Centro de Especializaciones Noeder

Diploma de Especialización Internacional

IMPLEMENTADOR Y AUDITOR SEGURIDAD DE LA INFORMACIÓN - ISO 27001 Y CONTINUIDAD DEL NEGOCIO - ISO 22301

MÓDULO II

IMPLEMENTACIÓN DE LA NORMA ISO 27001

CLASE 05

Mg. Ing. Julio Pereyra Rosales

1. Evaluación de desempeño

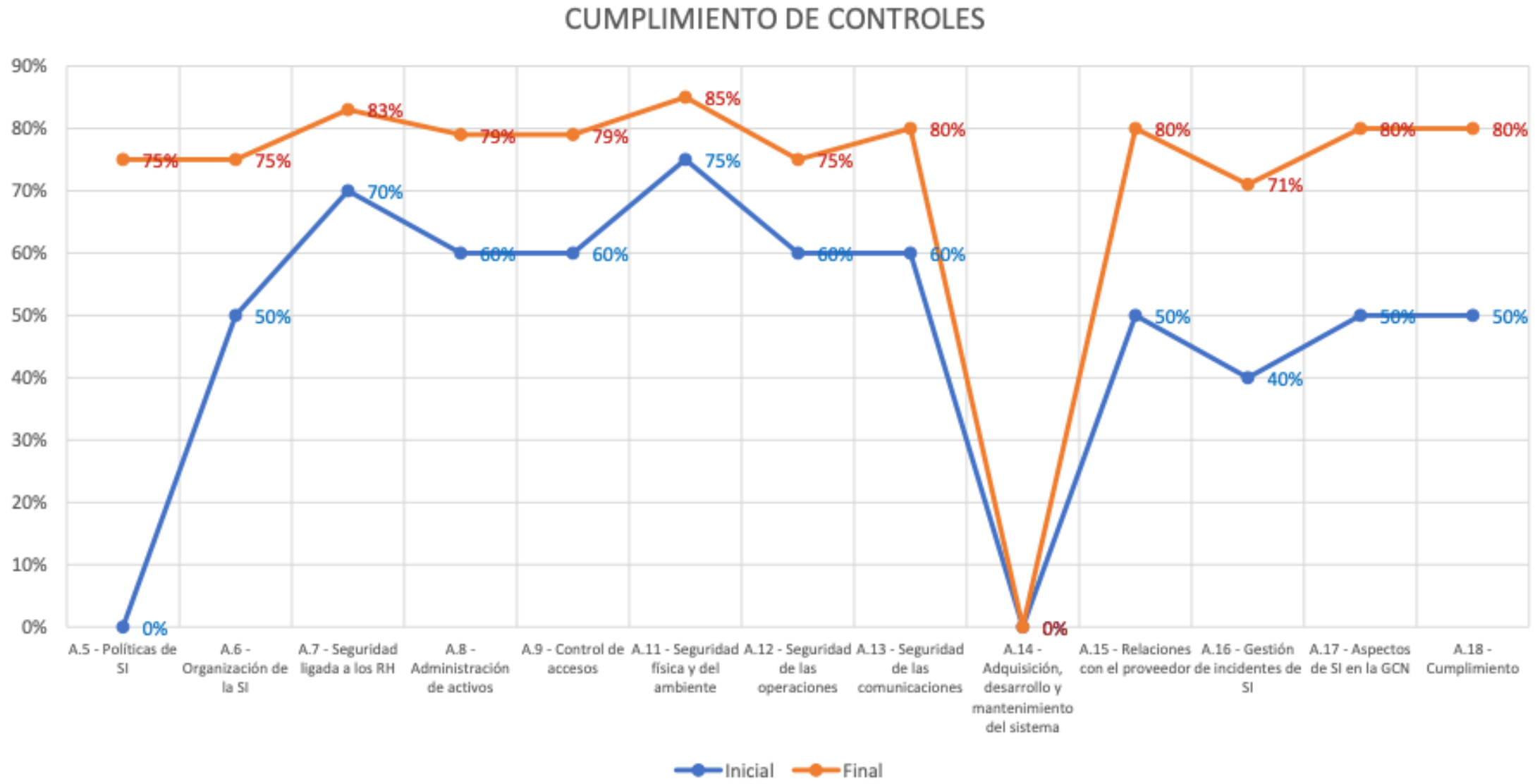
9. Evaluación de desempeño

9.1 Monitoreo, medición, análisis y evaluación

Política	Objetivo	Indicadores	Meta	Formato / Fuente de datos	Frecuencia de medición	Responsable
Preservar la confidencialidad, integridad y disponibilidad de la información de nuestras partes interesadas.	Controlar los riegos de información en los proceso de la empresa	RIESGOS SI. Control operacional: (N° acciones ejecutadas del Control Operacional del RIEGOS SI/ Total de acciones) x 100%	70%	Matriz de RIESGOS SI	Mensual	Procesos SIG/ Business Parte
	Controlar las amenazas en la seguridad de la información	% de ataques informáticos que impidieron la prestación de algún servicio	0	Registros de incidencias	Mensual	Procesos SIG/ Business Parte

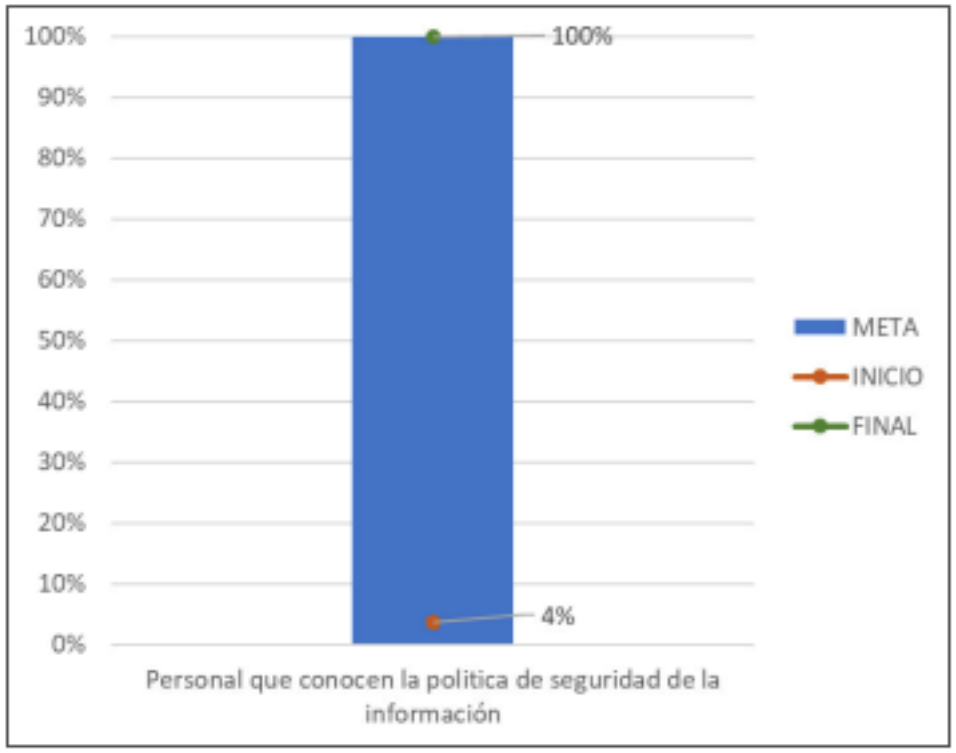
9. Evaluación de desempeño

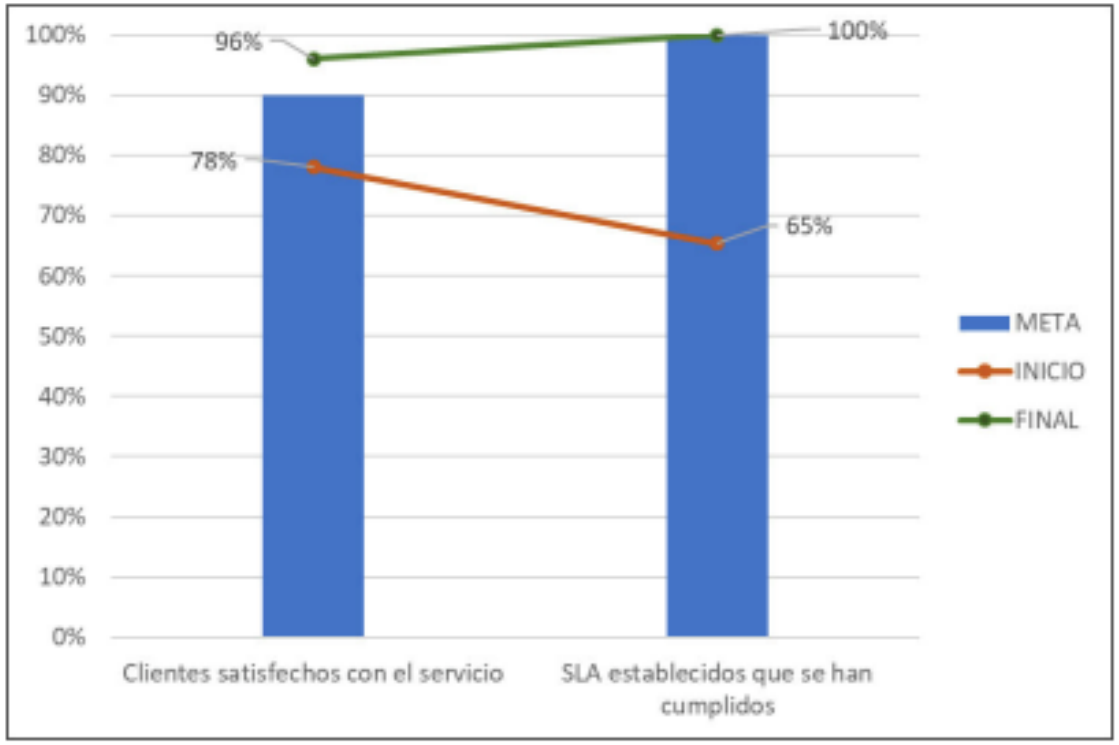
9.1 Monitoreo, medición, análisis y evaluación



