PROCESO DE GESTION DEL RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN "MSPI" DE LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO

Tabla de contenido

1. OBJETIVO

Establecer criterios, actividades y elementos necesarios para la metodología de riesgos de seguridad de la información y ciberseguridad de **LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO,** con el fin de posibilitar la identificación, análisis, evaluación y tratamiento del riesgo de seguridad de la información y ciberseguridad.

2. ALCANCE

El presente documento aplica para los riesgos de seguridad de la información y ciberseguridad de **LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO.**

3. DEFINICIONES

Aceptación del riesgo: decisión informada de tomar un riesgo particular.

Análisis de riesgo: proceso para determinar la naturaleza y el nivel de riesgo.

Amenaza: fuente potencial de un evento no deseado.

Evaluación de riesgo: proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo o su magnitud es aceptable o tolerable.

Incidente de seguridad de la información: un evento o serie de eventos de seguridad informática no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad informática. Todo incidente es un evento, más no todo evento es un incidente.

Identificación del riesgo: proceso de búsqueda, reconocimiento y descripción de riesgos.

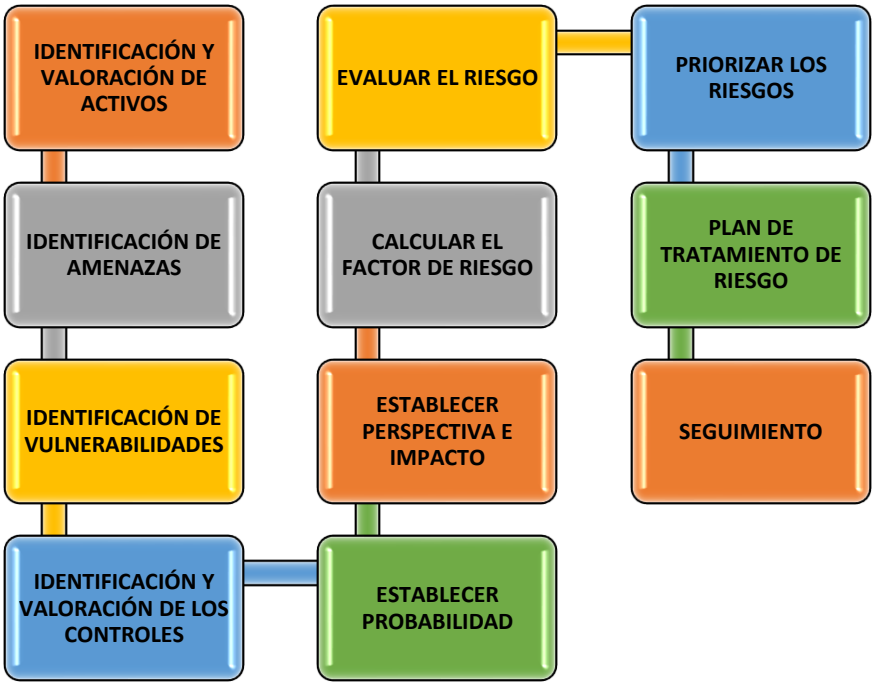
Riesgo: en el contexto del MSPI, los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

Valoración de riesgo: proceso general de identificación de riesgos, análisis de riesgos y evaluación de riesgos.

Vulnerabilidad: una debilidad en un sistema, que puede ser objeto de explotación o mal uso, esta puede existir por falta de actualizaciones o errores de configuración en las plataformas.

4. DESARROLLO

En este punto se muestra en la grafica las actividades que hacen parte del proceso de gestión del riesgo del modelo de seguridad y privacidad de la información de la institución universitaria de envigado, del mismo modo se explica en detalle cada una de dichas actividades para el desarrollo adecuado de la gestión de los riesgos de seguridad y ciberseguridad de la institución.



Grafica 1: Actividades del Proceso de Gestión de Riesgo de Seguridad

4.1. IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS

Actividad	Descripción	Responsable
Identificar los activos de información.	Recopilación de la información de los activos de información correspondientes al alcance del MSPI, posteriormente se registran en el formato correspondiente.	Encargado de la Ciberseguridad de la IUE

Entradas	Salidas
• El alcance deseado para el inventario (normalmente uno de los procesos de la cadena de valor institucional). • Metodología de identificación e inventario de activos. • Plantilla para registro del inventario de activos. • Información de propietarios, usuarios y demás consultados en la construcción del inventario.	• Inventario de activos completado. • Todos los activos de información dentro alcance del MSPI identificados y valorados.

