CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

TALLER DE AUDITORÍA SGSI

enfocado en **ISO 27.001**

DIPLOMADO
CIBERSEGURIDAD

Profesor – Jorge Vasconcelos

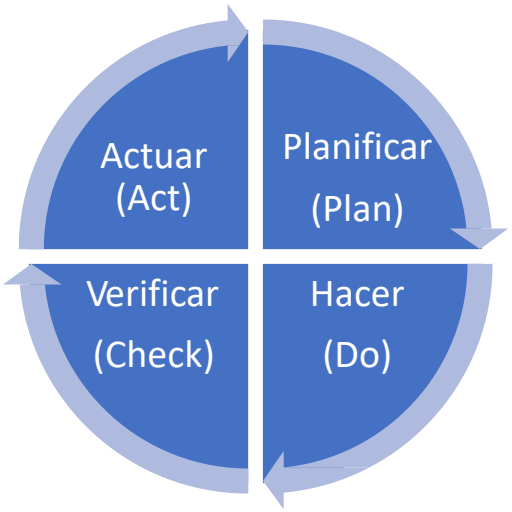
- Contador Público y Auditor con Diplomado en Gestión, Seguridad y Auditoría de Tecnología de Información y Postítulo E-Auditoria por la Universidad de Santiago de Chile. Especialista en la implementación y auditoría a los sistemas de información. Posee certificaciones internacionales ISO Lead Auditor 27001, ISO Lead Implementer ISO 29100, entre otras.
- Ayudante y docente en la Universidad de Santiago de Chile, Universidad Alberto Hurtado y Universidad Autónoma en ramos de Contabilidad, Finanzas, Auditoría y SAP.
- Coordinador de Calidad Académica, Programas de Ciberseguridad de Capacitación USACH Alignment SpA.
- Director de Finanzas - Alignment SpA.
- Auditor 1 ISO 27.001 – Austral Certificaciones.
- Auditor Interno - OSconsultores

jorge.vasconcelos@usach.cl

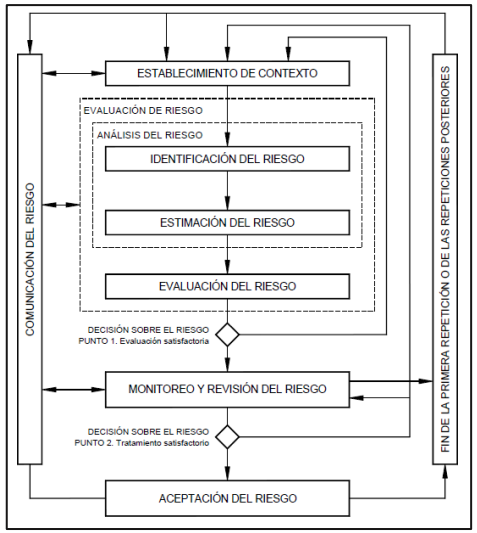
jdvasconcelos

¿Que ofrece ISO 27.001?

Una metodología basada en mejores prácticas
que posibilita la implementación de un SGSI



