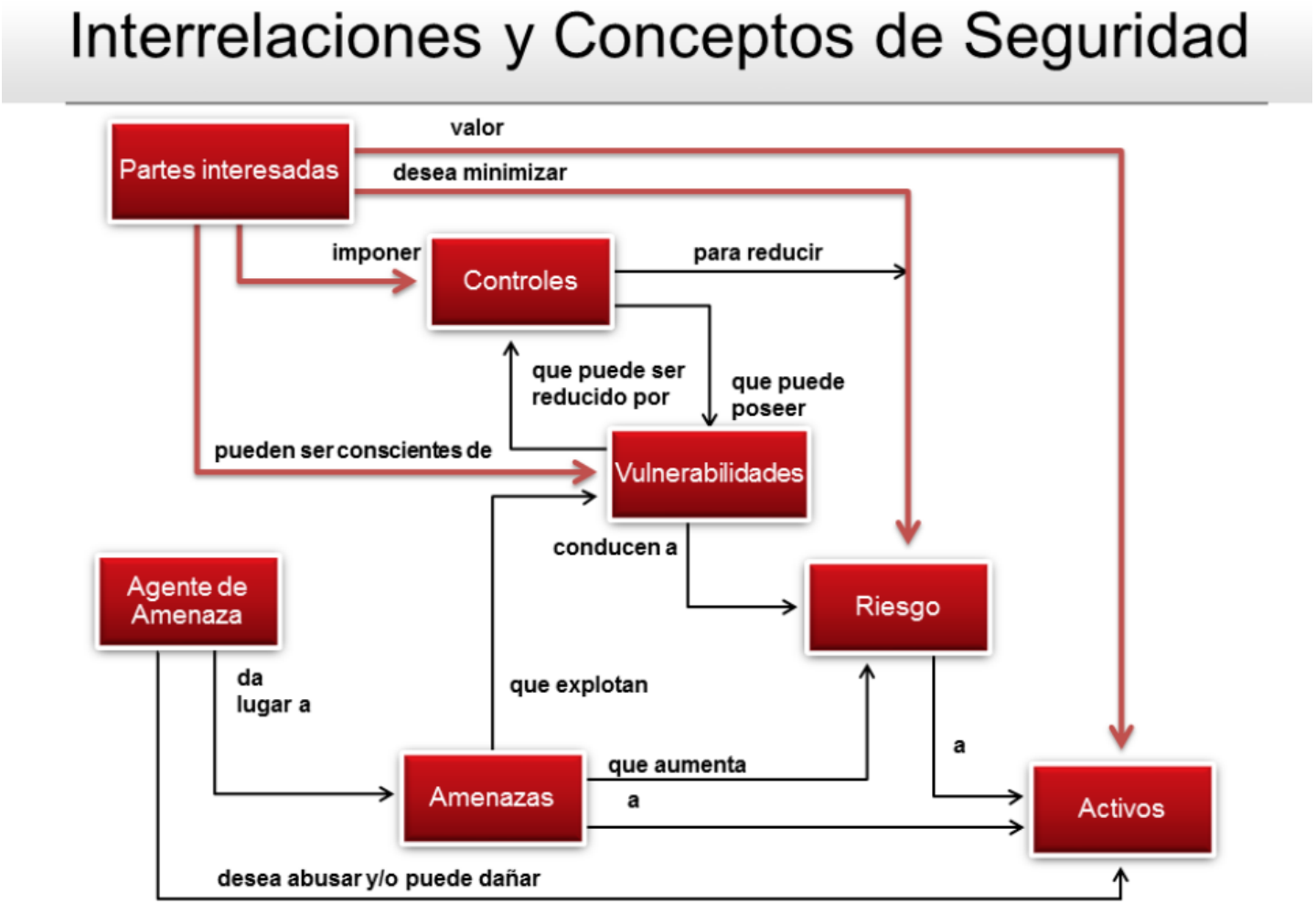
DIPLOMADO EN
CIBERSEGURIDAD

CONTROLES EN CIBERSEGURIDAD ESSENTIALS

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

SEGURIDAD DE LA INFORMACIÓN

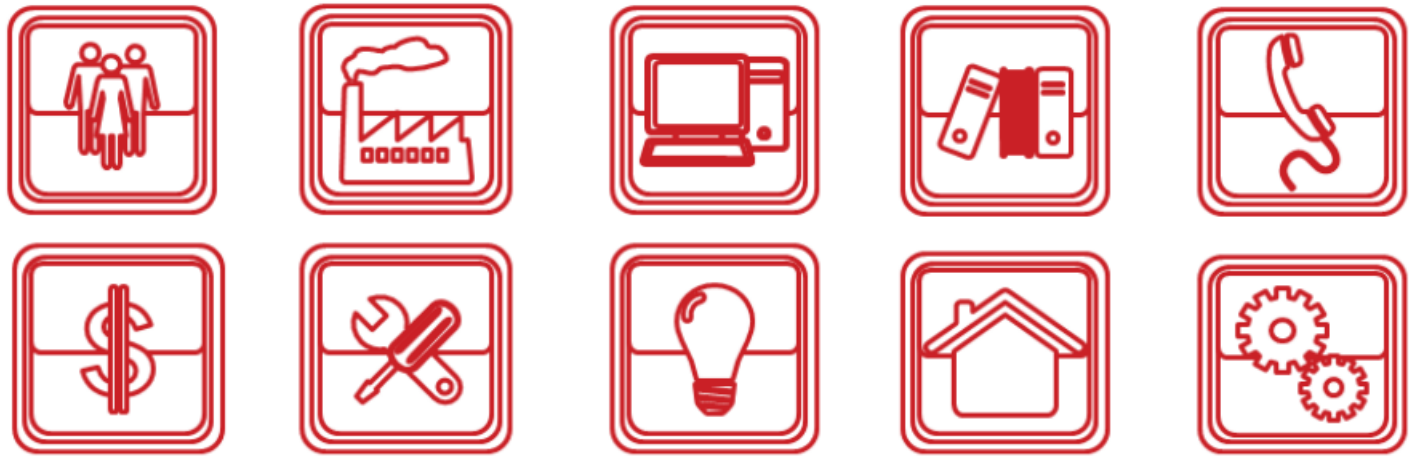


SEGURIDAD DE LA INFORMACIÓN

Activo

ISO 27032, cláusula 4.6

Todo lo que tiene valor para una persona, una organización o un gobierno



SEGURIDAD DE LA INFORMACIÓN

Información y Activo

ISO 9000, cláusula 3.7.1 e ISO 27032, cláusula 4.27

- **Información:** datos importantes
- **Activo de información**: conocimiento o datos que tiene un valor para el individuo o la organización

SEGURIDAD DE LA INFORMACIÓN

Activos en el Ciberespacio

Activos personales

- Activos físicos
- Activos virtuales

Activos de la organización

- Activos físicos
- Activos virtuales

NOTA: Un activo se considera como un Activo Crítico cuando tiene el potencial de impactar significativamente el logro de los objetivos de la organización.

SEGURIDAD DE LA INFORMACIÓN

Activos personales

Suscripciones en línea y PC

Identidad en línea del consumidor individual

Datos médicos

Cuenta bancaria

Cuentas de correo electrónico

Cuentas bancarias y pagos de cuentas en línea

Fotos, vídeos, música y

Registros de impuestos

SEGURIDAD DE LA INFORMACIÓN

Activos personales

Suscripciones en línea y PC

Identidad en línea del consumidor individual

Datos médicos

Cuenta bancaria

Cuentas de correo electrónico

Cuentas bancarias y pagos de cuentas en línea

Fotos, vídeos, música y

Registros de impuestos

SEGURIDAD DE LA INFORMACIÓN

Activos de la Organización

Redes

Servidores

Estaciones de trabajo

Reputación

Planes de

Propiedad intelectual

Marca

SEGURIDAD DE LA INFORMACIÓN

Amenazas

ISO 27032, cláusula 4.46

Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema, un individuo u organización