4.2. IDENTIFICACIÓN DE AMENAZAS

Actividad	Descripción	Responsable
Identificar las amenazas de seguridad de la información.	Reconocer las amenazas que pueden afectar a los activos previamente identificados. Las amenazas son causas potenciales de incidentes no deseados, que pueden resultar en daño a información, procesos o sistemas de la compañía. Las amenazas pueden ser identificadas preliminarmente en la etapa de inventario de activos, donde los usuarios y dueños de los activos hacen reconocimiento de estas, o posteriormente en la valoración de riesgo haciendo uso del catálogo de amenazas existente.	Encargado de la Ciberseguridad de la IUE

Entradas	Salidas
• Inventario de activos. • Plantilla de registro de riesgos. • Información de dueños, usuarios y demás consultados en la valoración de riesgos. • Catálogo de amenazas existente.	• Amenazas identificadas y registradas.

4.3. IDENTIFICACIÓN DE VULNERABILIDADES

Actividad	Descripción	Responsable
Identificar las vulnerabilidades.	La identificación consiste en reconocer las vulnerabilidades que pueden ser utilizadas por las amenazas para causar daños a los activos. La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que exista una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza asociada puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios. Conviene anotar que un control implementado de manera incorrecta, o un mal funcionamiento, podría por sí solo constituir una vulnerabilidad. Un control puede ser eficaz o ineficaz dependiendo del ambiente de funcionamiento. Las vulnerabilidades pueden ser identificadas por diferentes vías:	Encargado de la Ciberseguridad de la IUE y/o Contratista Externo

	• A través de la realización de pruebas de seguridad (escaneo de vulnerabilidades, pruebas de penetración caja negra, blanca o gris, hacking ético o pruebas de código dinámicas o estáticas). • La identificación de estas condiciones por parte de empleados, proveedores, practicantes o terceros y demás personas jurídicas o naturales involucrados en la administración o uso del activo de información.	

Entradas	Salidas
• Inventario de activos. • Plantilla de registro de riesgos de seguridad de la información y ciberseguridad. • Información de propietarios, usuarios y demás consultados en la valoración de riesgos.	• Vulnerabilidades identificadas y registradas.

4.4. IDENTIFICACIÓN Y VALORACIÓN DE LOS CONTROLES

Actividad	Descripción	Responsable
Identificar los controles asociados a los riesgos.	Se realiza la identificación de los controles existentes para mitigar los riesgos, reconociendo situaciones indeseadas como la duplicación de los controles. Además, mientras se ejecuta esta identificación es recomendable hacer una verificación para garantizar que los controles funcionan correctamente. Si el control no funciona como se espera, puede causar vulnerabilidades.	Encargado de la Ciberseguridad de la IUE

Entradas	Salidas
• Inventario de activos. • Plantilla de registro de riesgos de seguridad de la información y ciberseguridad. • Información de propietarios, usuarios y demás consultados en la valoración de riesgos. • Amenazas identificadas. • Vulnerabilidades identificadas.	• Controles actuales asociados a cada riesgo; identificados, caracterizados y registrados.

4.5. ESTABLECER PROBABILIDAD

Actividad	Descripción	Responsable
Establecer probabilidad del riesgo.	Con el fin de derivar una probabilidad o una estimación de la ocurrencia de un evento, los siguientes factores deben ser tomados en cuenta: • Fuente de la amenaza y su cabida. • Naturaleza de la vulnerabilidad. La probabilidad de que una vulnerabilidad pueda ser explotada por una amenaza, debe ser establecida de acuerdo con los criterios indicados en la sección 4.5.1.	Encargado de la Ciberseguridad de la IUE

Entradas	Salidas
• Plantilla de registro de riesgos de seguridad de la información, con amenazas, vulnerabilidades y controles actuales identificados para cada riesgo. • Información de propietarios, usuarios y demás consultados en la valoración de riesgos. • Criterios de probabilidad.	• Probabilidad de ocurrencia para cada riesgo identificado.

