UNE-ISO/IEC 27001:2014

Sistema de gestión de la seguridad de la información (SGSI). La ciberseguridad gestionada

Índice

Introducción

enColaboración
CONSULTORÍA COLABORATIVA

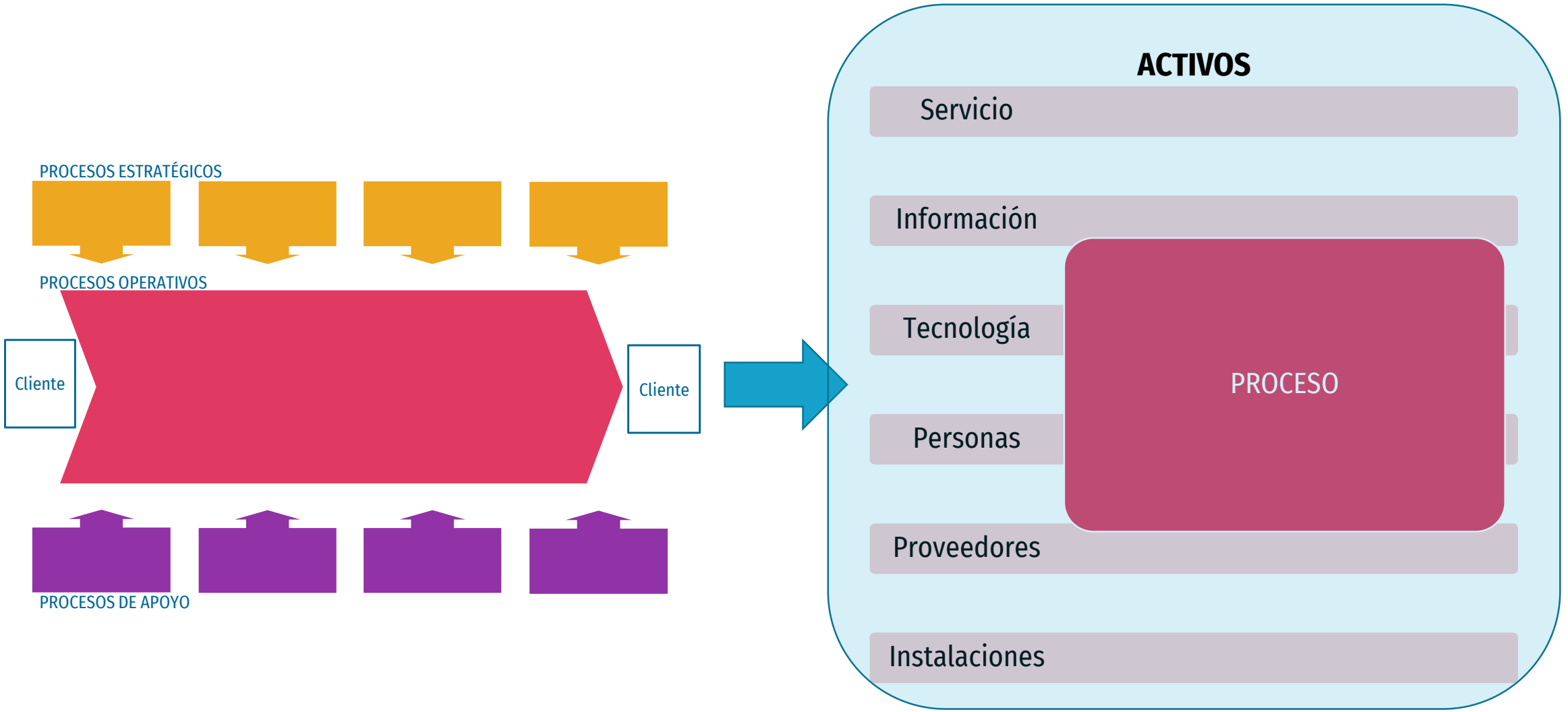
Información

- Activo
- Debidamente protegida
- Almacenada en muchas formas
- Transmitida por diversos medios
- Depende de las TI en todo su ciclo de vida
- Expuesta a más amenazas y vulnerabilidades

Seguridad de la información

- Activos de información
- No solo seguridad informática
- Protección de:
  - Confidencialidad
  - Integridad
  - Disponibilidad

Activo



Seguridad de la información

- Evitar incidentes
- Gestionarlos adecuadamente cuando suceden

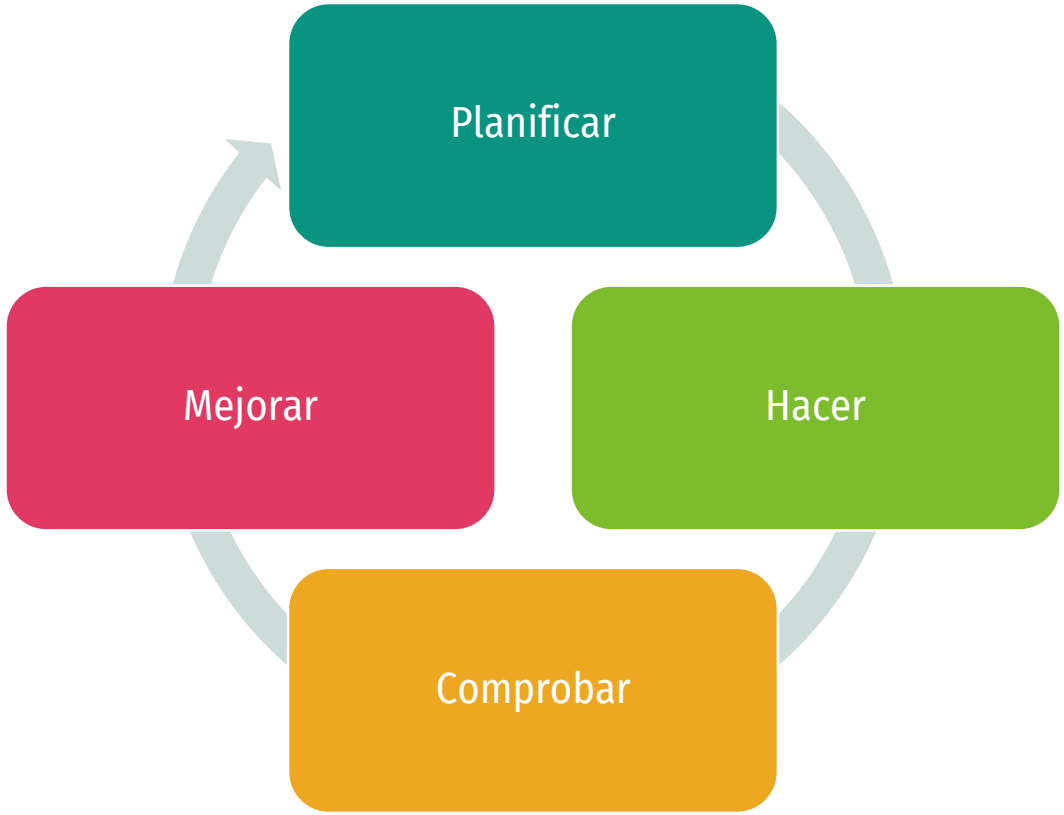
SGSI

- Conocimiento de los riesgos
- Gestión coherente, coordinada y proporcionada de los mismos que se revisa y mejora constantemente
- Formado por política, estructura organizativa, procedimientos, procesos, recursos necesarios, medidas de seguridad e indicadores
- Inversión, se ajusta a negocio

Beneficios

- Reducción de costes (prevención y respuesta ante incidentes, primas de seguros)
- Optimizar los recursos e inversiones en TI
- Protección de la organización
- Mejora de la competitividad
- Cumplimiento normativo
- Imagen corporativa

Ciclo de mejora continua



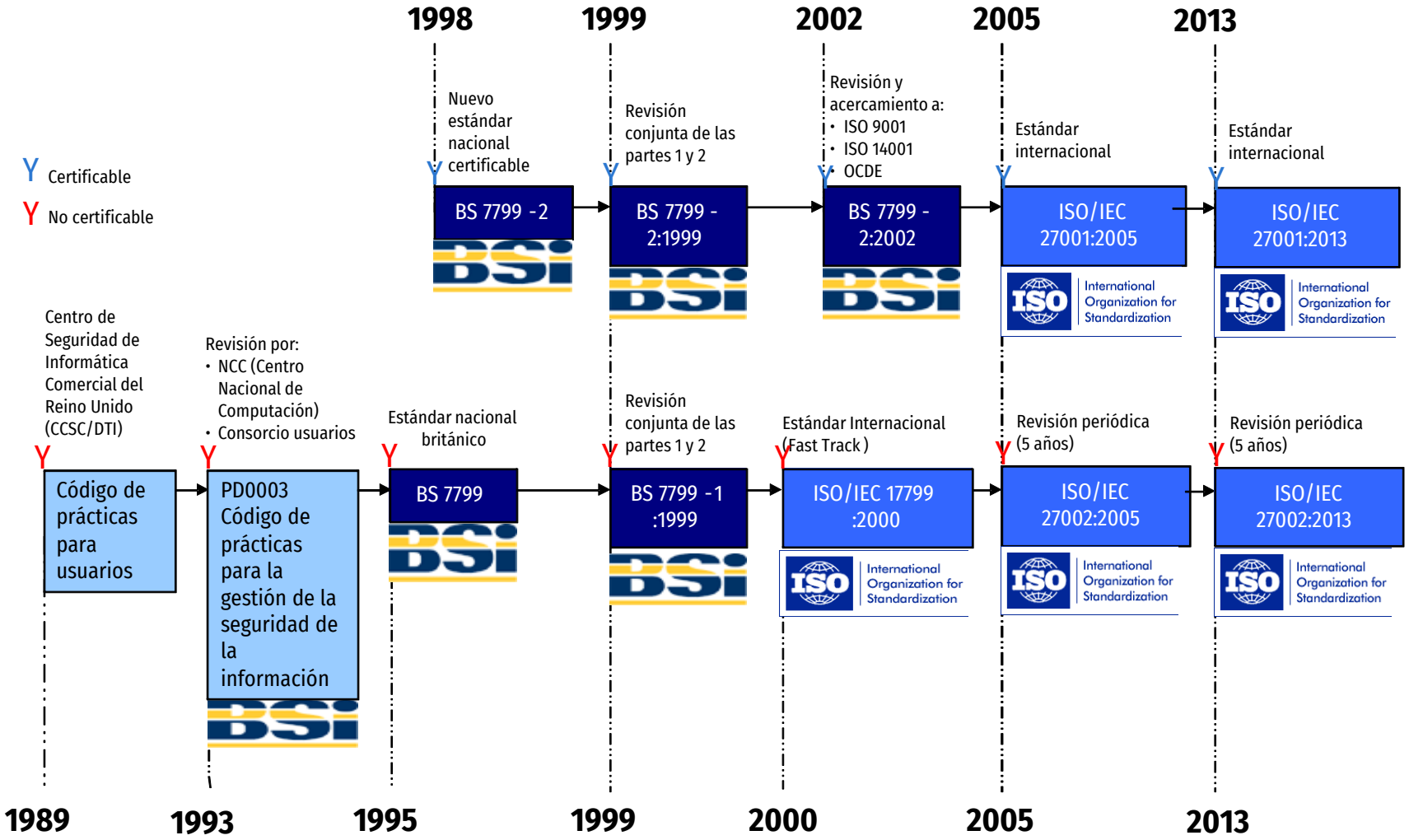
Anexo SL

- Sistemas integrados de gestión
- Términos comunes
- Desde 2011
- Coherencia, compatibilidad y sinergias
- 45 “debe” que implican un total de 84 requisitos base
- Cada norma ISO adherida le añadirá los suyos propios

Anexo SL

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora

Evolución



ISO/IEC 27001

- Requisitos ("debe") para establecer, implementar, documentar, operar, monitorizar, revisar, mantener y mejorar
- Certificable
- Independiente del tipo, tamaño o actividad
- Enfoque por procesos y mejora continua
- Medidas de seguridad (Anexo A)
- No se pueden excluir requisitos en los capítulos 4 al 10

ISO/IEC 27001

CONTEXTO
- Comprensión de la organización y contexto
- Expectativas de las partes interesadas
- Alcance
- SGSI

LIDERAZGO
- Liderazgo y compromiso
- Política
- Organización

PLANIFICACIÓN
- Acciones para tratar riesgos y oportunidades
- Objetivos y planes

SOPORTE
- Recursos
- Competencia
- Concienciación
- Comunicación
- Información documentada

MEJORA CONTINUA
- No conformidades y acciones correctivas
- Mejora continua

OPERACIÓN
- Planificación y control operacional
- Apreciación de riesgos
- Tratamiento de riesgos

EVALUACIÓN DESEMPEÑO
- Seguimiento, medición, análisis y evaluación
- Auditoría interna
- Revisión por la dirección

ISO/IEC 27002

- Medidas, también conocidos como medidas de seguridad y salvaguardas ("debería", "puede")
- Organizado en base a 14 dominios, 35 objetivos de control y 114 controles

Dominios

5. Políticas
6. Organización
7. Recursos Humanos
8. Activos
9. Acceso
10. Criptografía
11. Física y del entorno
12. Operaciones
13. Comunicaciones
14. Adquisición, desarrollo y mantenimiento

Dominios

15. Proveedores
16. Incidentes
17. Continuidad del negocio
18. Cumplimiento

Factores críticos de éxito

- Política, objetivos y actividades alineados con los objetivos de "negocio"
- Coherente con la cultura de la organización
- Apoyo de la alta dirección
- Entender los requisitos a partir de la gestión del riesgo
- Programa de concienciación, formación, educación y motivación
- Gestión eficaz de los incidentes
- Gestión eficaz de la continuidad de negocio
- Sistema de medición útil para medir la eficacia y el desempeño

Contexto de la organización

enColaboración
CONSULTORÍA COLABORATIVA

Organización

- Cuestiones internas y externas (p.e. Análisis DAFO)
- ISO 31000 (apartado 5.5)

Partes interesadas

- Clientes, personas, propiedad, proveedores y Sociedad
- Requisitos relevantes

Alcance

- Limites y aplicabilidad del SGSI
- Información documentada

SGSI

- Establecer, implementar, mantener y mejorar de manera continua

Liderazgo

enColaboración
CONSULTORÍA COLABORATIVA

Compromiso

- De la alta dirección:
  - Política y objetivos
  - Integración con los procesos
  - Asegurando recursos
  - Comunicando la importancia
  - Asegurando alcanzar los resultados previstos
  - Dirigiendo y apoyando a las personas
  - Promoviendo la mejora continua
  - Apoyando a otros líderes

Política

- Adecuada a la organización
- Marco de los objetivos
- Compromiso de cumplimiento de los requisitos
- Compromiso de mejora continua
- Información documentada
- Comunicada internamente
- Disponible para las partes interesadas

Organigrama

- Roles, responsabilidades y autoridades asignados y comunicados internamente (p.e. Propietario del activo, propietario del riesgo, Comité de Seguridad, ...)
- Asignar responsabilidad y autoridad para:
  - Asegurar la conformidad del SGSI
  - Informar a la alta dirección sobre el desempeño del SGSI

Planificación

enColaboración
CONSULTORÍA COLABORATIVA

Planificación

CONTEXTO
- Comprensión de la organización y contexto
- Expectativas de las partes interesadas
- Alcance
- SGSI

LIDERAZGO
- Liderazgo y compromiso
- Política
- Organización

PLANIFICACIÓN
- Acciones para tratar riesgos y oportunidades
- Objetivos y planes

SOPORTE
- Recursos
- Competencia
- Concienciación
- Comunicación
- Información documentada

Análisis de riesgos

- Es el diagnóstico
- Riesgos y oportunidades

Análisis de riesgos

- Inventario de activos
- Identificar amenazas (internas-externas, deliberadas-accidentales)
- Identificar vulnerabilidades
- Identificar medidas de seguridad

Análisis de riesgos

- Tener en cuenta a la organización y su contexto, y las partes interesadas
- Conseguir los resultados previstos
- Prevenir o minimizar efectos indeseados
- Lograr la mejora continua
- Planificar acciones
- Integrarlas e implementarlas en el día a día
- Evaluar su eficacia
- Definir criterios
- Obtener resultados consistentes, válidos y comparables

Apreciación de riesgos

- Identificar riesgos:
  - Pérdida de confidencialidad, integridad y disponibilidad
  - Dueños
- Analizar riesgos:
  - Posibles consecuencias
  - Probabilidad de ocurrencia
  - Niveles de riesgo
- Evaluar riesgos:
  - Comparando resultados con criterios de riesgo
  - Priorizando
- Información documentada

Activo

- Identificación:
  - Tiene valor y debe protegerse
  - Contiene o manipula información
  - Datos, hardware, software, comunicaciones, personas, proveedores, ubicaciones, equipamiento auxiliar
  - Debe tener una persona propietaria

Activo

- Inventario:
  - Identificación del activo
  - Tipo de activo
  - Descripción
  - Persona propietaria
  - Localización

  - Y:
    - Equilibrado y actualizado
    - Árbol de dependencias
    - Tan importante como el servicio/datos que soporta

Activo

- Valoración:
  - Qué valor tienen cuantitativo (dinero) o cualitativo
  - Decidir cómo se va a calcular (suma, mayor, media)
  - Criterios claros, fáciles de comprender, homogéneos y comparables
  - Decidir quiénes (representatividad y competencia)

Riesgo

- Aspecto clave, inversión en seguridad proporcional al riesgo
- Riesgo (probabilidad-consecuencias)

Gestión de riesgos

- Es el plan de trabajo

MINIMIZAR a través de medidas de seguridad

TRANSFERIR a un tercero

ELIMINAR el riesgo

ASUMIR el riesgo

Gestión de riesgos

- Seleccionar opciones (minimizar, transferir, eliminar y asumir)
- Determinar los controles (Mitigar)
- Compararlos con el anexo A
- Elaborar una "Declaración de aplicabilidad":
  - Controles necesarios
  - Justificación inclusiones
  - Implementados o no
  - Justificación exclusiones del anexo A
- Plan de tratamiento de riesgos
- Aceptar riesgos residuales por sus personas propietarias
- Información documentada

Objetivos

- En las funciones y niveles pertinentes
- Coherentes con la política
- Medibles (si es posible)
- Considerar los requisitos de seguridad y apreciación y tratamiento de riesgos
- Comunicados
- Actualizados
- Planificados (cómo, recursos, responsable, plazo, evaluación)
- Información documentada

Soporte

enColaboración
CONSULTORÍA COLABORATIVA

Recursos

- Determinar la competencia necesaria
- Asegurar la citada competencia (educación, formación y experiencia)
- Cuando sea necesario, adquirir la competencia, evaluando su eficacia
- Información documentada

Concienciación

- Personas conscientes de la política, de su contribución y de las consecuencias de no cumplir

Comunicación

- Interna y externa:
  - Contenido
  - Cuándo
  - A quién
  - Quién debe
  - Procesos (canales)

Información documentada

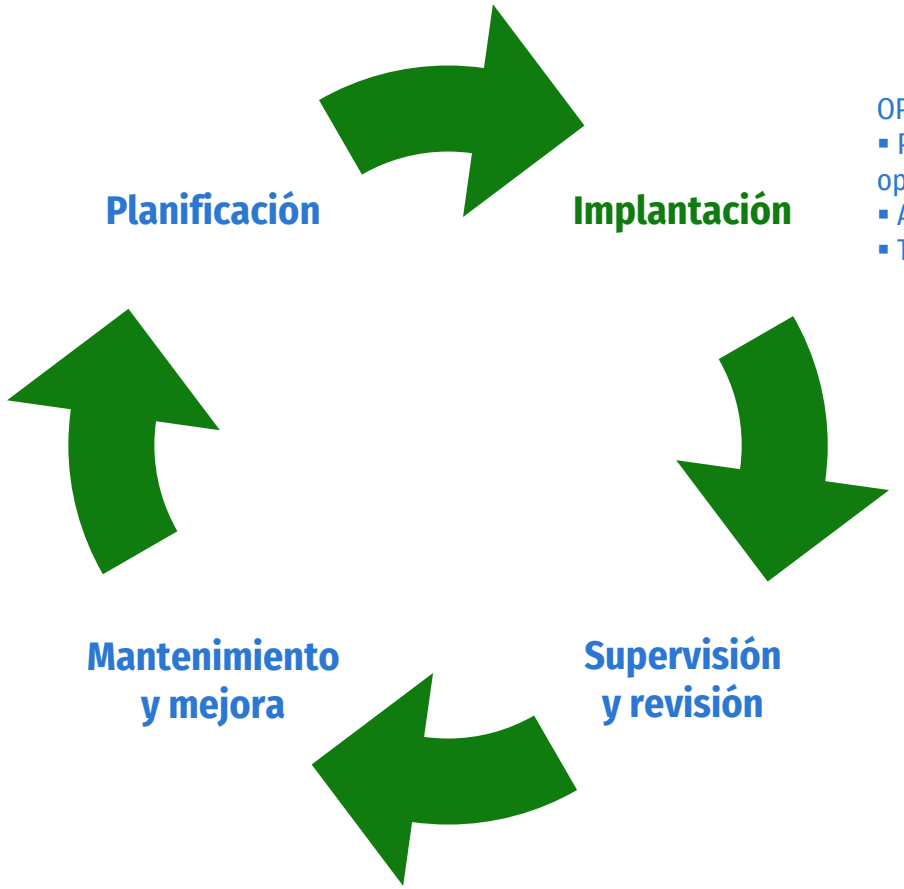
- Requerida
- Necesaria de acuerdo a la organización (tamaño, sector, complejidad, competencia de las personas)
- Actualizada, disponible, protegida
- Interna y externa

Información documentada

Operación

enColaboración
CONSULTORÍA COLABORATIVA

Operación



OPERACIÓN
- Planificación y control operacional
- Apreciación de riesgos
- Tratamiento de riesgos

Planificación y control operacional

- Planificar, implementar y controlar los procesos para cumplir requisitos
- Implementar el plan de tratamiento de riesgos
- Para alcanzar los objetivos de seguridad
- Controlar los cambios planificados
- Revisar consecuencias de cambios no previstos
- Controlar procesos contratados externamente
- Información documentada

Evaluación del desempeño

enColaboración
CONSULTORÍA COLABORATIVA

Evaluación del desempeño

EVALUACIÓN DESEMPEÑO
- Seguimiento, medición, análisis y evaluación
- Auditoría interna
- Revisión por la dirección

Seguimiento, medición, análisis y evaluación

- Evaluar el desempeño y la eficacia
- Determinar:
  - A qué es necesario hacer seguimiento y qué es necesario medir (procesos, controles, ...)
  - Métodos (resultados válidos, comparables y reproducibles)
  - Cuándo
  - Quién
- Información documentada

Auditoría interna

- Intervalos planificados
- Proporciona información de conformidad y eficacia
- Programa de auditoría (frecuencia, métodos, responsabilidades, requisitos de planificación y elaboración de informes)
- En cuenta importancia de los procesos y resultados auditorías previas.
- Criterios y alcance
- Selección de auditores (competencia, objetividad, imparcialidad)
- Informar a la alta dirección
- Información documentada

Revisión por la dirección

- Alta dirección
- A intervalos planificados
- Comprobación conveniencia, adecuación y eficacia del SGSI
- Información documentada

Revisión por la dirección

- Entradas:
  - Estado acciones de revisiones previas
  - Cambios contexto
  - Información comportamiento (tendencias):
    - No conformidades y acciones correctivas
    - Seguimiento y resultados de los indicadores
    - Resultados de auditorías
    - Cumplimiento de los objetivos de seguridad
  - Comentarios de las partes interesadas
  - Resultados de la apreciación del riesgo y del plan de tratamiento de riesgos
  - Oportunidades de mejora continua

Revisión por la dirección

- Salidas:
  - Decisiones relacionadas con las oportunidades de mejora continua
  - Cualquier cambio en el SGSI

Mejora continua

enColaboración
CONSULTORÍA COLABORATIVA

Mejora continua

MEJORA CONTINUA
- No conformidades y acciones correctivas
- Mejora continua

No conformidades y acciones correctivas

- Ante una no conformidad:
  - Acciones para controlarla
  - Acciones para corregirla
  - Afrontar las consecuencias
  - Evaluar la necesidad de acciones para eliminar las causas de la no conformidad (acción correctiva)
  - Revisar la eficacia
- Información documentada

Evento, fallo, incidente, no conformidad

- Evento: ocurrencia o cambio de un conjunto particular de circunstancias. Se puede o no clasificar como un incidente
- Fallo: algo que no funciona como debiera
- Incidente: evento, inesperado o no deseado, que tiene una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información
- No conformidad: incumplimiento de un requisito
- Información documentada

Contención, corrección, acción correctiva

- Contención: acción de control de un incidente o no conformidad
- Corrección: acción para eliminar un incidente o no conformidad detectada
- Acción correctiva: acción para eliminar la causa de una no conformidad y prevenir que vuelva a ocurrir
- Información documentada

Medidas de seguridad

enColaboración
CONSULTORÍA COLABORATIVA

Introducción

- Anexo A de la ISO/IEC 27001 y desarrolladas en la ISO/IEC 27002
- Medidas, también conocidos como medidas de seguridad y salvaguardas ("debería", "puede")
- Organizado en base a 14 dominios, 35 objetivos de control y 114 controles
- No son obligatorias
- Deben justificarse en la “Declaración de aplicabilidad”

Dominios

- Políticas
- Organización
- Recursos humanos
- Activos
- Acceso
- Criptografía
- Física y del entorno
- Operaciones
- Comunicaciones
- Adquisición, desarrollo y mantenimiento
- Proveedores
- Incidentes
- Continuidad del negocio
- Cumplimiento

Políticas

- 5.1 Dirección de la gestión de la seguridad de la información
  - 5.1.1 Políticas de seguridad de la información
  - 5.1.2 Revisión de las políticas de seguridad de la información

Organización

- 6.1 Organización interna
  - 6.1.1 Roles y responsabilidades relativas a la seguridad de la información
  - 6.1.2 Separación de tareas
  - 6.1.3 Contacto con las autoridades
  - 6.1.4 Contacto con grupos de especial interés
  - 6.1.5 Seguridad de la información en la gestión de proyectos
- 6.2 Dispositivos móviles y teletrabajo
  - 6.2.1 Política de dispositivos móviles
  - 6.2.2 Teletrabajo

Recursos humanos

- 7.1 Antes del empleo
  - 7.1.1 Investigación de antecedentes
  - 7.1.2 Términos y condiciones de contratación
- 7.2 Durante el empleo
  - 7.2.1 Responsabilidades de la Dirección
  - 7.2.2 Concienciación, formación y capacitación en seguridad de la información
  - 7.2.3 Proceso disciplinario
- 7.3 Cese del empleo y cambio de puesto de trabajo
  - 7.3.1 Terminación o cambio de responsabilidades laborales

Activos

- 8.1 Responsabilidad sobre los activos
  - 8.1.1 Inventario de activos
  - 8.1.2 Propiedad de los activos
  - 8.1.3 Uso aceptable de los activos
  - 8.1.4 Devolución de activos
- 8.2 Clasificación de la información
  - 8.2.1 Clasificación de la información
  - 8.2.2 Etiquetado de la información
  - 8.2.3 Manejo de activos
- 8.3 Manipulación de los soportes
  - 8.3.1 Gestión de soportes extraíbles
  - 8.3.2 Retirada de soportes
  - 8.3.3 Transferencia de soportes físicos

Acceso

- 9.1 Requisitos de negocio para el control de acceso
  - 9.1.1 Política de control de acceso
  - 9.1.2 Acceso a redes y servicios en red
- 9.2 Gestión del acceso de usuario
  - 9.2.1 Altas y bajas de usuarios
  - 9.2.2 Gestión de derechos de acceso de los usuarios
  - 9.2.3 Gestión de derechos de acceso especiales
  - 9.2.4 Gestión de la información secreta de autenticación de usuarios
  - 9.2.5 Revisión de derechos de acceso de usuario
  - 9.2.6 Terminación o revisión de los privilegios de acceso
- 9.3 Responsabilidades de usuario
  - 9.3.1 Uso de la información secreta de autenticación
- 9.4 Control de acceso al sistema y a las aplicaciones
  - 9.4.1 Restricción del acceso a la información
  - 9.4.2 Procedimientos seguros de inicio de sesión
  - 9.4.3 Gestión de las contraseñas de usuario
  - 9.4.4 Uso de los recursos del sistema con privilegios especiales
  - 9.4.5 Control de acceso al código fuente de los programas

Criptografía

- 10.1 Controles criptográficos
  - 10.1.1 Política de uso de los controles criptográficos
  - 10.1.2 Gestión de claves

Física y del entorno

- 11.1 Áreas seguras
  - 11.1.1 Perímetro de seguridad física
  - 11.1.2 Controles físicos de entrada
  - 11.1.3 Seguridad de oficinas, despachos e instalaciones
  - 11.1.4 Protección contra las amenazas externas y de origen ambiental
  - 11.1.5 Trabajo en áreas seguras
  - 11.1.6 Áreas de carga y descarga
- 11.2 Equipos
  - 11.2.1 Emplazamiento y protección de equipos
  - 11.2.2 Instalaciones de suministro
  - 11.2.3 Seguridad del cableado
  - 11.2.4 Mantenimiento de los equipos
  - 11.2.5 Retirada de materiales propiedad de la empresa
  - 11.2.6 Seguridad de los equipos fuera de las instalaciones
  - 11.2.7 Reutilización o retirada segura de equipos
  - 11.2.8 Equipo de usuario desatendido
  - 11.2.9 Política de puesto de trabajo despejado y pantalla limpia