SEGURIDAD DE LA INFORMACIÓN

Amenazas a los Activos Personales

Algunas de las amenazas pueden ser:

- La identidad en línea de la persona es robada o enmascarada
- el acceso no autorizado a la información financiera de una persona - robo del dinero de la persona y fraude
- un equipo de usuario final el cual se convirtió en un equipo zombie, robo virtual mediante redes botnets, o asaltos virtuales

SEGURIDAD DE LA INFORMACIÓN

Amenazas a los Activos de la Organización

La presencia en línea de las organizaciones es a menudo atacada por malhechores cuya intención es mayor que el simple vandalismo

Algunas de las amenazas pueden ser:

- Desfiguración o modificación de páginas web
- URL robada por un ciberdelincuente
- información revelada de empleados, clientes, socios o proveedores
- informes financieros interceptados
- acceso no autorizado a información importante de los gobiernos

SEGURIDAD DE LA INFORMACIÓN

Agente de Amenaza

ISO 27032, cláusula 9.2

Un agente de amenaza es un individuo o grupo de individuos que tienen algún rol en la ejecución o en el respaldo sobre un ataque.

Una comprensión profunda de sus motivaciones, capacidades e intenciones es crítica durante la evaluación de vulnerabilidades y riesgos, así como en el desarrollo e implementación de controles.

SEGURIDAD DE LA INFORMACIÓN

Vulnerabilidad

ISO 27032, cláusula 4.52 e ISO 27000, cláusula 2.89

La debilidad de un activo o de un control que puede ser explotada por una amenaza

CVE

CWE

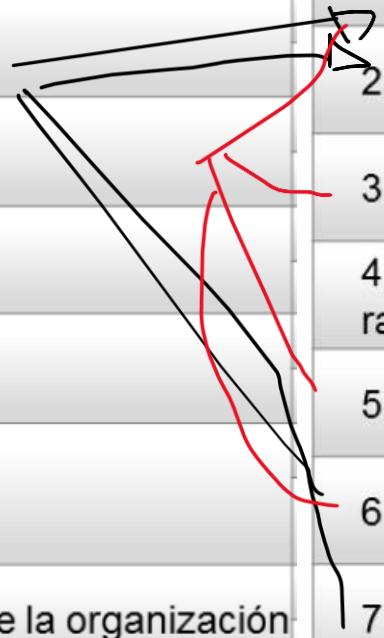
CVE-2025-4586

SEGURIDAD DE LA INFORMACIÓN

Tipos de Vunerabilidades

ISO 27005, Anexo D

Tipo de vulnerabilidad	Tipo de amenaza
1 Hardware	1 Daño físico
2 Software	2 Desastre natural
3 Red	3 Pérdida de servicios esenciales
4 Personal	4 Trastornos causados por la radiación
5 Sitio	5 Información comprometida
6 Estructura de la organización	6 Fallas técnicas
	7 Acción no autorizada



SEGURIDAD DE LA INFORMACIÓN

Tipos de Amenazas

ISO 27005, Anexo C

Tipo de amenaza	Ejemplo
1 Daño físico	Fuego
	Daño por agua
2 Desastre natural	Terremoto
	Inundación
3 Pérdida de servicios esenciales	Falta de aire acondicionado
	Corte de suministro eléctrico
4 Trastornos causados por la radiación	Radiación electromagnética
	Radiación térmica
5 Información comprometida	Escuchas telefónicas
	Robo de documentos
6 Fallas técnicas	Falla del equipo
	Sobrecarga de la red
7 Acción no autorizada	Acceso no autorizado
	Uso de software pirata

SEGURIDAD DE LA INFORMACIÓN

Relación: Vulnerabilidad y Amenaza

Ejemplos

Vulnerabilidades	Amenazas
Almacén desprotegido y sin vigilancia	Robo
Complicados procedimientos de proceso de datos	Error de entrada de datos por parte del personal
No segregación de tareas	Fraude, uso no autorizado de un sistema
Los datos no cifrados	Robo de Información
Uso de software pirata	Demanda, virus
No revisión de los derechos de acceso	Acceso no autorizado a las personas que han abandonado la organización
Procedimientos de backup	Pérdida de información

