INSTITUCIÓN UNIVERSITARIA
MAYOR DE CARTAGENA

Informe al Diagnóstico del Modelo de Seguridad y Privacidad de la Información

-2024-

Oficina de Soporte y Desarrollo Tecnológico
10 de agosto de 2024

1. Introducción

El presente informe tiene como objetivo presentar los resultados del diagnóstico realizado al modelo de seguridad y privacidad de la información de la Institución Universitaria Mayor de Cartagena. Esta evaluación se llevó a cabo con el fin de conocer el estado actual de madurez institucional en materia de protección de la información, identificar posibles riesgos y proponer oportunidades de mejora.

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

El futuro digital es de todos MinTIC

ENTIDAD EVALUADA	Institucion Universitaria Mayor de Cartagena
FECHAS DE EVALUACIÓN	08/05/2024
CONTACTO	3022316764
ELABORADO POR	Pedro Camargo

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	84	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	86	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	62	100	GESTIONADO
A.9	CONTROL DE ACCESO	99	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	80	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	28	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	97	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	97	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	93	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	90	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	94	100	OPTIMIZADO
A.18	CUMPLIMIENTO	94	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		85	100	OPTIMIZADO

2. Objetivo del Diagnóstico

Evaluar el nivel de cumplimiento de la Institución Universitaria Mayor de Cartagena respecto a los estándares y buenas prácticas en seguridad y privacidad de la información, en el marco de la protección de los activos digitales, la integridad de los datos y el cumplimiento de la normativa vigente.

3. Metodología

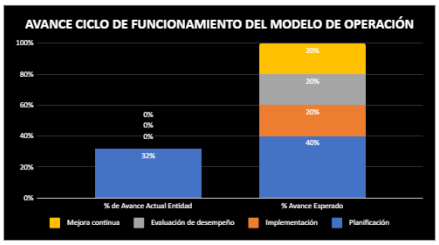
El diagnóstico fue realizado con base en los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), considerando los siguientes dominios clave:

- Gobierno de la Seguridad de la Información
- Gestión de Riesgos
- Protección de Activos de Información
- Control de Accesos
- Concienciación y Capacitación
- Gestión de Incidentes de Seguridad
- Cumplimiento Normativo y Legal

Se utilizaron encuestas, entrevistas a responsables de áreas clave, revisión documental, y análisis de controles implementados. La evaluación se basó en una escala porcentual, en la cual el 100% representa el cumplimiento total del modelo.

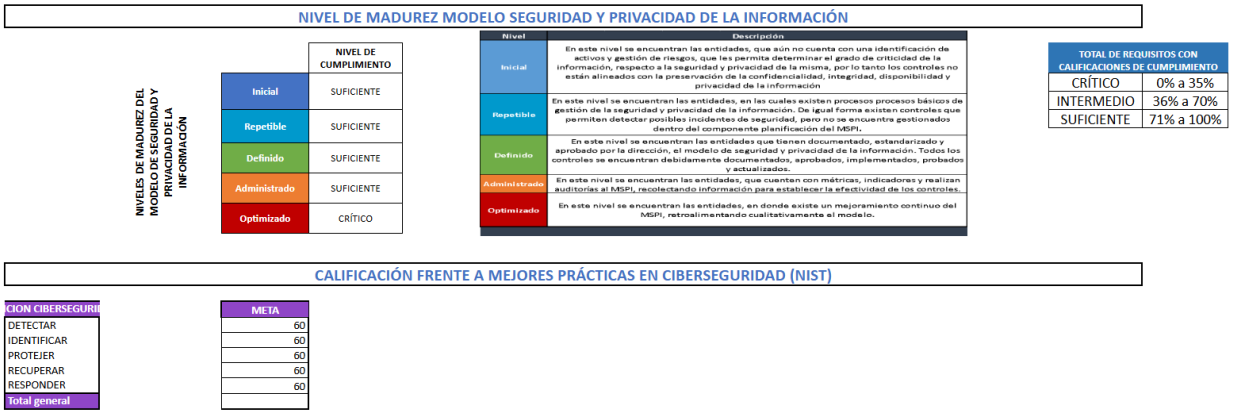
AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

AVANCE PHVA		
COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
Planificación	32%	40%
Implementación	0%	20%
Evaluación de desempeño	0%	20%
Mejora continua	0%	20%
TOTAL	**32%**	**100%**



4. Resultados Generales

La Institución Universitaria Mayor de Cartagena obtuvo una **calificación global de 85%**, lo cual indica un **alto nivel de cumplimiento** en la implementación del modelo de seguridad y privacidad de la información. Este resultado refleja un compromiso institucional significativo con la gestión segura de la información.



NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	SUFICIENTE
Definido	SUFICIENTE
Administrado	SUFICIENTE
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuentan con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

CION CIBERSEGURI	META
DETECTAR	60
IDENTIFICAR	60
PROTEJER	60
RECUPERAR	60
RESPONDER	60
Total general	

5. Resumen de Resultados por Dominio:

Dominio Evaluado	Nivel de Cumplimiento
Gobierno de la Seguridad	90%
Gestión de Riesgos	80%
Protección de Activos de Información	85%
Control de Accesos	88%
Concienciación y Capacitación	75%
Gestión de Incidentes de Seguridad	83%
Cumplimiento Normativo y Legal	92%

6. Fortalezas Identificadas

- Existencia de políticas actualizadas de seguridad de la información.
- Alta cobertura de controles de acceso a sistemas críticos.
- Procesos establecidos para la gestión de incidentes.
- Compromiso del equipo directivo con el gobierno de la seguridad.

7. Oportunidades de Mejora

- **Capacitación Continua:** Fortalecer los programas de concienciación para todos los niveles de la institución, con especial enfoque en estudiantes y docentes.
- **Gestión de Riesgos:** Implementar una metodología más robusta para la identificación, análisis y tratamiento de riesgos tecnológicos emergentes.
- **Monitoreo Permanente:** Incrementar la frecuencia de auditorías internas y controles proactivos para anticiparse a incidentes de seguridad.

8. Recomendaciones

- Establecer un **Plan de Mejora Continua** alineado con los hallazgos del diagnóstico.
- Actualizar el **Inventario de Activos de Información** periódicamente.
- Implementar campañas institucionales permanentes sobre el uso seguro de la información.
- Mantener actualizada la matriz de riesgos y planes de contingencia ante eventos críticos.

9. Conclusiones

La Institución Universitaria Mayor de Cartagena ha logrado avances significativos en la implementación de medidas de seguridad y privacidad de la información, alcanzando una calificación destacada del 85%. No obstante, se recomienda mantener una cultura organizacional orientada a la mejora continua, dado el contexto cambiante de los riesgos cibernéticos y los requerimientos normativos.