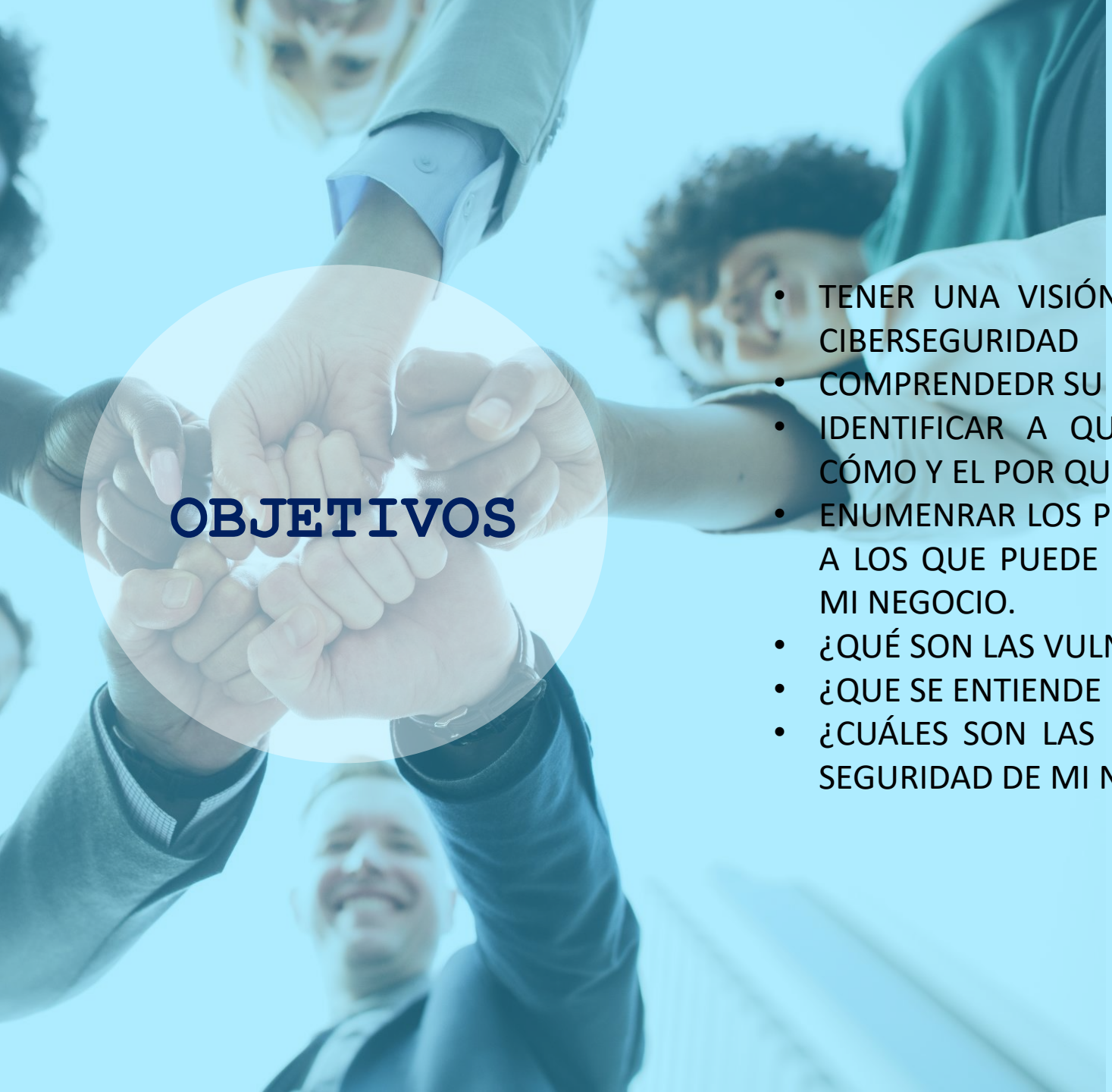
INICIO GRABACIÓN

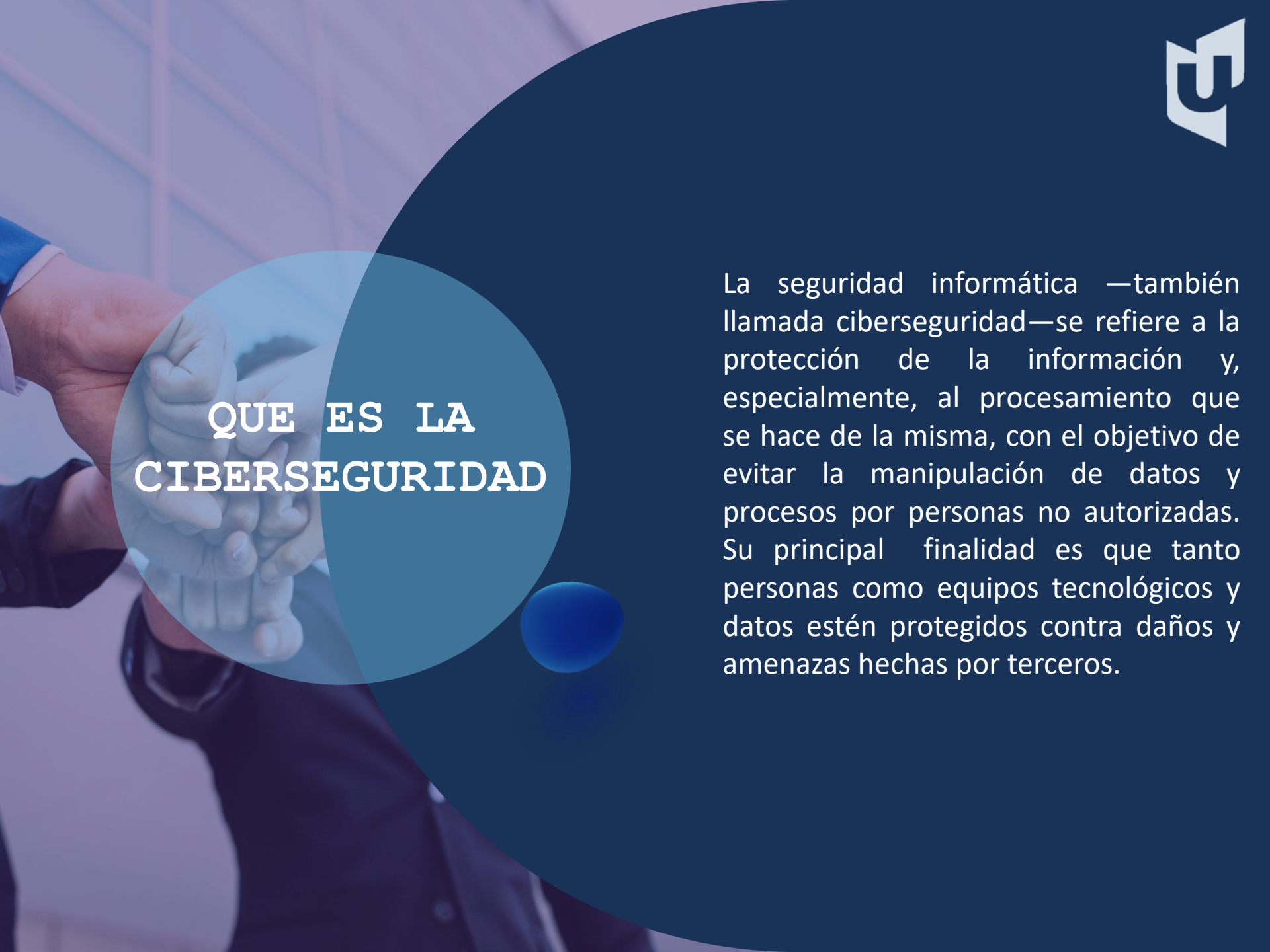
SANJOSÉ
FUNDACIÓN DE EDUCACIÓN SUPERIOR

INDICE



OBJETIVOS

- TENER UNA VISIÓN GLOBAL DE LA CIBERSEGURIDAD
- COMPRENDEDR SU SIGNIFICADO
- IDENTIFICAR A QUIEN AFECTA (EL CÓMO Y EL POR QUÉ)
- ENUMENRAR LOS POSIBLES RIESGOS A LOS QUE PUEDE ESTAR EXPUESTO MI NEGOCIO.
- ¿QUÉ SON LAS VULNERABILIDADES?
- ¿QUE SE ENTIENDE POR AMENAZAS?
- ¿CUÁLES SON LAS NECESIDADES DE SEGURIDAD DE MI NEGOCIO?



QUE ES LA CIBERSEGURIDAD

La seguridad informática —también llamada ciberseguridad—se refiere a la protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros.

CONCEPTOS

- Es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente. La seguridad informática es en realidad una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos. La seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, como scripts de Java, ActiveX, cuidar del uso adecuado de la computadora, los recursos de red o de Internet.

¿Por qué es tan importante la seguridad informática?

Prevenir el robo de datos tales como números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos relacionados con el trabajo, hojas de cálculo, etc. es algo esencial durante las comunicaciones de hoy en día. Muchas de las acciones de nuestro día a día dependen de la seguridad informática a lo largo de toda la ruta que siguen nuestros datos. Y como uno de los puntos iniciales de esa ruta, los datos presentes en un ordenador también puede ser mal utilizados por intrusiones no autorizadas. Un intruso puede modificar y cambiar los códigos fuente de los programas y también puede utilizar tus imágenes o cuentas de correo electrónico para crear contenido perjudicial, como imágenes pornográficas o cuentas sociales falsas. Hay también ciberdelincuentes que intentarán acceder a los ordenadores con intenciones maliciosas como pueden ser atacar a otros equipos o sitios web o redes simplemente para crear el caos. Los hackers pueden bloquear un sistema informático para propiciar la pérdida de datos. También son capaces de lanzar ataques DDoS para conseguir que no se pueda acceder a sitios web mediante consiguiendo que el servidor falle. Todos los factores anteriores vuelven a hacer hincapié en la necesidad de que nuestros datos deben permanecer seguros y protegidos confidencialmente. Por lo tanto, es necesario proteger tu equipo y eso hace que sea necesaria y muy importante todo lo que es la seguridad informática.

QUE ABARCA?

La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas.

Este tipo de información se conoce como información privilegiada o confidencial.

Las cuatro áreas principales que cubre la seguridad informática

1. **Confidencialidad**: Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
2. **Integridad**: Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.
3. **Disponibilidad**: Los datos deben estar disponibles para los usuarios cuando sea necesario.
4. **Autenticación**: Estás realmente comunicándote con los que piensas que te estás comunicando.

Principales tipos de seguridad informática

Al hablar de seguridad informática es fundamental distinguir algunas de las tipologías que existen, siendo los principales elementos a dar protección el software, la red y el hardware.

Seguridad de hardware

- Este tipo de seguridad se relaciona con la protección de dispositivos que se usan para proteger sistemas y redes —apps y programas de amenazas exteriores—, frente a diversos riesgos. El método más usado es el manejo de sistemas de alimentación ininterrumpida (SAI), servidores proxy, firewall, módulos de seguridad de hardware (HSM) y los data lost prevention (DLP). Esta seguridad también se refiere a la protección de equipos físicos frente a cualquier daño físico.

Seguridad de software

- Usado para salvaguardar los sistemas frente ataques malintencionados de hackers y otros riesgos relacionados con las vulnerabilidades que pueden presentar los softwares. A través de estos “defectos” los intrusos pueden entrar en los sistemas, por lo que se requiere de soluciones que aporten, entre otros, modelos de autenticación.

Bibliografía

Seguridad de red

- Principalmente relacionada con el diseño de actividades para proteger los datos que sean accesibles por medio de la red y que existe la posibilidad de que sean modificados, robados o mal usados. Las principales amenazas en esta área son: virus, troyanos, phishing, programas espía, robo de datos y suplantación de identidad.

SGSI

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de políticas de administración de la información. El término se denomina en Inglés “Information Security Management System” (ISMS).