SEGURIDAD DE LA INFORMACIÓN

Riesgo

ISO 27005, cláusula 3.9 e ISO 27000, cláusula 2.68

- Definición: Efecto de la incertidumbre en los objetivos
- El riesgo de la seguridad de la información es a menudo:
  - Expresado en términos de una combinación de las consecuencias de un suceso de seguridad de la información y la probabilidad de ocurrencia asociada
  - Asociado con la posibilidad de que las amenazas exploten vulnerabilidades de un activo de información o grupo de activos de información y por lo tanto causar un daño a la organización

SEGURIDAD DE LA INFORMACIÓN

Controles

Clasificación

Control Preventivo

Desalentar o prevenir la aparición de problemas

Control de Detección

Buscar, detectar e identificar problemas

Control Correctivo

Resolver problemas encontrados y prevenir la recurrencia

PROGRAMA DE CIBERSEGURIDAD

Establecer y administrar un Programa de Ciberseguridad incluye a todas las partes relevantes que trabajarán conjuntamente para proteger la inversión de la compañía en relación al hardware y los sistemas de software, y que asegurarán la disponibilidad, integridad y confidencialidad de la información.

En la creación de un Programa de Ciberseguridad se deben tener en cuenta, el tamaño, la complejidad de la organización, y la sensibilidad de la información de la empresa.

MARCO DE CIBERSEGURIDAD

Elegir el marco adecuado

Cuando se piensa en marcos de referencia, se requiere tener en mente las siguientes preguntas:

- La postura actual de la ciberseguridad
- El estado deseado para la ciberseguridad
- Los objetivos que desea alcanzar
- Oportunidades para mejorar
- Evaluar el progreso hacia el estado deseado
- El riesgo de la ciberseguridad
- Los requisitos de la legislación
- Los requisitos de la norma
- Los requisitos contractuales
- Los beneficios que le gustaría lograr

MARCO DE CIBERSEGURIDAD

Marco de Ciberseguridad

Elegir el marco adecuado

MARCO DE CIBERSEGURIDAD

ISO/IEC 27032:2012es una norma internacional publicada por ISO (Organización Internacional de Estandarización) que presenta una guía para la implementación de Ciberseguridad. Esta guía cubre las prácticas esenciales de seguridad para todas las partes interesadas en el ciberespacio. No es posible certificar una organización en la norma ISO 27032, porque no es un estándar que describe un sistema de gestión, sin embargo, es una ayuda muy importante para lo que respecta a la norma ISO 27001. Provee de una guía de prácticas de seguridad para partes interesadas en el Ciberespacio, una explicación de la relación entre Ciberseguridad y otros tipos de seguridad y también presenta un marco de referencia para permitir a las partes interesadas colaborar en la resolución de los asuntos de Ciberseguridad.

Marco de Ciberseguridad NIST, este marco es publicado por el Instituto Nacionalde Estándares y Tecnología, como una demanda publicada en febrero de 2014 por parte del Presidente Barack Obama en 2013, con el fin de establecer un conjunto de normas voluntarias de Ciberseguridad para empresas de infraestructura o misión crítica. El Marco de Referencia se centra en el uso de los impulsores del negocio para direccionar las actividades en Ciberseguridad y considerando los riesgos de la Ciberseguridad como parte de los procesos de gestión de riesgo de la organización. El Marco de Referencia incluye: el Marco Principal, el Perfil del Marco, y los Niveles de implementación del Marco.

MARCO DE CIBERSEGURIDAD

COBIT 5 es un marco emitido por ISACA (Asociación de Auditoría y Control de los sistemas de Información). Los Objetivos de Control para Información y Tecnologías Relacionadas (COBIT) proporciona las buenas prácticas a través de un Marco de Referencia por dominios y presenta las actividades dentro de una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de expertos. COBIT 5 está fuertemente centrado en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones de TI, garantizar la entrega del servicio y proporcionar una forma de medición contra el cual evaluarse cuando las cosas resultaron equivocadas.

