ROLES Y RESPONSABILIDADES SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborado por:

Revisado por:

Aprobado por:

PU Seguridad Digital

Director Gestión de Recursos
Tecnológicos

Rector(a)

ROLES Y RESPONSABILIDADES SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Proceso: Gestión de Recursos Tecnológicos			
Código 1.04.30.103.D.11	Versión 09	Emisión 09-04-2024	Página 2 de 9

1. OBJETIVO

Proponer la estructura de Gobierno de Seguridad que facilitará la emisión de políticas y el establecimiento de estándares, así como seguimiento al Sistema de Gestión de Seguridad de la Información que se aplicará en la Institución Universitaria Colegio Mayor del Cauca.

2. ALCANCE

El documento aplica para el Sistema de Gestión de Seguridad de la Información. Inicia con la definición de la estructura institucional y finaliza con la asignación de responsabilidades.

3. DEFINICIONES

Activo: Cualquier cosa que tenga valor para la organización.

Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Incidente de seguridad de la información: Un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

ROLES Y RESPONSABILIDADES SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Proceso: Gestión de Recursos Tecnológicos			
Código 1.04.30.103.D.11	Versión 09	Emisión 09-04-2024	Página 3 de 9

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

SGSI: Sistema de Gestión de Seguridad de la Información.

4. DOCUMENTOS Y REGISTROS

Los documentos y registros utilizados en el procedimiento se relacionan a continuación:

DOCUMENTOS Y REGISTROS	CÓDIGO
Política Seguridad y privacidad	1.0.D.16
Plan de tratamiento de riesgos de seguridad de la información.	1.04.30.103.D.13

5. ORGANIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Se establece la siguiente estructura institucional para el desarrollo, evaluación y mejora del SGSI:

5.1. COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Comité de Seguridad es un grupo asesor que tiene como objetivo armonizar el funcionamiento y los propósitos del sistema de seguridad de la información; sus responsabilidades son:

- ✓ Comunicar a los funcionarios, contratistas y/o partes interesadas que participan en actividades de forma directa o indirecta con la institución, la importancia de satisfacer los requisitos de seguridad y privacidad de la información.

ROLES Y RESPONSABILIDADES SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Proceso: Gestión de Recursos Tecnológicos			
Código 1.04.30.103.D.11	Versión 09	Emisión 09-04-2024	Página 4 de 9

- ✓ Establecer y modificar la política y los objetivos de seguridad de la información, orientados a la estrategia de la Institución, formulada en el plan estratégico, y los requisitos legales o contractuales.
- ✓ Evaluar periódicamente el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI).
- ✓ Asegurar la disponibilidad de recursos necesarios para la implementación del SGSI.
- ✓ Priorizar proyectos o iniciativas de seguridad cuando se presenten riesgos o se perciba posibilidad de incumplimiento regulatorio.
- ✓ Definir, revisar y aprobar los objetivos de seguridad y los indicadores de SGSI.
- ✓ Aprobar la elaboración, modificación y anulación de documentos del SGSI.
- ✓ Aprobar los documentos y actualizaciones que se vayan generando como complemento al SGSI.
- ✓ Oficializar el documento "Declaración de Aplicabilidad", verificar su aplicación y soportar los proyectos de mejora que de esta declaración se deriven.

El Comité de Seguridad debe contar con miembros que tengan un amplio conocimiento de la institución, así como posición de liderazgo quienes ayuden a dinamizar el SGSI. El Comité de Seguridad hace parte del Comité Institucional de Gestión y Desempeño.

5.2. QUORUM DEL COMITÉ

El Comité de Seguridad de la Información sesionará con la participación de 3 de sus integrantes y decidirá con el voto favorable de la mitad más uno de los participantes.

En caso de que la decisión del Comité presente empate se vuelve a llevar a una próxima reunión hasta que se logren los votos para la aprobación, dejando constancia en la respectiva acta.

5.3. PARTICIPANTES Y RESPONSABILIDADES

Se proponen los siguientes integrantes del comité de seguridad de la información:

ROLES Y RESPONSABILIDADES SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Proceso: Gestión de Recursos Tecnológicos			
Código 1.04.30.103.D.11	Versión 09	Emisión 09-04-2024	Página 5 de 9

5.3.1. RECTOR

El Rector, debe apoyar activamente la seguridad de la información al interior de la Institución con un rumbo claro, alineado a los objetivos estratégicos. Este compromiso se verá reflejado a través de las siguientes responsabilidades:

- ✓ Creación de un Comité de Seguridad de la Información donde sea participe y se logre un mejoramiento continuo en la protección de los activos críticos, ciber activos e información sensible.
- ✓ Asignación de un responsable en seguridad de la información (líder o responsable de seguridad de la información).
- ✓ Aprobación del alcance, política, objetivos y políticas específicas de seguridad de la información.
- ✓ Realizar la revisión por la dirección del SGSI.
- ✓ Asignar los recursos necesarios a los procesos para la implementación y mantenimiento del SGSI.
- ✓ Apoyar para que se cumpla con las políticas de seguridad de la información la interior de la Institución.

5.3.2. LÍDER O RESPONSABLE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

El líder o responsable de seguridad de la información tendrá las siguientes responsabilidades:

- ✓ Diseñar y presentar para aprobación, políticas, normas y procedimientos que fortalezcan la seguridad privacidad de la información, y someterlos a decisión del Comité de Seguridad, realizando la implementación y seguimiento de los mismos.
- ✓ Coordinar la gestión de riesgos de acuerdo con la periodicidad establecida, incluyendo la actualización de amenazas, vulnerabilidades y riesgos en los activos críticos, ciberactivos e información sensible.
- ✓ Asegurar que se establecen, mantienen e implementan los procesos necesarios para el desarrollo del Sistema de gestión de seguridad de la información, SGSI.
- ✓ Presentar los informes del SGSI, incluyendo las principales novedades, iniciativas e incidentes de seguridad de la información, así como las lecciones aprendidas.

ROLES Y RESPONSABILIDADES SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Proceso: Gestión de Recursos Tecnológicos			
Código 1.04.30.103.D.11	Versión 09	Emisión 09-04-2024	Página 6 de 9

- ✓ Coordinar las reuniones del Comité de Seguridad de la Información y/o convocar a Comité extraordinario cuando las circunstancias o uno de sus miembros lo requieran, con motivo de riesgo mayor para la institución.
- ✓ Velar por el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.
- ✓ Informar a la Alta Dirección sobre el desempeño del Sistema de Gestión de Seguridad de la Información y de cualquier necesidad de mejora.
- ✓ Estar en contacto con grupos especiales en temas de seguridad de la información, con el fin de estar documentado acerca de los nuevos métodos y herramientas de ataque.
- ✓ Coordinar las actividades correspondientes a la gestión de Incidentes de Seguridad de la información.
- ✓ Desarrollar, mantener y comunicar las políticas, estándares y guías de seguridad de la información.
- ✓ Identificar y reportar riesgos, eventos o incidentes de seguridad a través de los canales definidos.
- ✓ Realizar el proceso de gestión de incidentes de seguridad que se presenten en la institución.
- ✓ Soportar a los líderes de proceso en el análisis de riesgos de seguridad y privacidad de la información y consolidar los planes de manejo de los mismos.
- ✓ Recibir capacitaciones en seguridad de la información.
- ✓ Elaborar las campañas de sensibilización, capacitación y socialización del SGSI.
- ✓ Coordinar junto con el líder de gestión de Recursos Tecnológicos:
 - El fortalecimiento de la seguridad (hardening) de Servidores, Enrutadores y Switches involucrados en la red.
 - La correcta configuración y efectividad de las herramientas de seguridad instaladas.
 - La realización de pruebas de penetración y Ethical Hacking sobre la infraestructura de la institución.

ROLES Y RESPONSABILIDADES SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Proceso: Gestión de Recursos Tecnológicos			
Código 1.04.30.103.D.11	Versión 09	Emisión 09-04-2024	Página 7 de 9

5.3.3. LÍDER GESTIÓN DE RECURSOS TECNOLÓGICOS

El líder de gestión de Gestión de Recursos Tecnológicos en pro de garantizar el correcto uso y administración de los recursos informáticos de la institución y aseguramiento de la información debe:

- ✓ Actualizar el listado de activos de información, así como su valoración.
- ✓ Planear y ejecutar el plan de mantenimiento en los equipos de cómputo e infraestructura de la institución.
- ✓ Participar en la elaboración del cronograma de capacitación del SGSI en la institución.
- ✓ Implementar las mejoras identificadas en el SGSI que estén relacionado hardware, software, canales de comunicaciones de datos o infraestructura TI.
- ✓ Reportar riesgos, eventos o incidentes de seguridad a través de los canales definidos.
- ✓ Gestionar recursos para el SGSI.

5.3.4. LÍDERES DE PROCESO

Los líderes de procesos actúan como el “responsables de los activos de información” para todos los aspectos de seguridad de la información y tienen las siguientes responsabilidades:

- ✓ Verificar los informes de auditorías realizadas al SGSI y velar porque se apliquen las acciones correctivas identificadas, así como las recomendaciones entregadas por los auditores.
- ✓ Determinar opciones de mejora en seguridad de la información en los procesos a cargo.

6. PROPIETARIO DEL ACTIVO

Es el funcionario que tiene bajo su custodia (o se le ha asignado) un activo. Sus responsabilidades son:

ROLES Y RESPONSABILIDADES SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Proceso: Gestión de Recursos Tecnológicos			
Código 1.04.30.103.D.11	Versión 09	Emisión 09-04-2024	Página 8 de 9

- Acompañamiento para la clasificación del activo de información
- Identificación de riesgos relacionados con el activo.
- Verificar el cumplimiento de la política de seguridad y privacidad de la información.
- Respaldo permanente de la información del activo bajo su cargo.
- Implementar y cumplir con los controles relacionado con las funciones asignadas.
- Reporte inmediato de incidentes de seguridad de la información

7. DOCUMENTOS DE REFERENCIA

No aplica

8. ANEXOS

No Aplica

9. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIO REALIZADO
2 de diciembre de 2019	Se actualizó estructura del documento, título de documento, y se validaron responsabilidades por perfiles.
16 de junio de 2021	Se actualiza código del documento según nueva TRD. Se actualiza el documento eliminando requisitos ISO 27000. Se actualiza documentos y registros de referencia.
21 de septiembre del 2021	Se actualizó título del apartado 5.3.2
23 de junio del 2022	Se realizó revisión de la política en todos sus aspectos con el equipo de seguridad de la información donde se considera que actualmente no requiere modificación relevante a la fecha evaluada. Se realizó actualización de cargo de Asesor TIC a Director de Gestión de

**ROLES Y RESPONSABILIDADES
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Proceso: Gestión de Recursos Tecnológicos

Código 1.04.30.103.D.11	Versión 09	Emisión 09-04-2024	Página 9 de 9
-----------------------------------	----------------------	------------------------------	-------------------------

	Recursos Tecnológicos. Se actualiza el nombre del proceso, que ahora corresponde al macro proceso, de apoyo según el nuevo mapa de procesos.
6 de septiembre de 2022	Se actualiza código del documento según TRD.
13 de octubre de 2022	Se actualiza el documento según revisión realizada por el proceso de Gestión de Recursos Tecnológicos.
21 de junio del 2023	Actualización de responsabilidades del apartado 5.3.1. Actualización de responsabilidades del apartado 5.3.2. Actualización de responsabilidades del apartado 5.3.3. Actualización de responsabilidades del apartado 5.3.4. Actualización de responsabilidades del apartado 6. Revisión validada por el equipo de Seguridad de la Información.
9 de abril de 2024	Se actualiza código del documento según TRD aprobadas por el Consejo Departamental de Archivos. Se actualiza código de documentos de referencia.

COPIA CONTROLADA