Visión de Procesos
alineada al ciclo PDCA



Enfoque de Riesgos

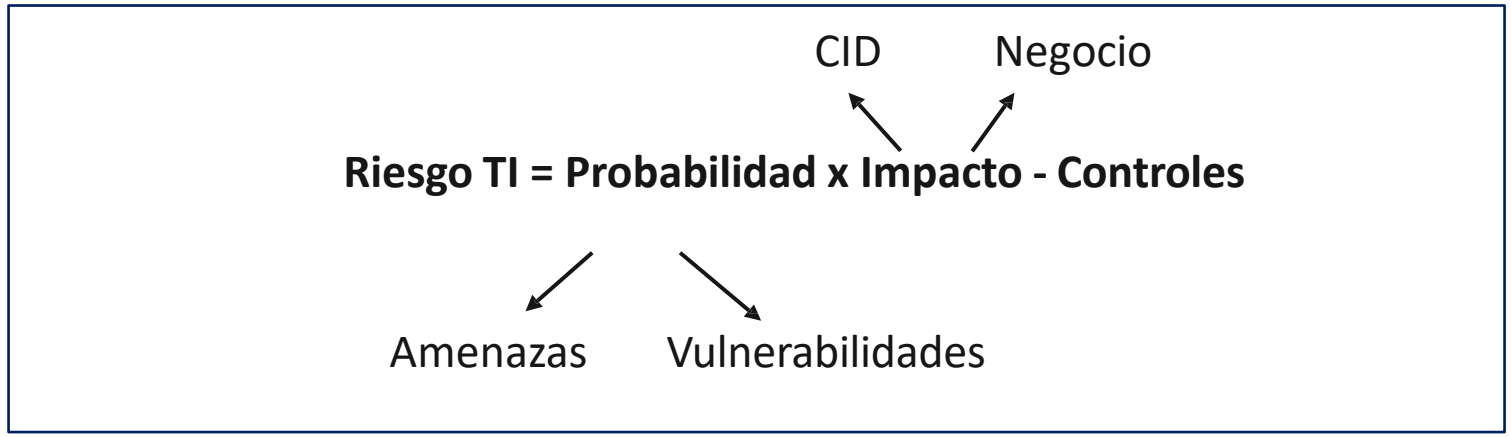
Controles de Seguridad
de la Información

Clausula 1:	Objeto y campo de aplicación
Clausula 2:	Referencias normativas
Clausula 3:	Términos y definiciones
Clausula 4:	Contexto de la organización
Clausula 5:	Liderazgo
Clausula 6:	Planificación
Clausula 7:	Soporte
Clausula 8:	Operación
Clausula 9:	Evaluación del desempeño
Clausula 10:	Mejora

Metodología
Estandarizada

Definiciones Importantes (ISO 73:2009)

- **Riesgo:** Efecto de la incertidumbre en la consecución de los objetivos.



- **Gestión de Riesgo:** Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.

- **Proceso de Gestión de Riesgo:** Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