4.5.1. CRITERIO DE PROBABILIDAD

Valor	Frecuencia
Casi seguro	Podría materializarse varias veces al año.
Probable	Podría materializarse una vez al año.
Posible	Se podría materializar en un espacio de 2 años.
Improbable	Podría materializarse una vez cada 5 años.
Raro	Podría materializarse una vez cada 10 años.

4.6. ESTABLECER PERSPECTIVA E IMPACTO

Actividad	Descripción	Responsable
Identificar los activos de información.	Esta actividad identifica los daños o las consecuencias para la institución que podrían ser causadas por un escenario de incidente. El impacto de los escenarios de incidente se determina tomando en consideración las perspectivas y los criterios de impacto formulados en la sección 4.6.1. Se deberían tener en cuenta los valores asignados a estos activos en la evaluación de las consecuencias.	Encargado de la Ciberseguridad de la IUE

Entradas	Salidas
• Plantilla de registro de riesgos de seguridad de la información y ciberseguridad, dentro del cual se reflejen amenazas, vulnerabilidades y controles actuales identificados para cada riesgo. • Información de propietarios, usuarios y demás consultados en la valoración de riesgos. • Criterios y perspectivas de impacto.	• Impacto de cada riesgo identificado en términos de la perspectiva seleccionada.

4.6.1. CRITERIO DE IMPACTO

Dimensión: Imagen Institucional

Valor	Descripción
Catastrófico	El evento podría tener una repercusión internacional, y podría desencadenar pérdidas por conceptos de multas, sanciones a la institución y perdida de estudiantes. Hay una pérdida grave de credibilidad en grupos de interés.
Mayor	El evento podría tener una repercusión nacional y podría desencadenar pérdidas por conceptos de multas, sanciones a la institución y perdida de estudiantes.
Moderado	El evento podría tener una repercusión regional y podría desencadenar pérdidas por conceptos de multas, sanciones a la institución y perdida de estudiantes.

Menor	El evento podría tener ser conocido internamente por los empleados, estudiantes, contratistas, proveedores, aprendices, practicantes o terceros y demás personas jurídicas o naturales que hagan uso de la información y de las tecnologías que la soportan. Podría desencadenar pérdidas por conceptos de perdida de estudiantes.
Insignificante	El evento podría generar discusiones o dificultades internas con los empleados, estudiantes, contratistas, proveedores, aprendices, practicantes o terceros y demás personas jurídicas o naturales que hagan uso de la información y de las tecnologías que la soportan.

Dimensión: Información Estudiantes

Valor	Descripción
Catastrófico	Se podría comprometer la confidencialidad o la integridad de la información de varios estudiantes de la institución por el aprovechamiento de una vulnerabilidad. (técnica, de procesos o personas)
Mayor	Se podría comprometer la confidencialidad o la integridad de la información de un solo estudiante de la institución por el aprovechamiento de una vulnerabilidad. (técnica, de procesos o personas)
Moderado	Se podría comprometer la capacidad de **LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO** para acceder a la información de los estudiantes para la prestación de un servicio (disponibilidad).

Menor	Se podría comprometer un fragmento de información (por ejemplo, las notas) o dato de un estudiante.
Insignificante	Se podría comprometer la información que no representa un impacto significativo para los estudiantes o para **LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO**.

Dimensión: Interrupción Servicios

Valor	Descripción
Catastrófico	El evento podría generar interrupción de la prestación de uno o más servicios críticos de **LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO** hasta por 5 días hábiles.
Mayor	El evento podría generar interrupción de la prestación de uno o más servicios críticos de **LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO** hasta por 2 días hábiles.

Moderado	El evento podría generar interrupción de la prestación de uno o más servicios no críticos de **LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO** hasta por 5 días hábiles.
Menor	El evento podría generar interrupción de la prestación de uno o más servicios no críticos de **LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO** hasta por 2 días hábiles.
Insignificante	El evento no genera interrupción de ningún servicio o genera una interrupción mínima de los servicios de **LA INSTITUCIÓN UNIVERSITARÍA DE ENVIGADO.**

4.7. CALCULAR EL FACTOR DE RIESGO

Actividad	Descripción	Responsable
Calcular el factor de riesgo.	Esta actividad consiste en estimar el factor del riesgo comparando los valores de probabilidad e impacto previamente determinados. El factor de riesgo se obtiene utilizando los criterios de valoración de riesgos definidos en 4.7.1	Encargado de la Ciberseguridad de la IUE

Entradas	Salidas
• Plantilla de registro de riesgos de seguridad de la información, con amenazas, vulnerabilidades, controles actuales, probabilidades e impacto identificados para cada riesgo. • Criterios de riesgo.	• Factor del riesgo calculado para cada riesgo analizado.

4.7.1. CRITERIOS DE VALORACIÓN DE RIESGO

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi Seguro	Bajo	Medio	Alto	Critico	Critico
Probable	Bajo	Bajo	Medio	Alto	Critico
Posible	Bajo	Bajo	Medio	Medio	Alto
Improbable	Bajo	Bajo	Bajo	Medio	Medio
Raro	Bajo	Bajo	Bajo	Medio	Medio

4.7.2. CRITERIOS DE ACEPTACIÓN DE RIESGO

Se consideran riesgos aceptables aquellos que se encuentren en un nivel “medio” o “bajo”.

4.8. EVALUAR EL RIESGO

Actividad	Descripción	Responsable
Evaluar el riesgo.	Esta actividad consiste en evaluar el riesgo utilizando los criterios de aceptación de riesgos establecidos.	Encargado de la Ciberseguridad de la IUE

Entradas	Salidas
• Plantilla de registro de riesgos de seguridad de la información, con el valor resultante del análisis de riesgos de cada activo de información. • Criterios de aceptación de riesgos. 4.7.2	• Riesgo evaluado en función de su aceptación.

4.9. PRIORIZAR LOS RIESGOS

Actividad	Descripción	Responsable
Priorizar los riesgos.	Esta actividad consiste en priorizar el tratamiento de los riesgos considerando su aceptabilidad y su valor. Para realizar esta actividad se requiere que todos los riesgos que han sido identificados se encuentren evaluados.	Encargado de la Ciberseguridad de la IUE

Entradas	Salidas
• Riesgos por priorizar. • Alternativa de tratamiento de riesgos. • Criterio de aceptación de riesgos. • Plantilla de plan de tratamiento de riesgos.	• Riesgo priorizado para su tratamiento.

4.10. PLAN DE TRATAMIENTO DE RIESGO

Actividad	Descripción	Responsable
Proponer alternativas de tratamiento.	Proponer estrategias para evitar, mitigar, compartir o aceptar el riesgo.	Propietarios y responsables de los activos asociados al riesgo.
Seleccionar alternativas propuestas.	Seleccionar una de las estrategias propuestas.	Líder del proceso o dueño del activo.
Aceptar el riesgo residual.	Aceptar el riesgo residual, es decir, el nivel de riesgo que quedará después de implementar el plan de tratamiento de riesgos.	Líder del proceso o dueño del activo.
Construir el plan de tratamiento de riesgos.	Detallar las actividades necesarias, los recursos y los responsables para lograr llevar a cabo la estrategia seleccionada.	Propietarios y responsables de los activos asociados al riesgo.

Entradas	Salidas
• Riesgos priorizados. • Alternativa de tratamiento de riesgos. • Criterio de aceptación de riesgos. • Plantilla de plan de tratamiento de riesgos.	• Plan de tratamiento de riesgos aprobado.

4.11. SEGUIMIENTO

Actividad	Descripción	Responsable
Realizar seguimiento a los planes de tratamiento.	Verificar que las acciones definidas en el plan de tratamiento de riesgos se hayan ejecutado satisfactoriamente.	Director de Informática

Entradas	Salidas
• Riesgos valorados. • Plan de tratamiento de riesgos documentado.	• Plan de tratamiento de riesgos verificado con registros de fecha, responsables y observaciones

5. DOCUMENTOS DE REFERENCIA

- ISO/IEC 27001:2013
- ISO/IEC 27005:2018
- ISO/IEC 31000:2018

6. PUNTOS DE CONTROL

Actividad 4.11 del presente documento “seguimiento”.

7. REGISTRO

- Formato diligenciado de inventario de activos.
- Formato diligenciado de valoración de riesgos.
- Formato diligenciado de tratamiento de riesgos.