El término SGSI es utilizado principalmente por la ISO/IEC 27001, que es un estándar internacional aprobado en octubre de 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": **PDCA** – acrónimo de **Plan, Do, Check, Act** (Planificar, Hacer, Verificar, Actuar), siendo éste un enfoque de mejora continua:

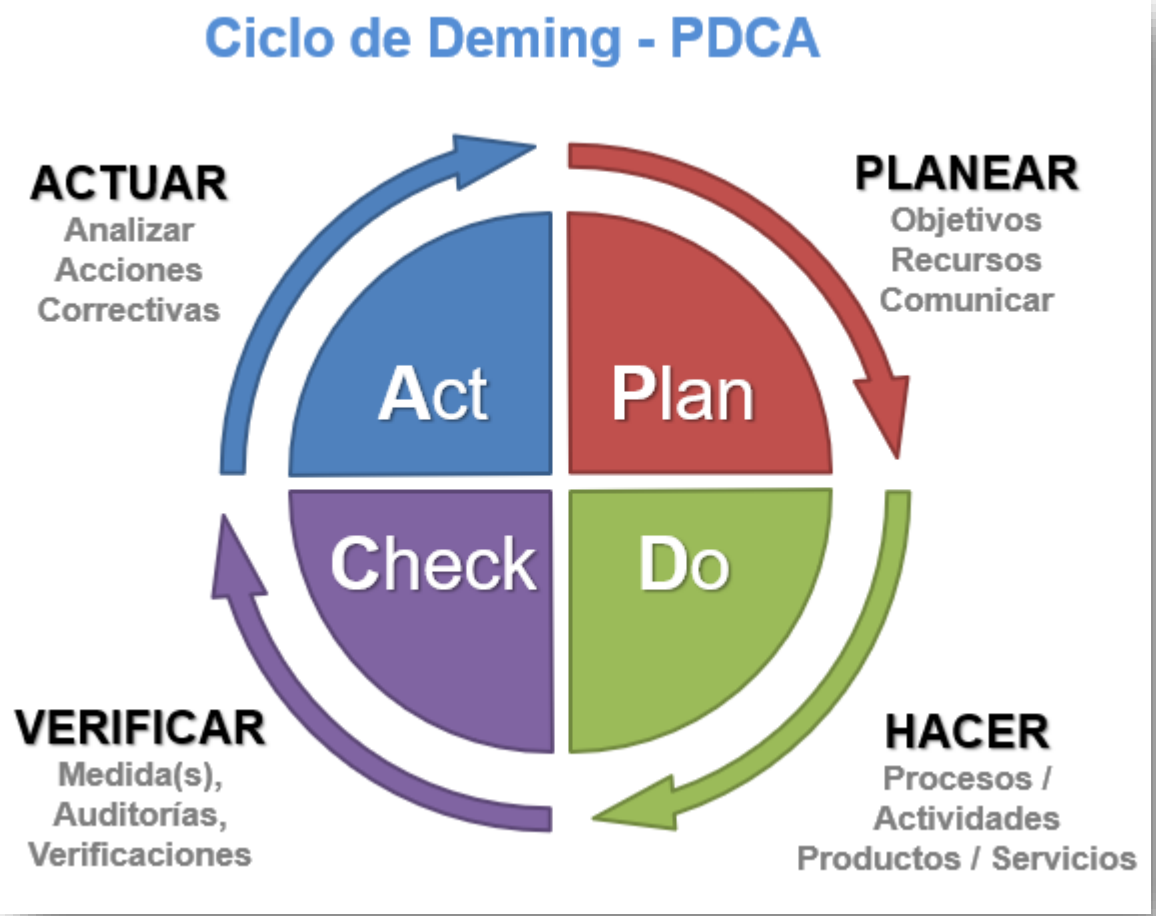
Plan (planificar): es una fase de diseño del SGSI de evaluación de riesgos de seguridad de la información y la selección de controles adecuados.

Do (hacer): es una fase que envuelve la implantación y operación de los controles.

Check (controlar): es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

Act (actuar): en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN



SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

SGSI

FUNDACIÓN DE EDUCACIÓN SUPERIOR
SANJOSÉ
INSTITUCIÓN TECNOLÓGICA

FIN DE GRABACIÓN