La Serie SP 800 de NIST ofrece una serie de documentos que describen las políticas, procedimientos, y directrices de seguridad informática del gobierno federal de los Estados Unidos. NIST (Instituto Nacional de Estándares y Tecnología) es una unidad dependiente del Departamento de Comercio. Las publicaciones de la Serie 800 de NIST surgió como resultado de una investigación exhaustiva en métodos viables y rentables para optimizar de forma proactiva la seguridad de las tecnologías de la información (TI), los sistemas y las redes. Las publicaciones cubren todos los procedimientos y criterios recomendados por el NIST para evaluar y documentar las amenazas y vulnerabilidades y para implementar medidas de seguridad para minimizar el riesgo de eventos adversos. Las publicaciones pueden ser útiles como guías para la aplicación de reglas de seguridad y como referencia legal en caso de litigios relativos a cuestiones de seguridad. La serie de documentos pueden ser útiles para empresas e instituciones educativas, así como también para organismos de gobierno.

DIPLOMADO EN CIBERSEGURIDAD

MARCO DE CIBERSEGURIDAD

ITIL, Biblioteca de Infraestructura de Tecnología de la Información, se ha publicado como un conjunto de series de cinco volúmenes básicos para la gestión de servicios de TI (ITSM) que se centra en la alineación de los servicios de TI con las necesidades del negocio. Al utilizar ITIL una organización puede establecer un punto de referencia a partir del cual se puede planificar, implementar y medir. ITIL describe los procesos, procedimientos, tareas y listas de verificación, los cuales no son específicos para una determinada organización, pero pueden ser aplicados por una organización para establecer la integración con su estrategia, ofrecer valor y mantener un nivel mínimo de competencia.

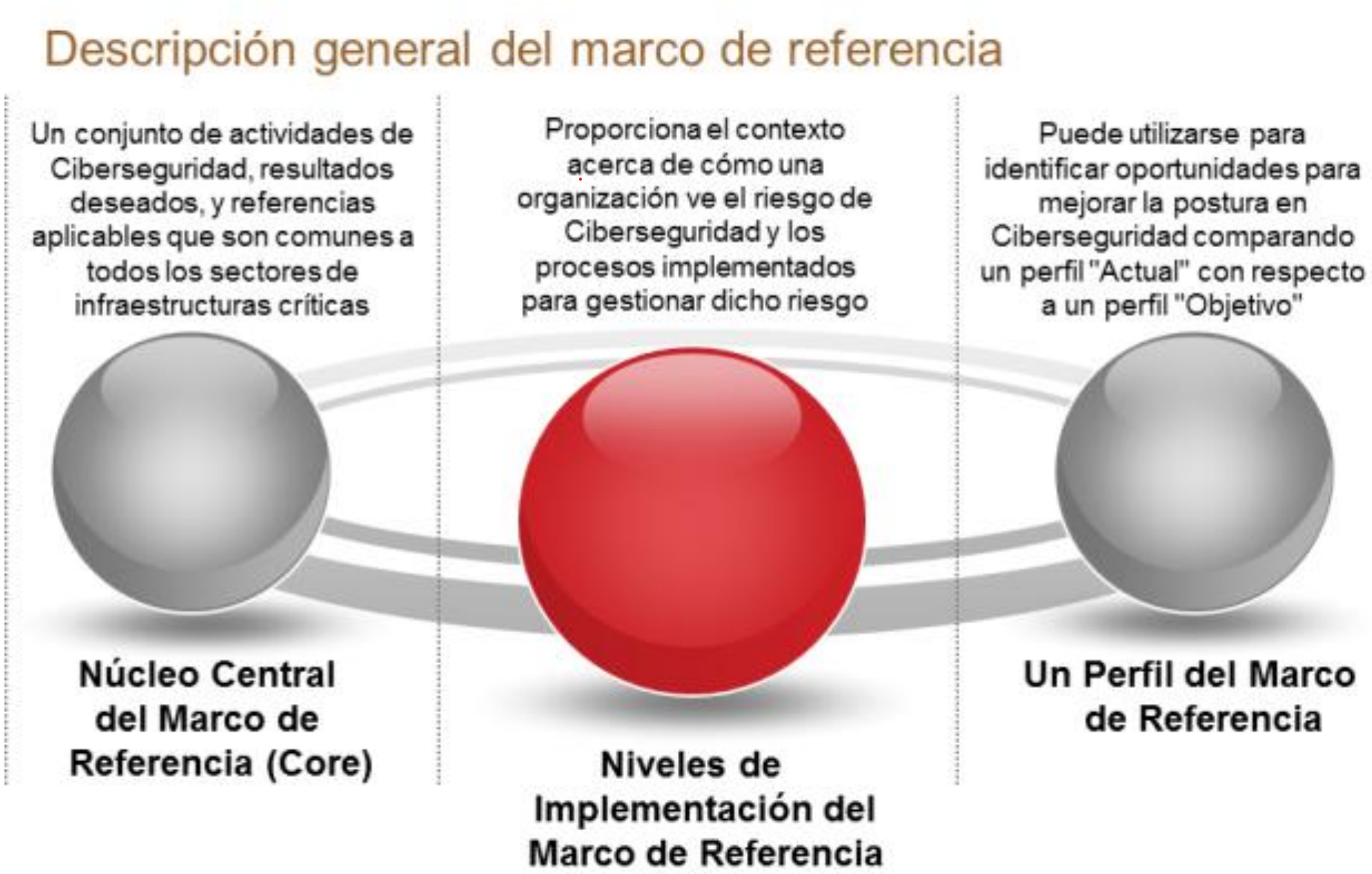
ISO/IEC 27001:2013 es una norma internacional publicada por ISO (Organización Internacional de Estandarización) que define la forma de implementar y operar el Sistema de Gestión de Seguridad de la Información. Esta Norma Internacional ha sido preparada para proveer requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI). Contiene un conjunto de requisitos para la selección de controles de seguridad adaptados a las necesidades de cada organización, basado en las mejores prácticas de la industria, un sistema de gestión que está integrado en el marco global del riesgo asociado con la actividad de la organización, y un proceso reconocido internacionalmente, definido y estructurado para gestionar la seguridad de la información.

