán y deberán aplicarse a diferentes niveles de la organización, incluyendo:

- Políticas
- Identificación de roles
- Métodos de implementación
- Procesos afectados
- Controles tecnológicos

Fase IV: Implementación

- Como tal, esta es la etapa que más esfuerzos va a requerir habitualmente dado que es en la que todas las acciones definidas en la fase anterior se plasmarán en el Plan de Acción.
- Esta fase del proyecto se focalizará entonces en la implementación de controles que deberán tener en cuenta el nivel de madurez en la gestión de la seguridad existente y que considerará, entre otros, aspectos como:

Existencia de Política de Seguridad

Procedimientos de Seguridad en SDLC

Marcos existentes para el intercambio de información

Planes de concienciación del personal

Metodología de AARR

Monitorización TIC

Gestión de incidentes

Fase IV: Implementación

Además de esto, en esta fase del proyecto se establecerán controles adicionales que incluirán:

- Controles a nivel de aplicación: gestión de sesiones, validación de datos, protección ante ataques, procesos de autenticación, etc.
- Controles a nivel de servidores: configuraciones seguras, gestión de parches, monitorización., revisiones periódicas, etc.
- Controles para los usuarios finales: Actualizaciones de SO, uso de aplicaciones, antivirus, herramientas y configuraciones de seguridad, etc.
- Controles contra ataques de Ingeniería social: Programas de concienciación, pruebas regulares, controles de seguridad, etc.

ISO 27000 vs ISO 27034

Enfoque:

- **ISO 27001:** Gestión de la seguridad de la información en su totalidad.
- **ISO 27032:** Enfocado en la ciberseguridad y protección en el ámbito digital.

Aplicación:

- **ISO 27001:** Ideal para cualquier organización que maneje información, independientemente de su naturaleza digital o no.
- **ISO 27032:** Específica para entidades que operan principalmente en línea o tienen una fuerte presencia digital.

ISO 27000 vs ISO 27034

Estructura:

- **ISO 27001:** Se basa en la implementación y mantenimiento de un SGSI.
- **ISO 27032:** Se centra en la gestión de riesgos cibernéticos y la promoción de una cultura cibernética segura.

Certificación:

- **ISO 27001:** Las empresas pueden obtener una certificación que valida su compromiso y adhesión a la norma.
- **ISO 27032:** No ofrece una certificación per se, pero proporciona directrices valiosas para la ciberseguridad.

2

Marco regulatorio cubano

Leyes, decretos y resoluciones

- Decreto No. 360/2019 Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional.
- Resolución 128/2019 Reglamento de seguridad de las tecnologías de la información Y la comunicación.
- Resolución 129/2019 Metodología para la gestión de la seguridad informática
- Decreto-Ley 35/2021 “De las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y el uso del Espectro Radioeléctrico”
- Resolución 105/2021 “Reglamento sobre el Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad”

C

Conclusiones

Estudio Independiente

- Investigar sobre los roles dentro de la gestión de la ciberseguridad.
- Hacer un resumen de las habilidades blandas de los especialistas en ciberseguridad y cómo desarrollarlas.

Orientaciones para el seminario

- Estándares y Metodologías para la Gestión de la Ciberseguridad

ISO

NIST

Enfoque Ágil

COBIT 5

CIS

Técnicas de IA en la gestión de CS

ITIL

Universidad de las Ciencias Informáticas

Práctica Profesional

Gestión de la Ciberseguridad

Tema 1: Introducción a la gestión de la ciberseguridad

A1C1: “Fundamentos de la gestión de la ciberseguridad”

Ing. Victor Alejandro Roque Dominguez

varoque@uci.cu

2024