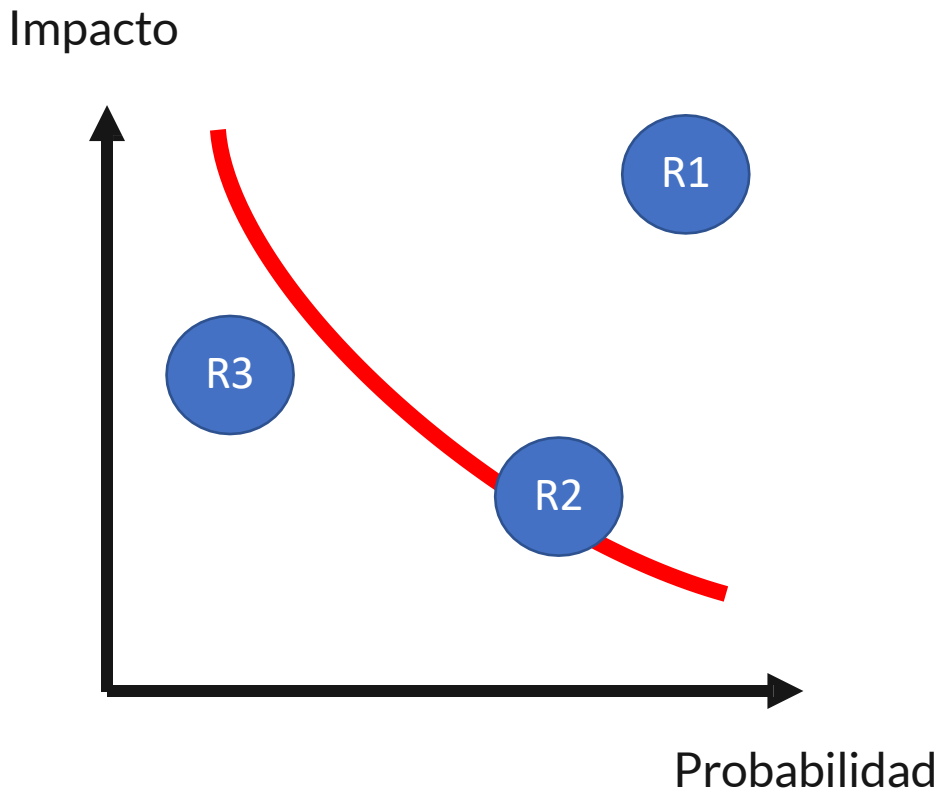
En términos Simples

1. La organización establece su apetito de riesgo.

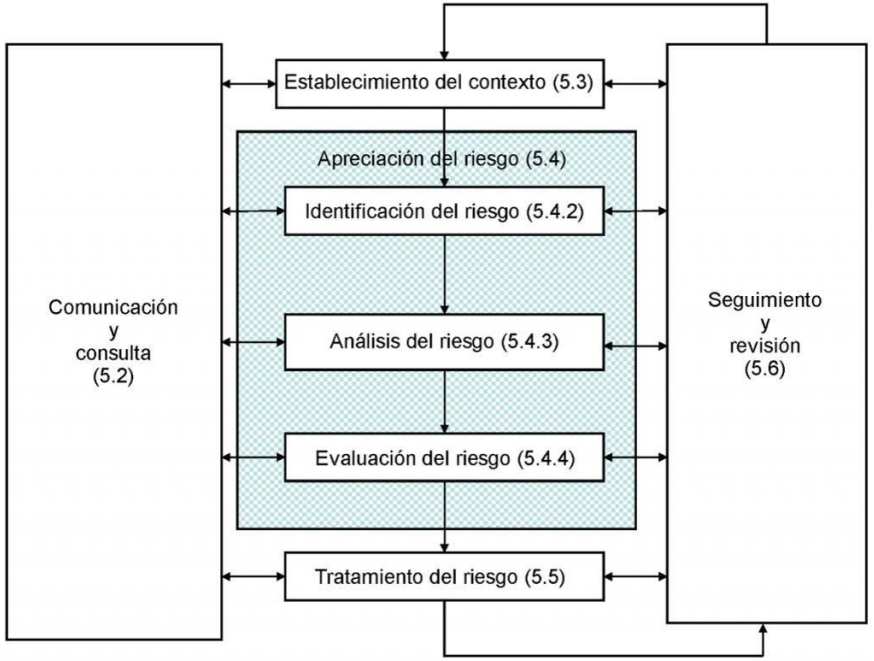
2. Realiza el proceso de apreciación de riesgos. El cual en base a la identificación del activo y su criticidad, el análisis de amenazas y vulnerabilidades, obtiene la evaluación del riesgo inherente.

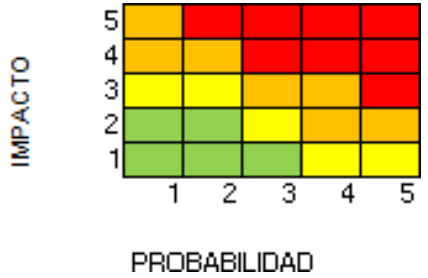
3.-Los riesgos que están por sobre el apetito o la tolerancia establecida deben ser tratados, los otros se aceptan.

4.- Analiza los controles existentes y los que implementará y en base a la evaluación de estos obtiene el riesgo residual.