MARCO DE CIBERSEGURIDAD NIST

Conceptos básicos del marco

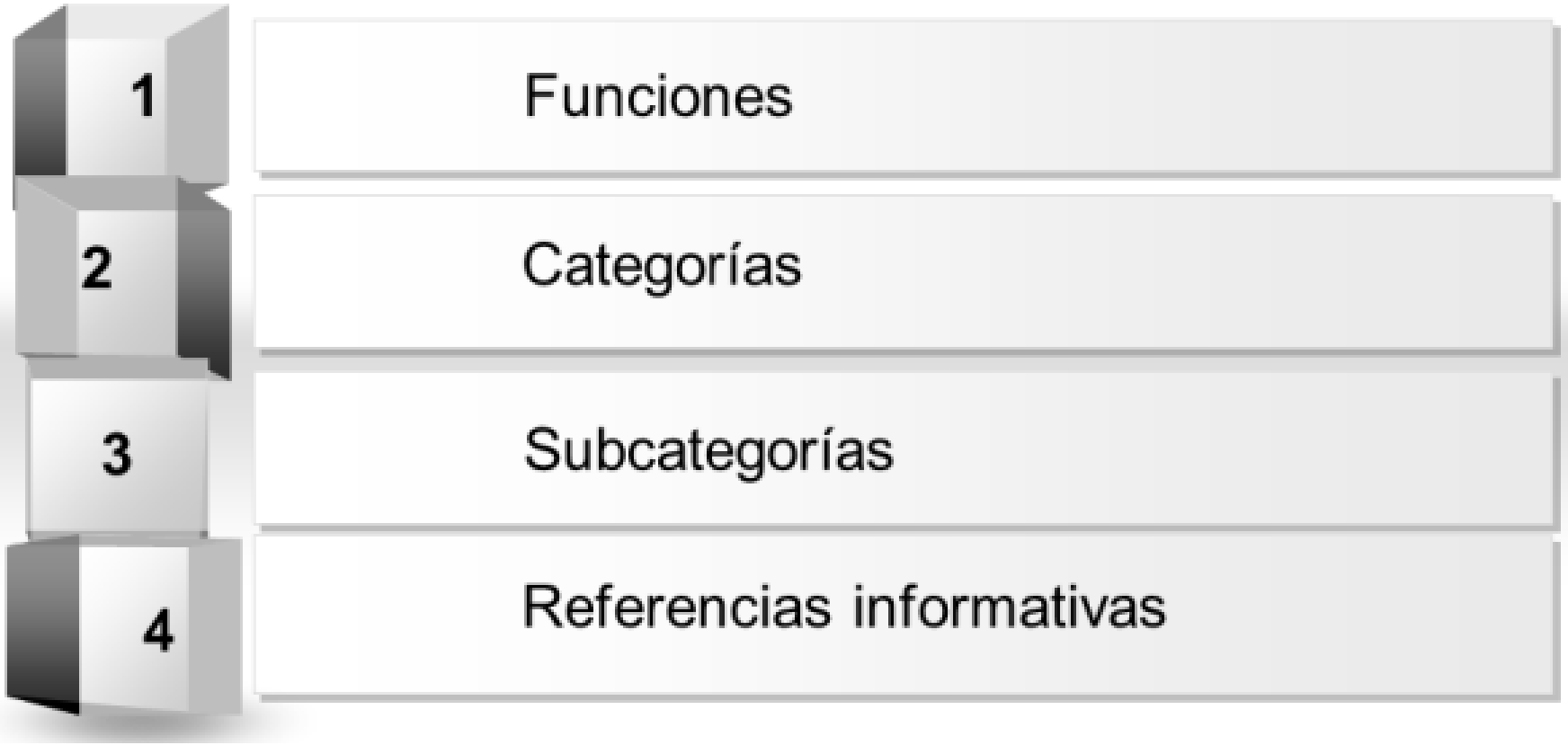
- El Marco de Referencia está diseñado para complementar las operaciones del negocio existentes y de Ciberseguridad
- Puede servir como base para un nuevo programa de Ciberseguridad o como un mecanismo para mejorar un programa existente
- El Marco de Referencia puede ayudar a identificar brechas en las prácticas de Ciberseguridad de una organización.

MARCO DE CIBERSEGURIDAD NIST



MARCO DE CIBERSEGURIDAD NIST

Núcleo central del marco de referencia (Core)



MARCO DE CIBERSEGURIDAD NIST

Funciones básicas de marco

MARCO DE CIBERSEGURIDAD

Dentro del objetivo de garantizar la seguridad de la información, la ciberseguridad se refiere específicamente al aprovisionamiento de hardware y software de procesamiento seguro. Las tareas de seguridad de la información y ciberseguridad se pueden clasificar en cinco funciones, siguiendo el marco desarrollado por el **Instituto Nacional de Estándares y Tecnología (NIST) (nist.gov/cyberframework/online-learning/five-functions)**:

MARCO DE CIBERSEGURIDAD

Identificar: desarrollar políticas y capacidades de seguridad. Evalúe riesgos, amenazas y vulnerabilidades y recomiende controles de seguridad para mitigarlos.

Proteger: adquiera/desarrolle, instale, opere y retire activos de hardware y software de TI con la seguridad como requisito integrado en cada etapa del ciclo de vida de estas operaciones.

DIPLOMADO EN CIBERSEGURIDAD

MARCO DE CIBERSEGURIDAD

Detectar: realice una supervisión continua y proactiva para garantizar que los controles sean eficaces y capaces de proteger contra nuevos tipos de amenazas.

Responda: identifique, analice, contenga y erradique las amenazas a la seguridad de los sistemas y los datos.

Recuperar: implemente resiliencia de ciberseguridad para restaurar sistemas y datos si otros controles no pueden prevenir ataques.

CORFO
BECAS Capital Humano CORFO
CHILETEC
CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE