UNIVERSIDAD NACIONAL AUTÓNOMA DE HONDURAS

UNAH
UNIVERSIDAD NACIONAL
AUTÓNOMA DE HONDURAS

IS-811, SEGURIDAD INFORMÁTICA
Primer Periodo 2025

Actividad#2

Elaborado por:

ORLIN RUDIEL AGUILAR VELASQUEZ

CUENTA:
20211030514

Catedrático:

RAFAEL EDGARDO DIAZ DEL VALLE OLIVA

Tegucigalpa M.D.C. 14 Marzo 2025

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

ÍNDICE

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

Introducción

Este reporte documenta la aplicación y evaluación de los controles de seguridad de la información según la norma ISO 27002:2013. Se establecieron subcontroles, dominios, objetivos de control y una serie de listas de verificación para evaluar el cumplimiento de la norma dentro del entorno organizacional. Al final del reporte se presenta un gráfico con la ponderación del cumplimiento de los distintos dominios.

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

1. Justificación

Esta actividad se ha incorporado para:

- Identificar desviaciones entre el estado actual del SGSI y los requisitos de la norma ISO/IEC 27002:2013.
- Priorizar acciones correctivas y mejorar el nivel de cumplimiento.

1.1 Resultados Esperados

- Identificación de brechas en los controles de seguridad.
- Elaboración de un plan de acción para cerrar las brechas identificadas.
- Mejora del nivel de madurez del SGSI.

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

2. Metodología de Implementación

Para la implementación de la norma se desarrollaron las siguientes actividades:

- Identificación de los dominios y objetivos de control según ISO 27002:2013.
- Creación de subcontroles específicos para cada dominio.
- Desarrollo de listas de verificación para evaluar el cumplimiento de cada control.
- Aplicación de encuestas y revisión documental para la validación del cumplimiento.
- Evaluación cuantitativa y cualitativa de los resultados obtenidos.

3. Principales Dominios Evaluados

Se evaluaron los siguientes dominios clave de la norma ISO 27002:2013:

➔ Políticas de Seguridad de la Información: Revisión de la existencia de políticas documentadas y su aplicación.

➔ Seguridad Organizativa de la Información: Análisis de roles y responsabilidades en la seguridad de la información.

➔ Gestión de Activos: Identificación y clasificación de activos de información.

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

- ➔ Control de Accesos: Evaluación de mecanismos de control y autenticación.
- ➔ Criptografía: Revisión del uso de cifrado en la protección de datos sensibles.
- ➔ Seguridad en Operaciones: Análisis de la gestión de cambios, copias de seguridad y monitoreo.
- ➔ Seguridad de las Comunicaciones: Verificación de medidas de protección de redes y sistemas de comunicación.
- ➔ Seguridad en Adquisición, Desarrollo y Mantenimiento de Sistemas: Evaluación de controles en el ciclo de vida del software.
- ➔ Gestión de Incidentes de Seguridad de la Información: Análisis de procedimientos para la respuesta ante incidentes.
- ➔ Continuidad del Negocio: Revisión de planes de continuidad y recuperación ante desastres.

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

4. Resultados y Evaluación

A partir de la aplicación de listas de verificación y auditorías internas, se obtuvieron los siguientes resultados:

Políticas de seguridad.	100
Aspectos organizativos de la seguridad de la información.	65
Seguridad ligada a los recursos humanos.	100
Gestión de activos.	70
Control de acceso.	95
Cifrado	100

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

Seguridad física y ambiental.	81
Seguridad en la operativa	96
Seguridad en las telecomunicaciones.	100
Adquisición, desarrollo y mantenimiento de los sistemas de información	78
Relaciones con suministradores.	59
Gestión de incidentes en la seguridad de la información.	86
Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	100

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

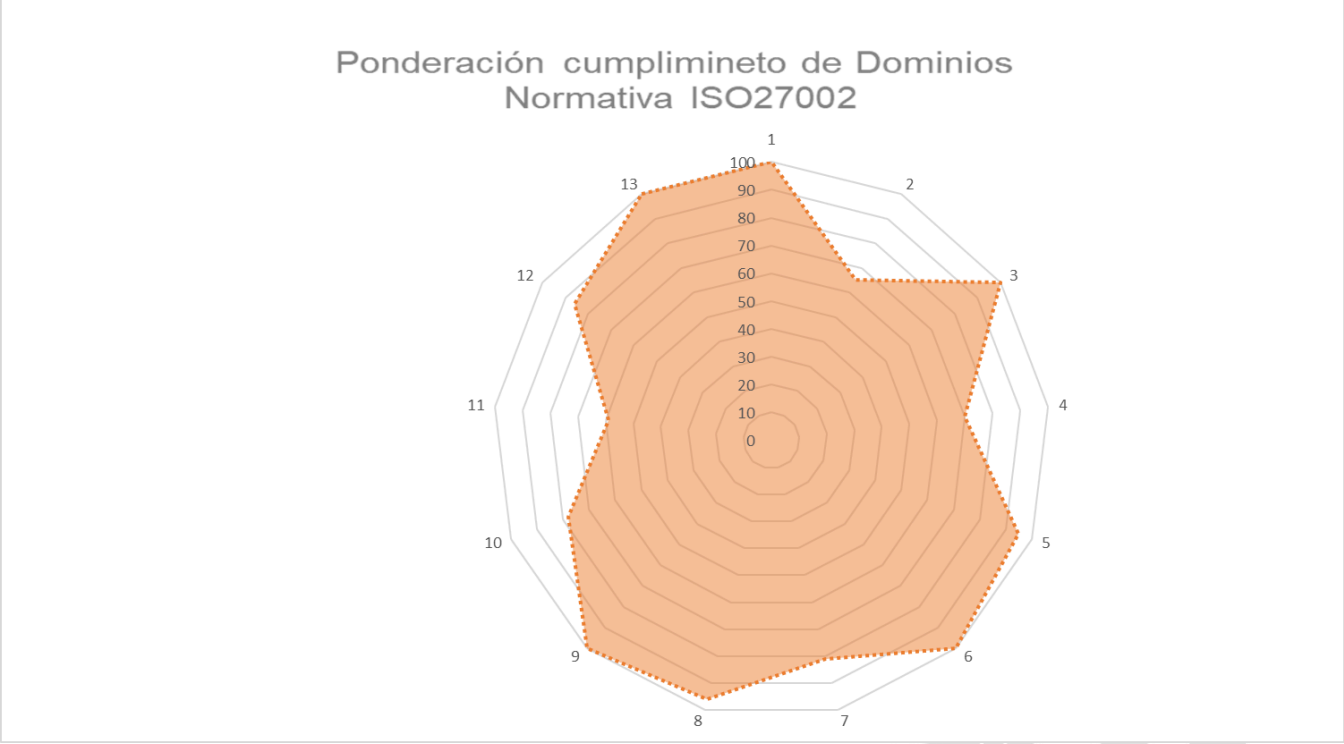
Cumplimiento.	100

Nivel de cumplimiento promedio por dominio:

- Políticas de seguridad: 100%
- Aspectos organizativos de la seguridad de la información: 65%
- Seguridad ligada a los recursos humanos: 100%
- Gestión de activos: 70%
- Control de acceso: 95%
- Cifrado: 100%
- Seguridad física y ambiental: 81%
- Seguridad en la operativa: 96%
- Seguridad en las telecomunicaciones: 100%
- Adquisición, desarrollo y mantenimiento de los sistemas de información: 78%
- Relaciones con suministradores: 59%
- Gestión de incidentes en la seguridad de la información: 86%
- "Aspectos de seguridad de la información en la gestión de la continuidad del negocio: 100%
- Cumplimiento: 100%

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

5. Gráfico de Cumplimiento



Se elaboró un gráfico que ilustra la ponderación del cumplimiento de cada dominio, permitiendo visualizar las áreas con mayor y menor nivel de conformidad con la norma ISO 27002:2013.

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

Plan de Contingencia y Continuidad del Negocio para el Departamento de TI

Alcance

Este plan aplica a todos los sistemas, infraestructuras, aplicaciones y servicios gestionados por el departamento de TI, incluyendo:

- Servidores y centros de datos.
- Redes y comunicaciones.
- Aplicaciones críticas para el negocio.
- Datos y backups.
- Equipos de trabajo y personal de TI.

Equipo de Respuesta y Roles

- Coordinador de Continuidad de TI: Responsable de supervisar la ejecución del plan.
- Equipo de Soporte Técnico: Encargado de la recuperación de sistemas y aplicaciones.
- Equipo de Seguridad Informática: Gestiona incidentes de ciberseguridad y protege los activos digitales.
- Comunicaciones: Responsable de informar a los stakeholders internos y externos.

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

Identificación de Riesgos

Realizar un análisis de riesgos para identificar posibles amenazas, como:

- Fallos de hardware o software.
- Ciberataques (ransomware, phishing, etc.).
- Cortes de energía o desastres naturales.
- Errores humanos o sabotaje interno.

Análisis de Impacto al Negocio (BIA)

- Identificar sistemas y servicios críticos.
- Establecer el tiempo máximo aceptable de inactividad (RTO, Recovery Time Objective).
- Definir la pérdida de datos aceptable (RPO, Recovery Point Objective).

Estrategias de Continuidad

- Redundancia de sistemas: Implementar servidores y redes redundantes.
- Backups: Realizar copias de seguridad periódicas y almacenarlas en ubicaciones seguras (on-site y off-site).

- Infraestructura en la nube: Utilizar servicios cloud para garantizar la disponibilidad.

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

- Planes de recuperación de desastres (DRP): Establecer procedimientos para recuperar sistemas críticos.

Procedimientos de Respuesta a Incidentes

1. Detección y Notificación:
    - Monitorear sistemas para detectar anomalías.
    - Notificar al equipo de respuesta inmediatamente.
2. Evaluación:
    - Determinar la gravedad y el alcance del incidente.
3. Contención:
    - Aislar sistemas afectados para evitar la propagación.
4. Recuperación:
    - Restaurar servicios utilizando backups y sistemas redundantes.
5. Comunicación:
    - Informar a los stakeholders sobre el estado del incidente y las acciones tomadas.

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

Roles y Responsabilidades

Rol	Responsabilidad
Gerente de TI	Coordinar la recuperación y la continuidad.
Administrador de Redes	Restablecer la infraestructura de comunicación.
Especialista en Seguridad	Identificar y mitigar amenazas.
Equipo de Soporte	Restaurar sistemas y asistir a usuarios.

Pruebas y Simulacros

- Realizar pruebas periódicas del plan de continuidad (ejercicios de recuperación de desastres).
- Simular escenarios de ciberataques, cortes de energía o fallos de hardware.
- Documentar las lecciones aprendidas y actualizar el plan según sea necesario.

Capacitación y Concientización

- Capacitar al personal de TI en procedimientos de continuidad y respuesta a incidentes.
- Concientizar a los empleados sobre buenas prácticas de seguridad informática.

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

Revisión y Actualización del Plan

- Revisar el plan anualmente o después de incidentes significativos.
- Actualizar el plan para reflejar cambios en la infraestructura de TI, nuevos riesgos o regulaciones.

Recursos Necesarios

- Herramientas de monitoreo y detección de incidentes.
- Soluciones de backup y recuperación.
- Infraestructura redundante (servidores, redes, energía).
- Presupuesto para implementar y mantener el plan.

Documentación y Registros

- Mantener documentación actualizada del plan, incluyendo procedimientos, contactos y diagramas de infraestructura.
- Registrar todos los incidentes y acciones tomadas para futuras revisiones.

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

6. Conclusiones y Recomendaciones

- Se identificaron oportunidades de mejora en la gestión de activos y criptografía, dado que presentan los menores niveles de cumplimiento.
- Se recomienda implementar un plan de acción para mejorar la seguridad en el desarrollo de sistemas y la gestión de activos.
- El cumplimiento general de la organización con ISO 27002:2013 es aceptable, pero se requieren ajustes en políticas y controles específicos.
- Se sugiere realizar auditorías periódicas y capacitaciones para fortalecer la cultura de seguridad en la organización.

Prof. Rafael E. Diaz del Valle O.
mail: rafael.diazdelvalle@unah.edu.hn

7. Anexos

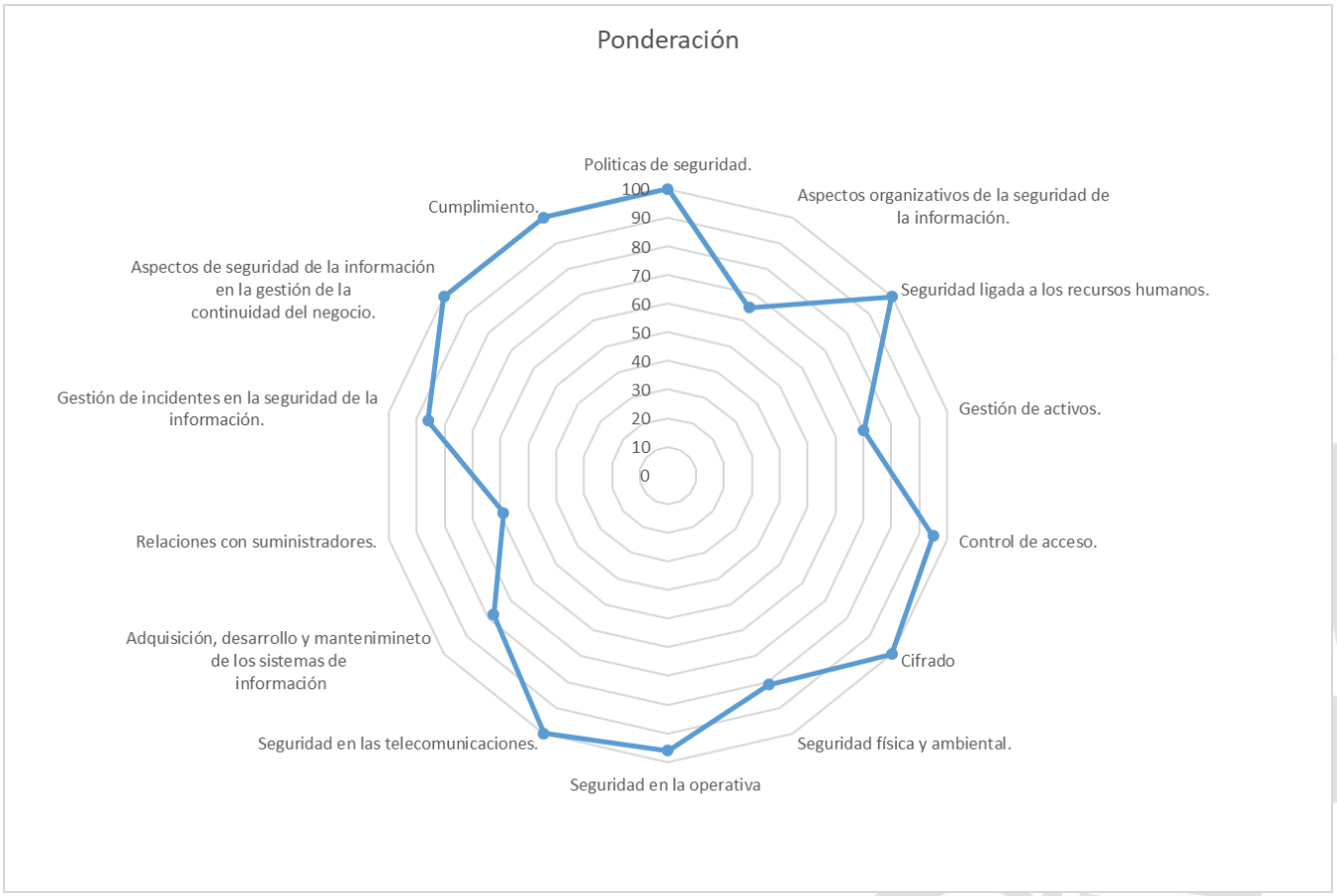


Gráfico de ponderación de cumplimiento.

Este reporte refleja los esfuerzos realizados en la evaluación de la seguridad de la información basados en ISO 27002:2013 y proporciona una guía clara para futuras mejoras en la organización.