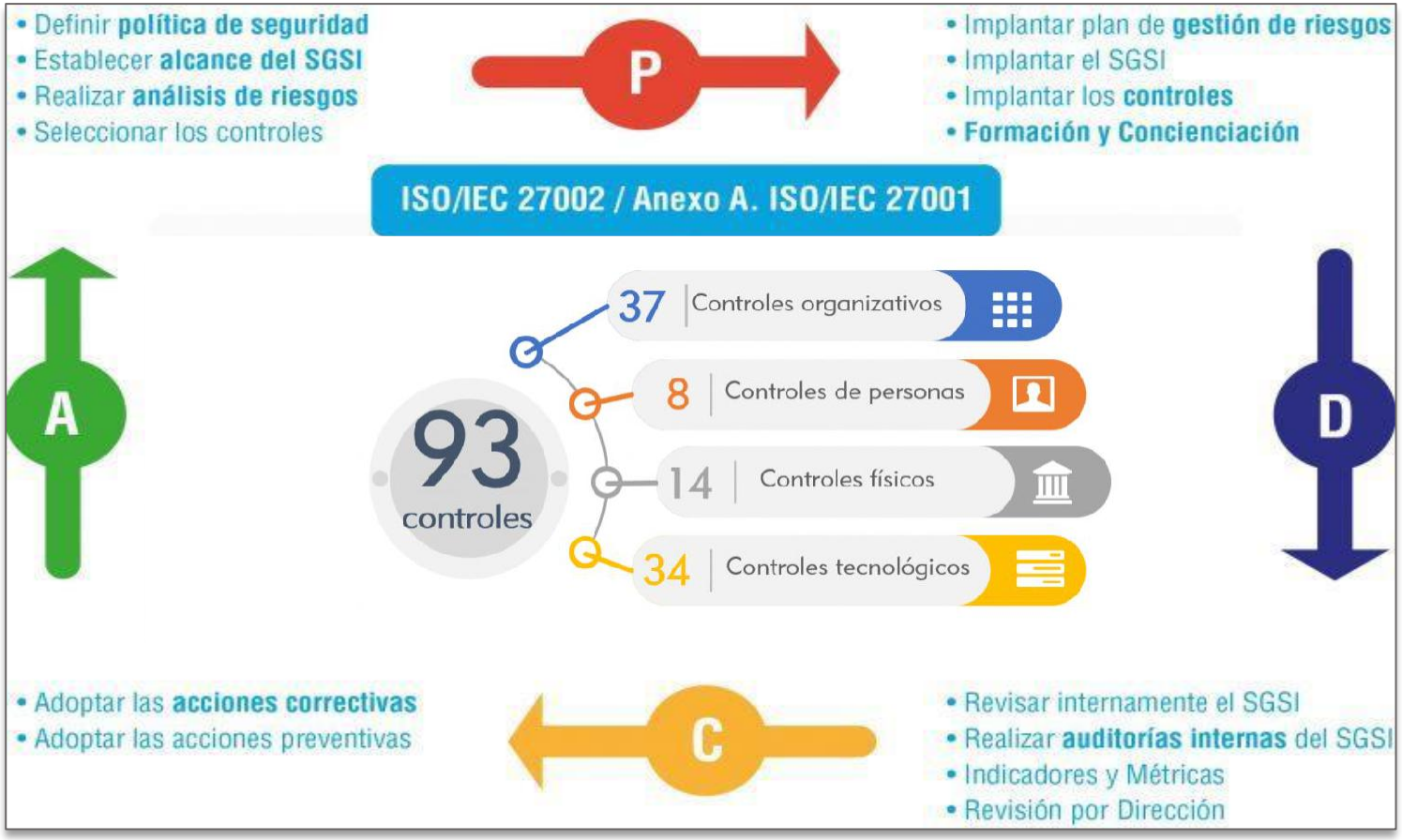
Proceso de Gestión de Riesgos – ISO 31.000





Actividad	Severidad
Actividad 11	Catastrófico
Actividad 2	Catastrófico
Actividad 4	Alto
Actividad 7	Moderado

La evolución de las Normas



Fuente: Adaptción https://revista.aenor.com/348/isoiec-27001-y-ens-binomio-perfecto-para-la-ciberseguridad.html

7.5 Información documentada

Según ISO 27001 – Información Documentada:

- Alcance
- Política de Seguridad de la Información
- Proceso de apreciación de riesgos
- Proceso de tratamiento de riesgos
- Objetivos de SI
- Competencias
- Registros de la ejecución del SGSI (Si es necesaria)
- Resultados de las evaluaciones de riesgos de seguridad de la información
- Resultados del tratamiento de riesgos de seguridad de la información
- Evidencias para el seguimiento, medición, análisis y evaluación
- Resultados de la Auditoría y sus resultados
- Resultados de la revisión por la dirección
- No conformidades y acciones correctivas

- Documentación de origen externa (Si es necesaria)
- Todo información que la empresa estime necesaria para SGSI

Certificación ISO 27.001

- Es un proceso en la cual las organizaciones buscan validar sus capacidades en la implementación del SGSI mediante un tercero.

- Los organismos certificadores de ISO 27.001 en general corresponden a organismos internacionales acreditados con organismos de acreditación de alcance global, poco están acreditados en LATAM.

Por que certificarse?

- Entérminos prácticos la certificación en general tiene como propósito:
  - Avanzar hacia una mejora continua en la organización
  - Diferenciarse en el mercado
  - Dar mayor confianza a partes interesadas
  - Acceder a nuevas oportunidades y negocios

- El valor de la certificación guarda relación con variascosas:
  - Con quien se certifica
  - El alcance del SGSI
  - El propósito mismo
  - La finalidad

- En un sentido positivista las organizaciones deberían certificarse para fortalecer la implementación de su SGSI, contando con evaluaciones independientes periódicas que le posibilitaran mayores y mejores herramientas para su mejora continua.

Rol del Auditor SGSI

La Auditoría como Medio Estratégico

- Verificar que los controles son eficaces y adecuadas
- Asegurar que el SGSI se mantiene, revisa y mejora de forma continua
- Alinear la seguridad de la Información con los objetivos estratégicos de la organización

Roles, Responsabilidades y el Campo de Juego

Los Roles Clave

- **Auditor/ Equipo Auditor**

Conducen la investigación. Reúnen y verifican la información.

- **Auditado**

El socio en la investigación. Proporciona acceso a la evidencia.

- **Cliente de Auditoría**

Quien encarga la investigación y recibe los resultados.

El Modelo de las Tres Líneas de Defensa

1ª Línea Gerencia Operativa	2ª Línea Control y Supervisión	3ª Línea Aseguramiento Independiente
Dueña y gestora de los riesgos y controles.	Funciones de gestión de riesgos y cumplimiento que monitorean la primera línea	Auditoría Interna, proporcionando una visión objetiva a la alta dirección

Una auditoría exitosa requiere una clara coordinación entre las tres líneas de defensa.

Principios fundamentos del Auditor

Integridad
El fundamento de la profesionalidad.

Objetividad
La obligación de ser imparcial y justo.

Confidencialidad
Seguridad y discreción con la información.

Debido Cuidado Profesional
Diligencia y juicio en la auditoría.

Enfoque Basado en Evidencia
Conclusiones fiables y reproducibles a través de un proceso sistemático.

Independencia
La base para la imparcialidad y objetividad de las conclusiones.

¿Por Qué Auditamos?

Verificar

Confirmar que los procesos y controles cumplen con los requisitos establecidos (normas, políticas, contratos).

Cumplir

Demostrar conformidad ante regulador es, clientes y otras partes interesadas, gestionando el riesgo de Compliance.

Mejorar

Identificar oportunidades, optimizar recursos y fortalecer la cultura de mejora continua. El ciclo PDCA es inherente al sistema.

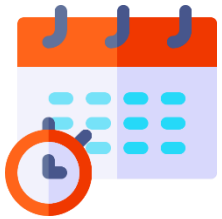
"La auditoría no es un examen para encontrar culpables, es un diagnóstico para generar valor."

Anatomía de un Plan de Auditoría Eficaz

Objetivos de la auditoría.

Alcance y Criterios (previamente definidos).

Equipo auditor y roles.



Agenda (fechas, horas y lugares).

Logística y recursos necesarios.

Confidencialidad y seguridad de la información.

Consejo del Guía

"Determinación de la viabilidad de la auditoría" (ISO/IEC 27.007)

Antes de seguir, asegúrese de tener la cooperación, el tiempo y los recursos adecuados.

Proceso de Auditoria: Recorrido Estructurado

Planificar

- Confirmar alcance
- Revisar documentación base (SoA, auditorías previas)
- Comunicación formal al auditado.

Ejecutar

- Reunión de apertura.
- Recolección de evidencias
- Registros de Hallazgos/No conformidades

Informar

- Análisis y consolidación de No conformidades
- Reunión de cierre
- Emisión de informe final

Mejorar

- Gestión de las No Conformidades
- Seguimiento de acciones correctivas.
- Integración de Revisión por la dirección

De hallazgos a Oportunidad de Fortalecimiento

No Conformidad
Incumplimiento de un requisito de la norma, política interna o obligación legal/contractual.

*Requiere un **Plan de acciones correctivas formal** con análisis de causa raíz.

Observación/Oportunidad de mejora
Una debilidad o situación que, sin ser una incumplimiento, podría convertirse en uno o cuya mejora fortalecería el SGSI.

*Se registra como una **recomendación** para la mejora proactiva.

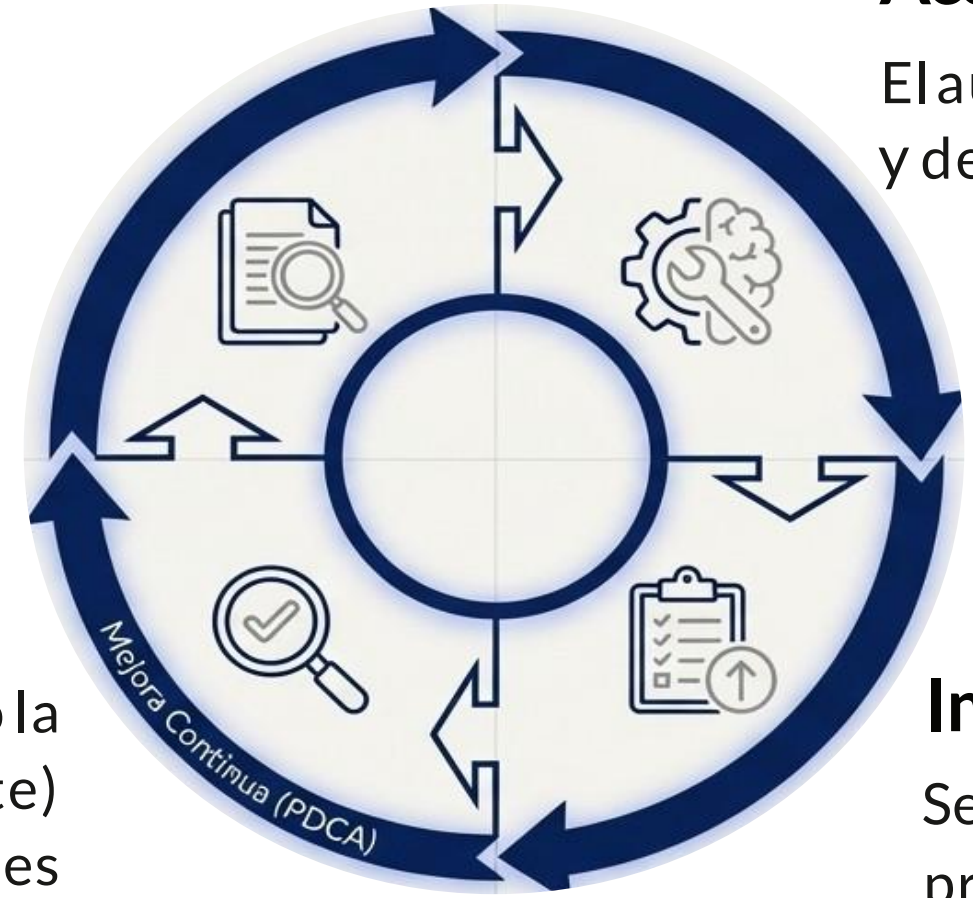
Proceso de Auditoria: Recorrido Estructurado

Acciones Correctivas

El auditado analiza la causa raíz y define un plan de acción.

Informe de Auditoría

Presenta los hallazgos objetivos.



Verificación de Seguimiento

El auditor (o la función correspondiente) verifica que las acciones fueron eficaces.

Implementación

Se ejecutan las mejoras en los procesos y controles.

Evidencia Objetiva

NO es evidencia objetiva

- "Me dijeron que siempre lo hacen así."
- "Creo que el proceso es seguro."
- "Generalmente, cumplimos con el plazo."

SÍ es evidencia objetiva

- "Revisé los últimos 50 registros del sistema de control de acceso."
- "Observé a 3 operadores seguir el procedimiento XYZ-01documentado."
- "El informe de vulnerabilidades del 15 de mayo muestra 3 ítems críticos sin resolver."

El verdadero rol del Auditor: Agregar Valor

Hemos pasado de la percepción de la auditoría como un control a entenderla como una disciplina para:

- Comprender el contexto.
- Verificar con evidencia objetiva.
- Comunicar con claridad.
- Impulsar la mejora.

'Si crees que la tecnología puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología.''

Bruce Schneier

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

TALLER DE AUDITORÍA SGSI

enfocado en **ISO 27.001**

DIPLOMADO
CIBERSEGURIDAD