9. Evaluación de desempeño

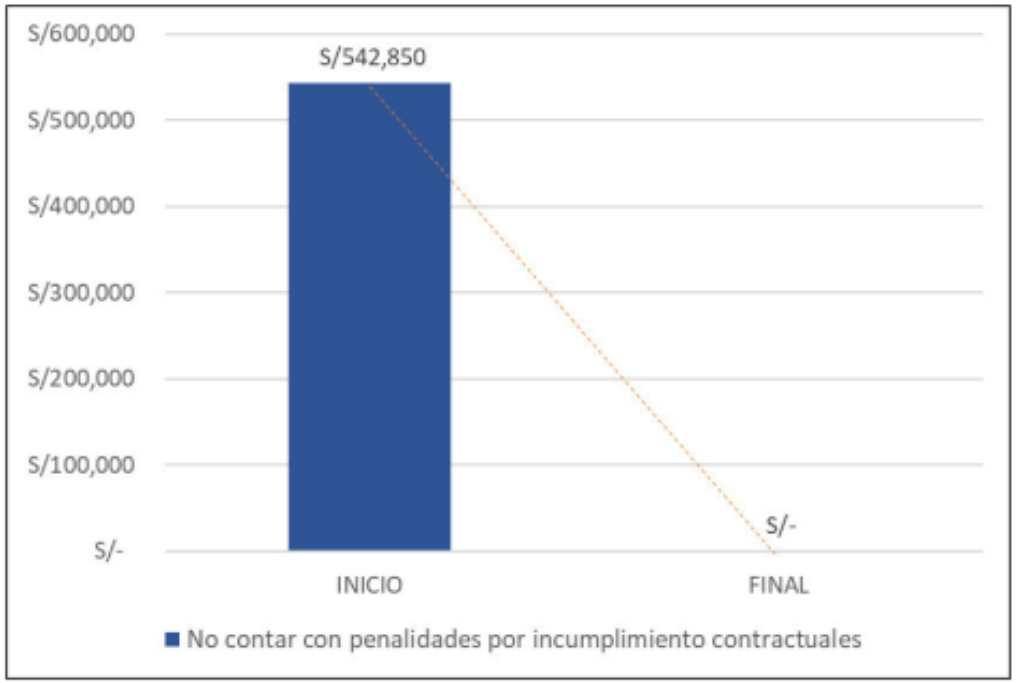
9.1 Monitoreo, medición, análisis y evaluación

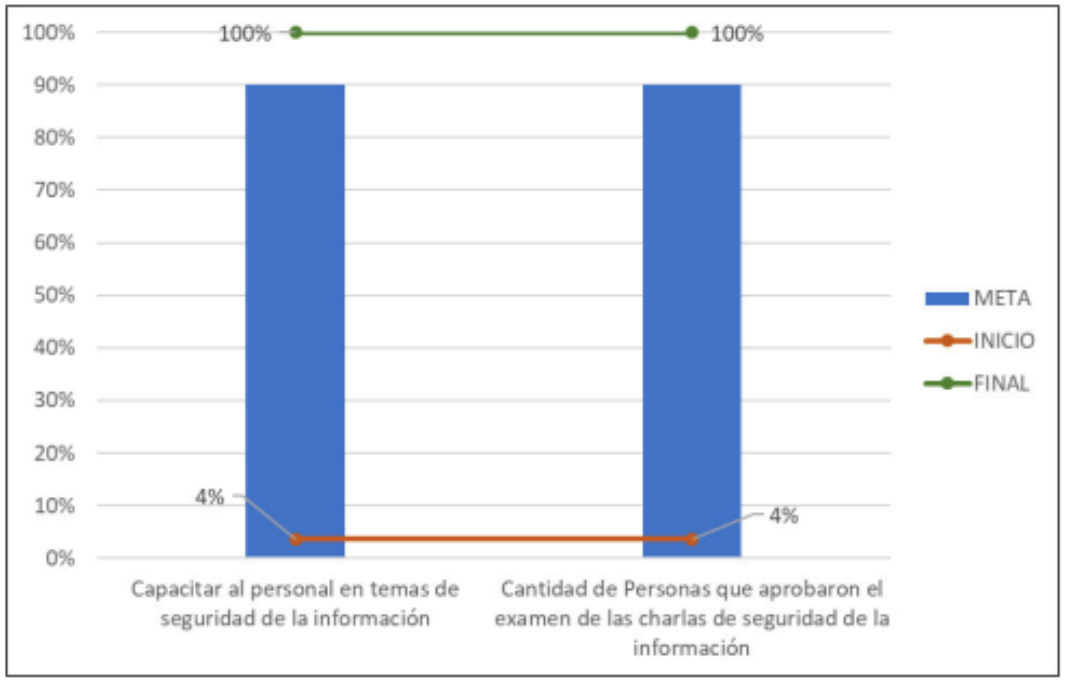




9. Evaluación de desempeño

9.1 Monitoreo, medición, análisis y evaluación





9. Evaluación de Desempeño

9.2 Auditoría Interna

PLAN DE AUDITORÍA INTERNA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2022	
Auditor Líder: Julio Pereyra **Equipo Auditor**: No aplica **Especialista**: No aplica **Auditor en Entrenamiento**: No aplica	**Fecha de Inicio**: 22.8.2024 **Fecha de Finalización:** 22.8.2024 **Día de Informe**: 26.8.2024 **Norma a auditar**: ISO 27001:2022

Objetivos de la Auditoría:

- Verificar el cumplimiento de los requisitos de las Normas ISO 27001:2015
- Verificar el cumplimiento de los requisitos legales
- Verificar el cumplimiento de los requisitos inherentes al servicio

Metodología: Entrevista y muestreo

Criterios de auditoría: Documentación del sistema de gestión de seguridad de la información, regulatorio, normativo y propios de la organización; a través de muestreo, observación y entrevista.

Alcance:

Consultoría y outsourcing en aplicaciones informáticas empresariales: implementación, desarrollo de software, outsourcing, soporte y mesa de ayuda.

9. Evaluación de Desempeño

9.2 Auditoría Interna

Horario	Proceso/ Área a Auditar	Requisitos de las Normas Aplicables	Responsable del área auditada	Auditor
		ISO 27001:2022		
09:00 a 09:15	Reunión de apertura			Julio Pereyra
09:15 a 10:00	Gestión Estratégica	4.1,4.2,4.3,4.4,5.1,5.2,5.3,6.1,7.1,9.1, 9.3,10.1,10.2	Gerente General	Julio Pereyra
10:00 a 11:00	Sistema de gestión de la seguridad de la información	4.1,4.2,4.3,4.4,5.2,5.3,6.1,6.2,6.3, 7.3, 7.4,7.5,9.1, 9.2,10.1,10.2	Responsables del SIG	Julio Pereyra
11:00 a 12:00				
12:00 a 12:30	Gestión de innovación y marketing	4.4,5.2,5.3,6.1,6.3, 7.3, 7.4,7.5,8.1,8.2,8.3, 9.1,10.1,10.2	Gerente de Innovación y marketing	Julio Pereyra
12:30 a 13:00	Gestión comercial	4.4,5.2,5.3,6.1,6.3, 7.3, 7.4,7.5,8.1,8.2, 8.3,9.1,10.1,10.2	Gerente Comercial	Julio Pereyra
13:00 a 14:00	Almuerzo			
14:00 a 14:30	Gestión de Telecomunicaciones	4.4,5.2,5.3,6.1,6.3, 7.3, 7.4,7.5,8.1,8.2, 9.1,10.1,10.2	Gerente de Consultoría	Julio Pereyra
14:30 a 15:00	Gestion de Eventos y Respaldo	4.4,5.2,5.3,6.1,6.3, 7.3, 7.4,7.5,8.1,8.2,8.3, 9.1,10.1,10.2	Gerente de Desarrollo	Julio Pereyra
15:00 a 15:30	Logística	4.4,5.2,5.3,6.1,6.3, 7.1, 7.3, 7.4,7.5,8.1, 8.2,8.39.1,10.1,10.2	Gerente de Administraciónn y Trasformación Digital	Julio Pereyra
15:30 a 16:00	Gestión de Mesa de Ayuda	4.4,5.2,5.3,6.1,6.3, 7.1, 7.3, 7.4,7.5,8.1,8.2.8.3, 9.1,10.1,10.2		
16:00 a 17:00	Talento Humano	4.4,5.2,5.3,6.1,6.3, 7.1, 7.2,7.3, 7.4,7.5,8.1,8.2,8.3 , 9.1,10.1,10.2	Gerente de Talento Humano	Julio Pereyra
17:00 a 17:15	Consolidación de hallazgos			
17:15 a 17:45	Reunión de cierre			

Auditor Líder

Gerente

9. Evaluación de Desempeño

9.3 Revisión por la dirección

Entradas

a. Estado de las Revisiones por la Dirección previas

b. Cambios en cuestiones internas y externas

c. Cambios en necesidades y expectativas de P.I.

d. Información sobre el comportamiento de la S.I.:

Tendencias:

- No conformidades y acciones correctivas.
- Seguimiento y resultados de la evaluación de la medición.
- Resultado de auditorías
- Cumplimiento de los objetivos de S.I.

e. Comentarios de las partes interesadas

f. Resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos.

g. Oportunidades de mejora

Resultados

Oportunidades de mejoramiento continuo

Cualquier necesidad de cambio en el SGSI

9. Evaluación de Desempeño

9.3 Revisión por la dirección

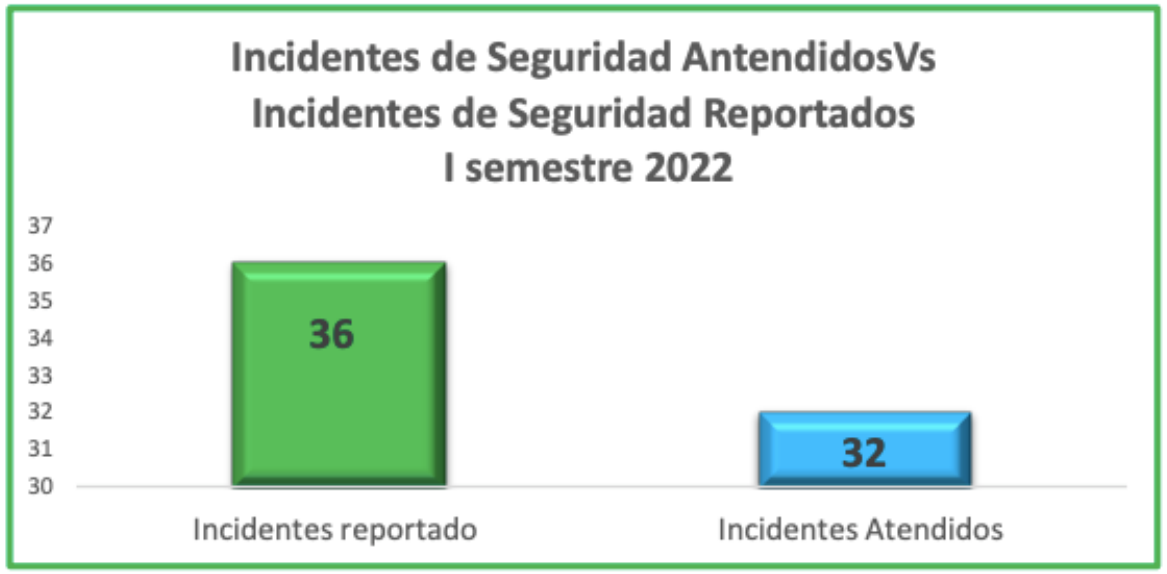


Tabla 1 Incidentes de Seguridad Atendidos Vs Reportados

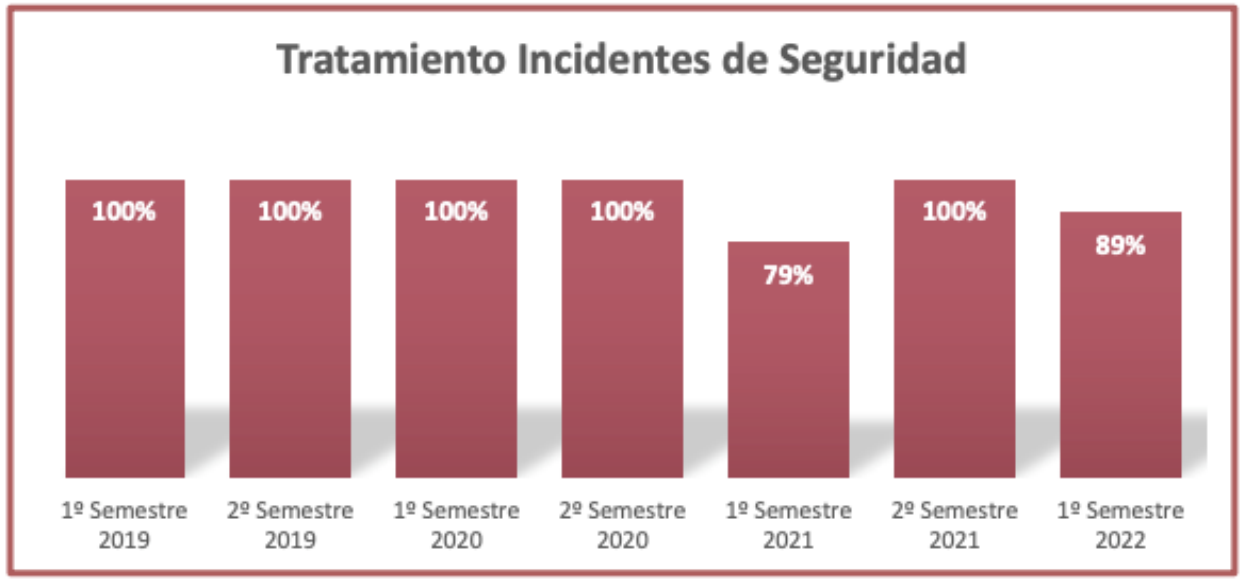


Tabla2 Histórico de incidentes y peticiones

9. Evaluación de Desempeño

9.3 Revisión por la dirección

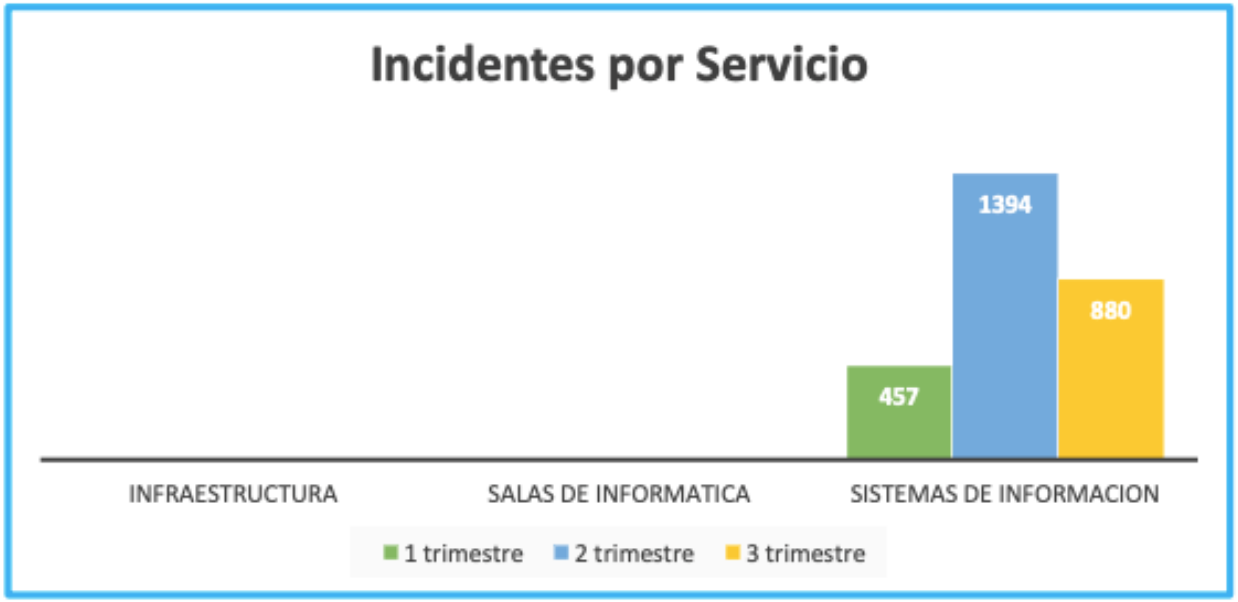


Tabla5 Incidentes por servicio

Tabla7 Histórico Satisfacción de usuarios

9. Evaluación de Desempeño

9.3 Revisión por la dirección

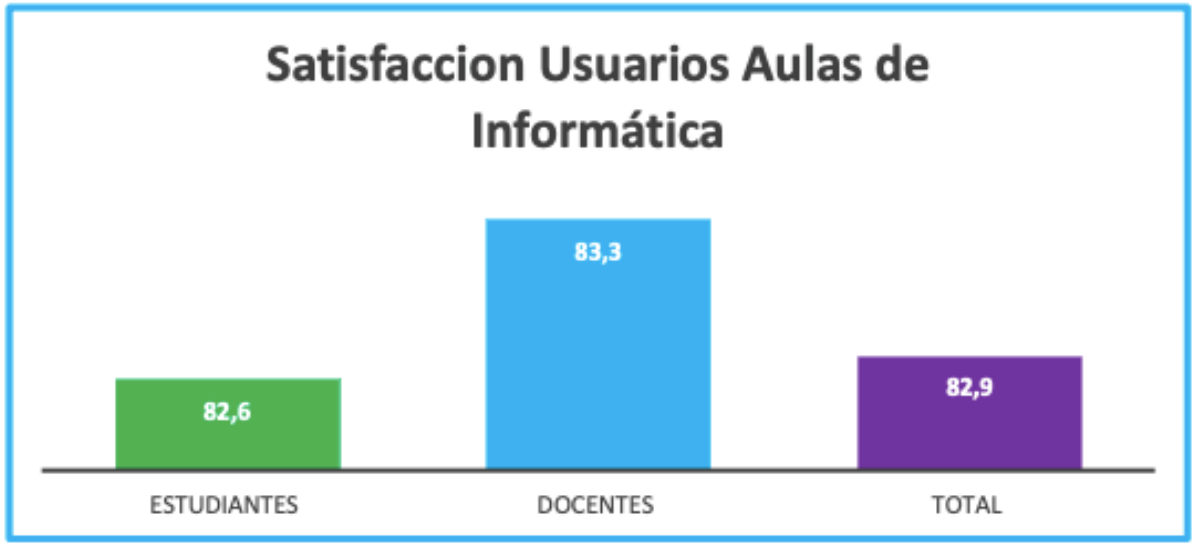


Tabla 8 Satisfacción de usuarios Aulas de Informática (los datos se encuentran en %)

No	Nombre del indicador	Frecuencia	Meta	1º Semestre 2021	2º Semestre 2021	1º Semestre 2022	2º Semestre 2022
1	Cumplimiento de los acuerdos de nivel de servicio	Semestral	80%	100%	100%	100%	
2	Satisfacción de usuarios de los acuerdos informáticos	Semestral	80%	100%	100%	100%	

Tabla 9 Resultados Indicadores

9. Evaluación de Desempeño

9.3 Revisión por la dirección

	# Activos	INACTIVOS	ACTIVOS	OBSOLETOS	CRITICOS
HARDWARE	1557	0	1557	0	1
SOFTWARE	149	5	138	2	8
INFORMACIÓN	3	0	3	0	1
SERVICIOS	33	0	33	0	0
RECURSO HUMANO	47	4	43	0	0
TOTAL ACTIVOS	**1789**	**9**	**1778**	**2**	**10**

