MANUAL DE ROLES Y RESPONSABILIDADES DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN “MSPI” DE LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO

Tabla de Contenido

1. BASES CONCEPTUALES

La **INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO** ha utilizado para la definición de los roles y responsabilidades de seguridad de información, el principio de separación de funciones de Gobierno y las funciones de Gestión, diferenciándolas así:

Gobierno (o gobernanza)	Gestión
El gobierno garantiza que las necesidades, condiciones y opciones de las partes interesadas se evalúen para acordar los objetivos institucionales que serán alcanzados; establecer dirección a través de la priorización y la toma de decisiones; así como monitorear el desempeño y el cumplimiento frente a las decisiones de la dirección y los objetivos antes mencionados.	La administración planifica, construye, ejecuta y monitorea las actividades en alineación con la dirección establecida por el órgano de gobierno para lograr los objetivos de la IUE.

Para abordar correctamente las necesidades de la seguridad de la información y ciberseguridad de la **INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO**, los roles y responsabilidades establecidas deberán cubrir las actividades tanto de la gestión como las de gobierno; actividades que se describen gráficamente en el siguiente diagrama:

Ilustración 1: Separación de funciones de gobierno y gestión

Tomando en cuenta lo anterior, en el presente documento se abordarán la definición de los roles tanto de gestión como los de gobierno.

Adicionalmente se establecerán las responsabilidades de:

- Los dueños de los activos de información.
- Los custodios de los activos de información.
- Los usuarios de los activos de información.
- Un (o varios) proveedores(s) encargado(s) de apoyar asuntos específicos de la seguridad de la información.

2. ROLES Y REPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Los roles y responsabilidades para desempeñar las múltiples funciones y actividades tanto del gobierno como de la gestión de seguridad de la información y ciberseguridad se presentan de forma gráfica en la presente ilustración:

Ilustración 2: Roles y Responsabilidades

Independiente de la cantidad de integrantes, el área o equipo de seguridad de la información al depender de la Oficina Informática debe evitar convertirse en juez y parte, para lo cual debe existir una separación entre los roles de gestión y gobierno.

3. ROLES DE GOBIERNO

3.1 Comité directivo de seguridad de la información:

Equipo interdisciplinario con capacidad de decisión, sus responsabilidades incluyen:

- Asegurar la alineación de la seguridad de la información con las necesidades de la institución.
- Aprobar los objetivos y la estrategia de seguridad de la información de la institución.
- Aprobar las políticas de seguridad de la información.
- Establecer prioridades de acción.
- Hacer seguimiento a la gestión de seguridad de la información.
- Asignar recursos para la realización de planes, actividades o iniciativas de seguridad de la información.
- Aprobar planes correctivos y de mejora para la gestión de seguridad de la información.
- Realizar seguimiento sobre el avance de las iniciativas o proyectos de seguridad de la información.

- Dar retroalimentación sobre el desempeño de la seguridad de la información.

- Dar retroalimentación sobre la valoración de riesgos de seguridad de la información.

- Dar retroalimentación y línea de acción frente a auditorías y otras evaluaciones de la seguridad de la información.

- Recibir retroalimentación de las partes interesadas.

4. ROLES DE GESTIÓN

Ilustración 3: Roles de Gestión

4.1 Líder del equipo de seguridad de la información:

Responsable de:

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

- Establecer el programa (proyecto) de seguridad de la información, previa aprobación de la estrategia por parte del comité de seguridad de la información.

- Coordinar las operaciones de las tecnologías de seguridad de la información.

- Coordinar la gestión de seguridad de la información y ciberseguridad, gestión que incluye: Identificación y cumplimiento de requisitos legales o regulatorios, 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.

- Coordinar respuestas a requerimientos de seguridad de entes regulatorios y/o clientes.

- Coordinar las contrataciones y adquisiciones relacionadas con seguridad de la información y ciberseguridad.

4.2 Profesional de Gestión y Cumplimiento

Profesional de inclinación administrativa en asuntos de seguridad de la información, cuyas responsabilidades incluyen:

- Ejecución de las actividades asociadas a la gestión de los riesgos, que encierra: Identificación, valoración y evaluación de riesgos, así como el seguimiento al tratamiento de éstos.

- Cumplimiento de requerimientos legales (en cuanto a seguridad de la información) que le sean asignados al equipo de seguridad.

- Coordinación de actividades con proveedores de consultoría o servicios relacionados: por ejemplo: auditoría de seguridad de la información.

- La actualización y la vigencia de los procedimientos del MSPI.

- Realizar una correcta ejecución del procedimiento(s) de tratamiento de incidentes de seguridad.

- Documentar las políticas, procedimientos, instructivos y guías de seguridad de la información específicas para su posterior aprobación.

- Generación de métricas de seguridad asociadas a sus áreas de responsabilidad.

- Realización y actualización del inventario de activos de información. Identificación de estándares y buenas prácticas para la mejora y entrega de valor a la entidad.

- Identificación de estándares y buenas prácticas para la mejora y entrega de valor a la entidad.

4.3 Profesional de Operación de Ciberseguridad

Profesional de inclinación técnica cuyas responsabilidades incluyen:

- Verificación de la aplicación de las políticas, controles y criterios de seguridad de la información en los sistemas de información y la infraestructura tecnológica de la entidad.

- Implementación y despliegue de nuevas tecnologías de seguridad de la información.

- Definición de estándares y líneas base para la configuración segura de los sistemas de información, así como para la infraestructura tecnológica de la entidad.

- Participar activamente en respuestas eficaces y oportunas a incidentes de seguridad de la información.

- Operación eficaz de los sistemas para la protección de la seguridad de la información que le sean asignados (como firewall, antivirus, antispam).

- Constante afinamiento y mejora de las tecnologías de seguridad de la información que sean administrados.

- Aplicación de controles de seguridad pertinentes a nuevos equipos o sistemas de información.

- Gestión de vulnerabilidades (identificación, registro y remediación).

- Generación de métricas de seguridad asociadas a las áreas de responsabilidad.

- Coordinación con proveedores de naturaleza técnica relacionados con seguridad de la información.

5. IMPLEMENTACIÓN DE ROLES

5.1 Comité directivo de seguridad de la información:

Las funciones de este comité serán integradas al "**comité de gestión y desempeño**" ya existente en la Institución Universitaria de Envigado, el cual está integrado por su alta dirección.

5.2 Líder del equipo de seguridad de la información:

Este rol será soportado por los siguientes cargos de la institución:

- **Director de Informática**

5.3 Profesional de Gestión y Cumplimiento:

Las funciones de este rol serán integradas con las de Operación y Ciberseguridad, dicho rol se llamará "**Encargado de la Ciberseguridad de la IUE**".

5.4 Profesional de Operación de Ciberseguridad:

Las funciones de este rol serán integradas con las de Gestión y Cumplimiento, dicho rol se llamará "**Encargado de la Ciberseguridad de la IUE**".

6. OTROS ROLES RELEVANTES PARA LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Todos los servidores públicos, estudiantes, contratistas, practicantes o terceros y demás personas jurídicas o naturales que hagan uso de la información y de las tecnologías que la soportan, tienen un rol de seguridad de la información, según el nivel de involucramiento con la información con la que trabajan. Los roles descritos en esta sección son: propietarios, custodios y usuarios de la información.

6.1 Propietarios de Activos de Información

Rol, proceso o área con la capacidad de tomar decisiones sobre activos de información. Por ejemplo: cambiar, eliminar, conceder acceso, o compartir; sus responsabilidades incluyen:

- Autorizar y/o denegar acceso a los activos de información que se encuentren bajo su responsabilidad.
- Participar en los procesos de gestión del riesgo de seguridad de la información.
- Validar que los activos de información bajo su responsabilidad se encuentren dentro del inventario de activos de información.

- Velar por la existencia de custodios de los activos de información bajo su responsabilidad.

- Apoyar la realización de actividades de gestión del riesgo sobre los activos bajo su responsabilidad; lo que incluye, por ejemplo, la entrega oportuna de información y la asistencia a sesiones de trabajo celebradas para tal fin.

6.2 Custodio de Activo de Información

Rol con mandato de aplicar y mantener controles para proteger la seguridad de activos de información. Los administradores de sistemas de información, por ejemplo, son custodios de los sistemas que administran. Sus responsabilidades incluyen**:**

- Aplicar, operar y mantener los controles para la protección de los activos de información.

- Participar en las actividades de mitigación o tratamiento de riesgos en las que sea requerido.

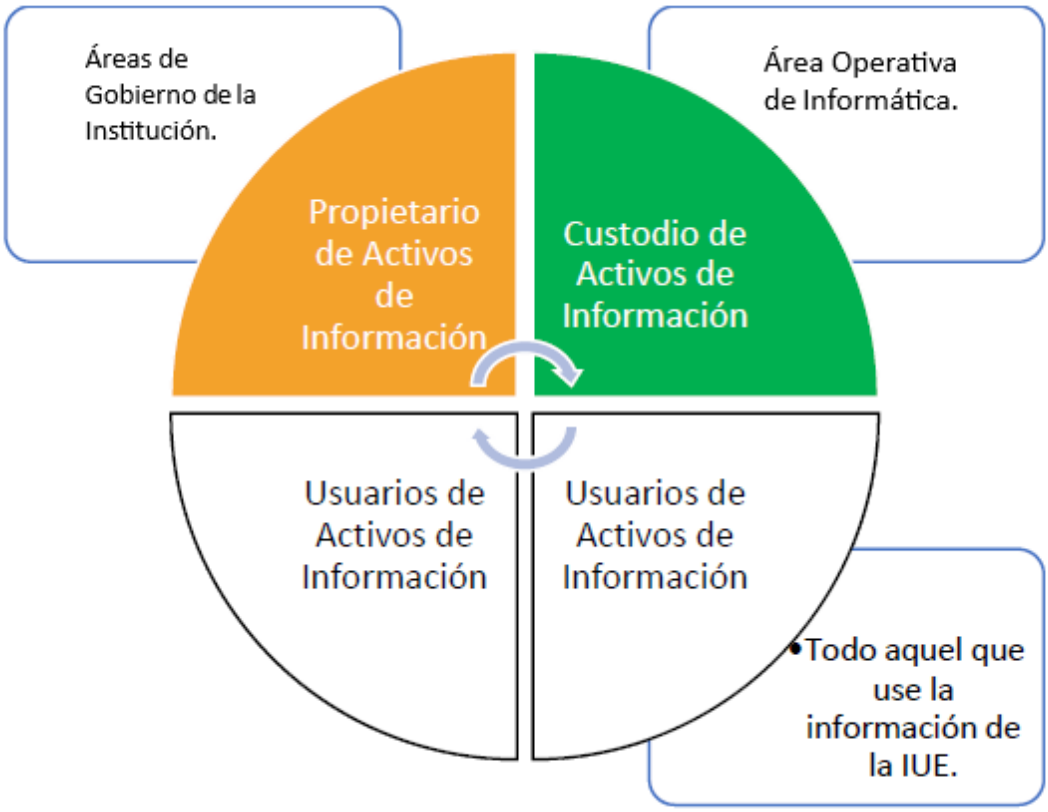
- Rendir cuentas sobre la eficacia de los controles aplicados a los activos de información bajo su responsabilidad.

6.3 Usuarios de Activos de Información

Corresponde a todos los usuarios de la información de la **INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO** y de otros activos que la soportan, por ejemplo, los sistemas de información. Sus responsabilidades incluyen:

- Apoyar, asesorar y cuando sea requerido coordinar las actividades de gestión del riesgo de información.
- Reportar cambios en procesos, estrategias, o activos de información al comité de dirección de seguridad de la información.
- Cumplir las políticas de seguridad de la información de la entidad.
- Atender las iniciativas de cultura en seguridad de la información en las que se requiera de su participación.
- Reportar cualquier anomalía que puede desencadenar en incidentes de seguridad.

En la **INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO** este rol es asignado a los servidores públicos, estudiantes, contratistas, practicantes o terceros y demás personas jurídicas o naturales que hagan uso de la información y de las tecnologías que la soportan.



6.4 Auditor de Seguridad de la Información

El auditor de seguridad informática comprueba que las medidas de seguridad y control de los sistemas informáticos se adecúan a la normativa que se ha desarrollado para la protección de los datos; identifica las deficiencias, y propone medidas correctoras o complementarias.

Este debe ser un rol con objetividad e independencia del área que supervisa, responsabilidades incluyen:

- Validar el cumplimiento de la normativa “MSPI” emitida por Min Tic.
- Reportar hallazgos y sugerencias al comité de dirección de seguridad de la información.
- Cumplir las políticas de seguridad de la información de la entidad.
- Reportar cualquier anomalía que puede desencadenar en incidentes de seguridad.

7 REFERENCIAS

- ISO/IEC 27001
- COBIT 2019