MANUAL DE ROLES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE SISTEMAS

CONTENIDO

INTRODUCCIÓN

El presente manual pretende establecer los roles y responsabilidades que contribuyan con la confidencialidad, integridad y disponibilidad de la información al interior de la Universidad ya que es un aspecto clave para el correcto funcionamiento del Modelo de Seguridad de la Información (MSPI) el cual hace parte de la Política de Gobierno Digital y debe ser implementado en todas las entidades públicas.

1. OBJETO

Definir los roles y responsabilidades que componen la estructura organizacional para la gestión de la seguridad y privacidad de la información en la Universidad de los Llanos.

2. ALCANCE

El alcance del presente manual está establecido para los roles que aquí se describen y el cumplimiento de las responsabilidades asignadas.

3. REFERENCIAS NORMATIVAS

- **Guía Roles y Responsabilidades,** Ministerio de Tecnologías de la Información y las Comunicaciones.
- **Anexo 1: Modelo de Seguridad y Privacidad de la Información,** Ministerio de Tecnologías de la Información y las Comunicaciones.

4. DEFINICIONES

- **Activo de Información**: En relación con la seguridad de la información, se entiende como cualquier información o elementos tecnológicos que tienen relación directa con la información (sistemas de información, servicios tecnológicos, archivos físicos, archivos digitales, infraestructura tecnológica incluso personas) que tenga valor para la organización.
- **Clasificación**: Agrupar o categorizar los activos en términos de información pública, reservada y clasificada.
- **Confidencialidad**: Propiedad de la información que determina que esté disponible a personas autorizadas.
- **Criticidad**: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Disponibilidad**: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.
- **Evento de seguridad:** Cualquier ocurrencia identificada en un sistema de información, servicio o estado de la red que indica una posible infracción en la seguridad de la información, en la política o fallo en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

- **Incidente de seguridad:** Es la materialización de un evento de seguridad que afecta la integridad, disponibilidad o confidencialidad de la información.

- **Información**: Se entiende por información todo aquel conjunto de datos organizados que posean valor para la institución, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.).

- **Integridad**: Propiedad de la información que hace referencia a su exactitud y completitud.

- **MSPI**: Modelo de seguridad y privacidad de la información.

- **Política**: Declaración de alto nivel que describe la posición de la organización sobre un tema específico.

- **Riesgo de seguridad de la información:** Es el potencial de que una o varias amenazas se materialicen causando daños a uno o un grupo de activos de información.

- **Usuario**: Cualquier persona, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Universidad, para propósitos propios de su labor.

5. CONDICIONES GENERALES

6. CONTENIDO

6.1. Roles y responsabilidades

A continuación, se describen los roles que intervienen en la gestión de la seguridad y privacidad de la información:

a. Alta dirección (Consejo Superior-Rectoría)

Garantizar la disponibilidad de recursos para diseñar, implementar, mantener y mejorar la seguridad y privacidad de la información en la Universidad.

b. Comité Institucional de Gestión y Desempeño Institucional

Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:

- Aprobar los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad y privacidad de la información.

- Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la Universidad.

- Aprobar acciones y mejores prácticas que contribuyan a la implementación del MSPI.

- Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.

- Revisar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.

- Realizar seguimiento sobre el avance de las iniciativas o proyectos de seguridad de la información.

- Gestionar la asignación de personal y recursos necesarios para la implementación de planes y actividades relacionadas con seguridad de la información, en los Planes Operativos Institucionales, Plan Anual de Contrataciones y otros.

- Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

c. *Oficina de Sistemas*

Responsable de coordinar las acciones que el Comité Institucional de Gestión y Desempeño establezca en materia de Seguridad y privacidad de la Información ~~de~~ así como impulsar la implementación y cumplimiento de las políticas.

- Fomentar la implementación de la Política de Gobierno Digital.

- Coordinar la gestión de seguridad de la información y ciberseguridad, que incluye identificación y cumplimiento de los requisitos legales, gestión del riesgo de seguridad de la información, elaboración y actualización de documentos que soporten el MSPI, generación de indicadores, formulación de la política de seguridad de la información, y aplicación de mejoras.

- Formular los objetivos y estrategia de seguridad de la información y ciberseguridad, asegurando que esté alineada con las necesidades de la Universidad.

- Coordinar la realización del análisis, identificación, evaluación y control de riesgos y su respectivo tratamiento.

- Definir la implementación de programas de formación y toma de conciencia relacionados con seguridad de la información.

- Validar la definición y establecimiento de los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.

- Promover el desarrollo de iniciativas sobre seguridad de la información.

d. *Responsable de Seguridad de la Información*

La responsabilidad será liderar la implementación del Modelo de seguridad y privacidad de la información en la Universidad y tendrá las siguientes responsabilidades:

- Asesorar a la Universidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información para la Universidad de conformidad con la regulación vigente.

- Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI.

- Realizar el acompañamiento correspondiente en materia de seguridad y privacidad de la información a cada uno de los procesos que así lo requieran.

- Liderar y brindar acompañamiento a los procesos de la Universidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.

- Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información.

- Definir e implementar las estrategias de sensibilización y difusión de temas de seguridad y privacidad de la información.

- Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información.

- Poner en conocimiento de las dependencias con competencia funcional cuando se detecten irregularidades, incidentes o prácticas que atenten contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.

e. ***Oficina Asesora de Planeación***

- Asesorar a las áreas para realizar los cambios a que haya lugar en los procesos, procedimientos, instructivos y formatos para ajustarlos y alinearlos con el Sistema Integrado de Gestión – SIG.

- Acompañar y orientar sobre la metodología para la identificación, análisis, calificación y valoración del riesgo de seguridad de la información.

- Liderar la elaboración y consolidación del mapa de riesgos de seguridad de la información.

f. Oficina Asesora Jurídica

- Representar jurídicamente a la Universidad ante las autoridades competentes, en asuntos relacionados con seguridad y privacidad de la información.

- Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.

- Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.

- Representar a la Universidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.

- Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.

- Realizar la gestión de vinculación, capacitación, y desvinculación del personal contratado como contratista por prestación de servicios, dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

- Controlar y salvaguardar la información de datos personales del personal que labora como contratista por prestación de servicios en la Universidad, en concordancia con la normatividad vigente.

g. Oficina de Personal

- Controlar y salvaguardar la información de datos personales del personal que labora en la Universidad, en concordancia con la normatividad vigente.

- Realizar la gestión de vinculación, capacitación, y desvinculación del personal dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

- Incluir en el Plan de Capacitación anual de inducción y reinducción la Políticas de Seguridad y Privacidad de la información.

- Incluir en el plan anual de capacitaciones temas relacionados con seguridad y privacidad de la información.

h. Oficina de Control Interno

- Realizar seguimiento y evaluación con base en la priorización del Plan Anual de Auditorías aprobado en cada vigencia.

i. Área de Comunicaciones

- Diseñar y elaborar las piezas gráficas que requiera la Oficina de Sistemas en materia de seguridad y privacidad de la información.

- Apoyar la publicación y difusión de los contenidos alusivos a seguridad y privacidad de la información, a través de los diferentes medios de comunicación institucional.

j. Líderes de procesos

- Promover la difusión y sensibilización de la seguridad de la información hacia los funcionarios.

- Cumplir y hacer cumplir todo lo relacionado con el SGSI y protección de datos personales.

k. Usuarios

Es el personal de la Universidad de los Llanos sin importar su vínculo, régimen laboral, modalidad de contratación, o nivel jerárquico, las personas naturales o jurídicas que prestan y hacen uso de los servicios en la Universidad, así como las personas y entidades públicas o privadas que utilizan la información de la Universidad de los Llanos. Tienen como responsabilidades:

- Acatar y cumplir con las políticas, lineamientos y procedimientos de seguridad y privacidad de la información.
- Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos.
- Utilizar la información de la Universidad de los Llanos únicamente para los fines autorizados.
- Participar en las capacitaciones y programas de sensibilización en seguridad de la información.
- Reportar cualquier incidente relacionado con seguridad de la información.
- No divulgar información institucional, ni hacer uso de ella, con fines ajenos al desarrollo de sus labores; manteniendo la debida confidencialidad y protección de los datos.

7. FLUJOGRAMA

No aplica

8. LISTADO DE ANEXOS

No aplica.

9. HISTORIAL DE CAMBIOS

Versión	Fecha	Cambios	Elaboró/Modificó	Revisó	Aprobó
01	29/11/2023	Documento nuevo.	Mónica Hernández *Prof. Seguridad de la Información*	Roiman A. Sastoque *Oficina de Sistemas*	Comité Institucional de Gestión y Desempeño