Operaciones

- 12.1 Responsabilidades y procedimientos de operación
  - 12.1.1 Documentación de los procedimientos de operación
  - 12.1.2 Gestión de cambios
  - 12.1.3 Gestión de capacidades
  - 12.1.4 Separación de los entornos de desarrollo, prueba y operación
- 12.2 Protección contra el código malicioso
  - 12.2.1 Controles contra el código malicioso
- 12.3 Copias de seguridad
  - 12.3.1 Copias de seguridad de la información
- 12.4 Registro y monitorización
  - 12.4.1 Registro de eventos
  - 12.4.2 Protección de la información de los registros
  - 12.4.3 Registros de administración y operación
  - 12.4.4 Sincronización del reloj
- 12.5 Control del software en explotación
  - 12.5.1 Instalación de software en sistemas operacionales
- 12.6 Gestión de las vulnerabilidades técnicas
  - 12.6.1 Gestión de las vulnerabilidades técnicas
  - 12.6.2 Restricciones a la instalación de software
- 12.7 Consideraciones sobre la auditoría de los sistemas de información
  - 12.7.1 Controles de auditoría de los sistemas de información

Comunicaciones

- 13.1 Gestión de la seguridad de las redes
  - 13.1.1 Controles de red
  - 13.1.2 Seguridad de los servicios de red
  - 13.1.3 Segregación de redes
- 13.2 Transferencia de información
  - 13.2.1 Políticas y procedimientos de transferencia de información
  - 13.2.2 Acuerdos de transferencia de información
  - 13.2.3 Mensajería electrónica
  - 13.2.4 Acuerdos de confidencialidad o no divulgación

Adquisición, desarrollo y mantenimiento

- 14.1 Requisitos de seguridad de los sistemas de información
  - 14.1.1 Análisis y especificación de los requisitos de seguridad de la información
  - 14.1.2 Aseguramiento de los servicios de aplicaciones en las redes públicas
  - 14.1.3 Protección de las transacciones de servicios de aplicación
- 14.2 Seguridad en los procesos de desarrollo y soporte
  - 14.2.1 Política de desarrollo seguro
  - 14.2.2 Procedimientos de control de cambios en el sistema
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma
  - 14.2.4 Restricciones a los cambios en los paquetes de software
  - 14.2.5 Principios para la ingeniería de sistemas seguros
  - 14.2.6 Entorno de desarrollo seguro
  - 14.2.7 Externalización del desarrollo de software
  - 14.2.8 Pruebas de seguridad del sistema
  - 14.2.9 Pruebas de aceptación del sistema
- 14.3 Datos de prueba
  - 14.3.1 Protección de los datos de prueba

Proveedores

- 15.1 Seguridad de la información en las relaciones con proveedores
  - 15.1.1 Política de seguridad de la información en las relaciones con proveedores
  - 15.1.2 Tratamiento de la seguridad en contratos con proveedores
  - 15.1.3 Cadena de suministro de tecnologías de la información y comunicaciones
- 15.2 Gestión de los servicios prestados por terceros
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros
  - 15.2.2 Gestión del cambio en los servicios prestados por terceros

Incidentes

- 16.1 Gestión de incidentes de seguridad de la información y mejoras
  - 16.1.1 Responsabilidades y procedimientos
  - 16.1.2 Notificación de eventos de seguridad de la información
  - 16.1.3 Notificación de puntos débiles de seguridad
  - 16.1.4 Evaluación y decisión respecto de los eventos de seguridad de la información
  - 16.1.5 Respuesta a incidentes de seguridad de la información
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información
  - 16.1.7 Recopilación de evidencias

Continuidad del negocio

- 17.1 Continuidad de la seguridad de la información
  - 17.1.1 Planificación de la continuidad de la seguridad de la información
  - 17.1.2 Implementación de la continuidad de la seguridad de la información
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
- 17.2 Redundancia
  - 17.2.1 Disponibilidad de los medios de procesamiento de información

Cumplimiento

- 18.1 Cumplimiento de los requisitos legales y contractuales
  - 18.1.1 Identificación de la legislación aplicable y requisitos contractuales
  - 18.1.2 Derechos de propiedad intelectual (IPR)
  - 18.1.3 Protección de los documentos de la organización
  - 18.1.4 Protección de datos y privacidad de la información de carácter personal
  - 18.1.5 Regulación de los controles criptográficos
- 18.2 Revisiones de seguridad de la información
  - 18.2.1 Revisión independiente de la seguridad de la información
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad
  - 18.2.3 Comprobación del cumplimiento técnico

enColaboración

CONSULTORÍA COLABORATIVA

Ciberseguridad, continuidad de negocio y calidad

info@encolaboracion.net
667840499

enColaboración
CONSULTORÍA COLABORATIVA