9. Evaluación de Desempeño

9.3 Revisión por la dirección

En 2022, A partir de la identificación de activos de información, se trabajó en el análisis e identificación de riesgos de los diez (10) activos de información que fueron valorados como ALTO, siguiendo el procedimiento A-RI-P35, por lo tanto, se realizó Plan de Tratamiento a algunos de estos activos los cuales son:

- Servidor LDAP (2020)
- Servidor SIIUPS (2020)
- A-RI-P35-F01 (2022)
- Mesa de Servicio Institucional (2022)

Respecto a los activos de información aplicativo GOOBI y esquema GOOBI, no se realizó plan de tratamiento, debido a que se determinó que se asume el riesgo de acuerdo al análisis y evaluación de riesgos realizada.

Como resultado, se obtiene un nivel de riesgo Alta y cinco niveles de riesgo Moderada.

Se destaca que los controles implementados a partir de la operación del SGSI, han eliminado el número de riesgos que se tenían en extremo; esto evidencia que los controles han sido efectivos permitiendo disminuir los niveles de los riesgos residuales.

9. Evaluación de Desempeño

9.3 Revisión por la dirección

En cuanto a los cambios que pueden afectar al Sistema de Gestión de Servicios de TI y Sistema de Gestión de Seguridad de la Información se identificaron los siguientes:

- La desvinculación o no continuidad de personal en la Dirección afecta negativamente la prestación de los servicios, generando atrasos o el incumplimiento de los acuerdos de niveles de servicio con los usuarios.

- La vinculación de personal no capacitado o sin experiencia en programación o manejo de herramientas avanzadas como SPRING, ANGULAR u ORACLE, genera demora en el desarrollo de aplicaciones y cumplimiento de condiciones seguras en el desarrollo.

- Por falta de interés por parte de la alta dirección en el cumplimiento de las normas ISO 20000-1 e ISO 27001 se pueden presentar

    - La poca toma de conciencia de la comunidad
    - Desacato a los requisitos de la norma
    - Incumplimiento a los requisitos de la norma
    - Fallas en los procedimientos
    - Afectación en la prestación de los servicios
    - Daño en la infraestructura tecnológica y no contar con el respaldo requerido
    - Perdida de le certificación
    - Detrimento patrimonial por la pérdida de las certificaciones de las nomas internaciones ocasionando una mala imagen a nivel regional y nacional de la universidad

- Por falta de recursos no se pueda dar cumplimiento a la ejecución de los proyectos que se encuentran estipulados en el Plan de Desarrollo Institucional.

- Respaldo de personal indispensable para el desarrollo de procedimientos críticos de la Dirección

2. Mejora continua

10.Mejora

10.1 Mejora Continua

	OPORTUNIDAD DE MEJORA	OBJETIVO	ORIGEN	CONVENIENCIA					¿Es conveniente?	Sede o filiales	Acciones a tomar	RESPONSABLE DE LA OPORTUNIDAD DE MEJORA	¿Es ADECUADA la Oportunidad de Mejora? (avances en campo)	¿Es EFICAZ la Oportunidad de Mejora? (en base al Objetivo)	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
				Objetivos SGSI	Partes Interesad	Impacto en los riesgos	Mejora Continua	Total																	
1	Adecuar la Matriz de Riesgos del SGSI a TODAS las Filiales.	Reducir la detección de no conformidades y riesgos del SGSI en las filiales	Auditoría externa 2023	2	2	2	3	9	Si	Cusco, Arequipa, Lima, Huancayo	1. Actualizar el AMFE 2. Difundir el AMFE actualizado	Coordinador del SGSI	1. Se identificó todos los riesgos por cada sede / filial. 2. Los trabajadores participaron en los cursos de capacitación	A través de una auditoria seguimiento (vía remota), se verificó que todas las sedes y filiales identificaron sus riesgoS											
2	Revisar la factibilidad de cambiar las metas, ya que las actules se mantienen en permanente cumplimiento en los últmos 6 meses.	Aumentar el compromiso y la toma de conciencia en el personal, sobre la mejora continua	Auditoría externa 2023	3	1	2	3	9	Si	Cusco, Arequipa, Lima, Huancayo	1. Generar el informe de resultados 2. Realizar la planificación en función a los datos obtenidos	Responsables de procesos y filiales	Se realizaron reuniones de revisión de nueva metas. Para el caso del proceso de gestión de accesos, se ha reducido la meta de índice de eventos de 10 a 5 (medido a nivel mensual)	Se mantienen las nuevas metas cumplidas y en proceso de mejora para el periodo 2024											
3	Integrar / reducir el número de instructivos en la operación, ya que a la fecha existe 134 documentos en calidad de instrucciones / instructivos de trabajo.	Mejorar la trazabilidad de las actividades operativas en el SGSI	Revisión por la Dirección Dic 2023	2	2	1	3	8	Si	Cusco, Arequipa, Lima, Huancayo	Los requisitos documentarios son los mínimos requeridos y se plasma así en el procedimento.	Responsables de procesos y filiales	De 134 documentos (instructivos) se ha reducido a 77. Los cuales son especificamente operativo y cn su respectiva integración de formatos / registros.	Se ha verificado que se han reducido las no conformidades por causa de poca disponibilidad a los documentos y el personal mantiene conocimiento mas oportuno											
4	Revisar la velocidad y disponibilidad de los sistemas de información, se indicó que en ocasiones el sistema es lento. (Esto podría afectar a la gestión de indicadores , gestión de pedidos de emergencia y el FODA).	Mantener eficaz el desarrollo de la información y registros del SIG.	Sugerencias del personal	1	1	2	3	7	No	No aplica	No aplica	No aplica	No aplica	No aplica											

10. Mejora

10.2 Conformidades y acciones correctivas

Origen de la No Conformidad		Proceso / Lugar en donde se detectó la No Conformidad
Reclamo		Operaciones () Gestión de Activos () Ingeniería () Gestión de Mesa de Ayuda (x) Gestión de Telecomunicaciones ()
Salida No Conforme		
Incumplimiento de Procedimientos Misionales		
Incumplimiento de Procedimientos del SGSI		
Incumplimiento de Metas de Indicadores		**Persona quien detecta la No Conformidad**
Seguimiento y Evaluación de Proveedores		Coordinador del SGSI
Auditoria Interna	x	
Auditoria Externa		
Otros :		

DECRIPCIÓN DE LA NO CONFORMIDAD

Incumplimiento:

No se almacena la documentación del proceso de gestión de Mesa de Ayuda.

Evidencia:

Se solicitó al responsable del proceso los siguientes registros:

a. REG-SGSI-004 Registro de eventos
b. REG-SGSI-005 Registro de Seguimiento de eventos
c. REG-SGSI-008 Reporte de Evento Mensuales

De acuerdo con el REG-SGSI-002 Lista de Registro se menciona que los respectivos registros (descritos en líneas arriba) se deben almacenar a 12 meses, 18 meses y 6 meses respectivamente. Se solicitó las siguientes evidencias:

a. REG-SGSI-004 Registro de eventos (del periodo: diciembre 2023 y enero 2024). No se presentó evidencias.
b. REG-SGSI-005 Registro de Seguimiento de eventos (del periodo: noviembre 2023 y marzo 2024). No se presentó evidencias.
c. REG-SGSI-008 Reporte de Evento Mensuales (del periodo: enero 2024 y febrero 2024). No se presentó evidencias

REQUISITO: 7.5.3 Control de la información documentada (acápite d)

Generado por : Irwin Damasco Gogin **Responsable de Área :** Aquiles Zine

ACCIÓN (ES) INMEDIATA (S) (acción que elimina la no conformidad)

Búsqueda y almacenamiento de los registros solicitados. Ordenamiento integral del almacenamiento de los registros.

Responsable (s) de Acción (es) Inmediata (s): Aquiles Zapata

EVALUACIÓN DE NECESIDAD DE ACCIÓN CORRECTIVA

¿Es necesaria la implementación de acciones correctivas?

Si (x) No () ¿por qué?

Los registros solicitados son de alto impacto para el seguimiento de los resultados del sistema de gestión de seguridad de la información (gestión de eventos)

Responsable (s) de la Evaluación: Aquiles Zapata

ANÁLISIS DE CAUSAS (describir las principales causas de la no conformidad)

1. **¿Por qué no se ubicaron los registros seleccionados?**

   Respuesta: Se evidencio que no existen criterios de orden para el almacenamiento físico de registros.

2. **¿Por qué no existen criterios de orden para el almacenamiento de registros?**

   Respuesta: No se ha priorizado la identificación de métodos de almacenamientos físicos.

3. **¿Por qué no se ha priorizado la identificación de métodos de almacenamientos físicos?**

   Respuesta: Se desconoce metodología de almacenamiento físico de registros

Responsable (s) del Análisis de Causa (s) : Aquiles Zine / Gonzalo López

ACCIONES CORRECTIVAS

	Descripción de Acción Correctiva	Responsable	Plazo	Plazo de Eficacia
1.	Implementar la metodología de orden y limpieza en relación a las 5 S.	Karla Mullén	Inmediato	3.5.2024

VERIFICACIÓN DE LA EFICACIA DE ACCIONES CORRECTIVAS (llenado por el Coordinador del SGSI)

Verificación: Al día 3.05.2024, se realizó la revisión de los siguientes registros en el proceso de gestión de Mesa de Ayuda:

a. REG-SGSI-004 Registro de eventos (del periodo: octubre 2023). Se evidencia los registros.
b. REG-SGSI-005 Registro de Seguimiento de eventos (del periodo: febrero 2024). Se evidencia los registros.
c. REG-SGSI-008 Reporte de Evento Mensuales (del periodo: marzo2024). Se evidencia los registros.

La acción correctiva implementada ha sido eficaz.

Fecha: 3.5.2024.

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón