TABLA DE CONTENIDO

1. OBJETIVO GENERAL

Proteger los derechos de los usuarios de la universidad y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información.
La Universidad implementa el plan de seguridad y privacidad de la información, clasifica y gestiona controles para minimizar el riesgo asociado a los procesos tecnológicos, con el fin de salvaguardar los activos de información.

2. ALCANCE

Se define el alcance del presente plan de tratamiento de riesgos de seguridad y privacidad de la información, en los procesos de servicios de infraestructura tecnológica para el control y mitigación de los riesgos de seguridad de la información institucional gestionada por la Oficina de informática.

3. RESPONSABILIDAD

El jefe de la Oficina de Informática es el responsable de que el plan se lleve a cabo y la difusión a las partes interesadas para el conocimiento y aplicabilidad del mismo, velará por la integridad, confidencialidad y no repudio de los datos o información ante cualquier eventualidad a la que pueda quedar expuesta la oficina de informática.

4. GLOSARIO DE TÉRMINOS

En este espacio se listan algunas definiciones que utilizaremos en el desarrollo del plan de tratamiento de riesgos de la información de la Universidad del Atlántico.

ACTIVO DE INFORMACIÓN: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización.
ADMINISTRACIÓN DEL RIESGO: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente

el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

ANÁLISIS DE RIESGO: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

BASE DE DATOS PERSONALES: Conjunto organizado de datos personales que sea objeto de tratamiento.

CAUSA: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CONSECUENCIA: Resultado de un evento que afecta los objetivos.

CRITERIOS DEL RIESGO: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

CONTROL: Medida que modifica el riesgo.

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

EVALUACIÓN DE RIESGOS: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

EVENTO: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico. Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

EVITACIÓN DEL RIESGO: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

FACTORES DE RIESGO: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad. Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

GRAVEDAD: Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).

IDENTIFICACIÓN DEL RIESGO: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

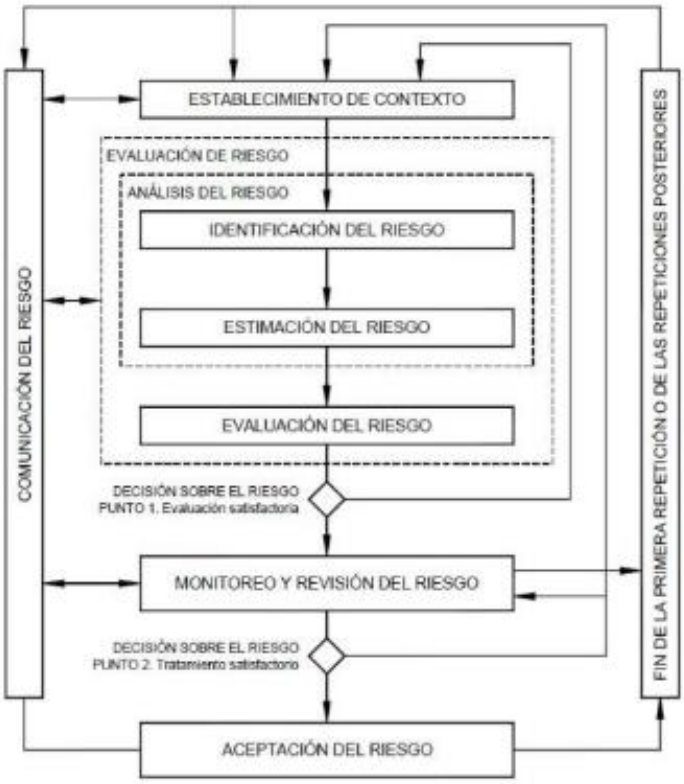
INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad

significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.
IMPACTO: Cambio adverso en el nivel de los objetivos del negocio logrados.
NIVEL DE RIESGO: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
MATRIZ DE RIESGOS: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
MONITOREO: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión. Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
PLAN DE CONTIGENCIA: Es una estrategia que se compone de una serie de procedimientos que facilitan una solución alternativa que permite restituir rápidamente el funcionamiento de los servicios críticos de la Institución ante la eventualidad que lo afecte de forma parcial o total.
PLAN DE TRATAMIENTO DE RIESGOS: documento donde se definen las acciones para gestionar los riesgos e implantar los controles necesarios.
PROCESO: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
REDUCCIÓN DEL RIESGO: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular
RIESGO INHERENTE: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
RIESGO RESIDUAL: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
RIESGO: Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.
RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

SEGUIMIENTO: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.
SEGURIDAD: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.
TRATAMIENTO DEL RIESGO: Proceso para modificar el riesgo" (Icontec Internacional, 2011).
USUARIOS: Se refiere a todos los empleados, contratistas, consultores, trabajadores temporales, y cualquier otra persona o entidad que por razón de su trabajo se le permita acceso, se le asignen derechos de uso y utilicen los recursos que componen los medios electrónicos de almacenamiento y transmisión de datos de la universidad del Atlántico. Igualmente se clasifica como usuario a cualquier empleado, contratista, consultor, o trabajador temporal de compañías asociadas a la universidad del Atlántico, a quienes se les preste cualquier tipo de servicio que implique la utilización de los medios electrónicos de transmisión de datos de la universidad del Atlántico.
VALORACIÓN DEL RIESGO: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
VULNERABILIDAD: Es aquella debilidad de un activo o grupo de activos de información
Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.
SGSI: Sistema de Gestión de Seguridad de la Información.

5. VISION GENERAL DEL PROCESO DE GESTIÓN DE RIESGOS

El siguiente diagrama representa el modelo de gestión de riesgos de seguridad de la información, diseñado a partir de la norma ISO/IEC 27005



El plan de tratamiento de riesgos de seguridad y privacidad de la información, propone una gestión iterativa en cuanto a las actividades de valoración del impacto y el tratamiento de los riesgos identificados.

5.1. Establecimiento del contexto de riesgos de seguridad de la información

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la Universidad del Atlántico y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos de la Universidad del Atlántico, en el análisis de las debilidades y amenazas asociadas, en la

valoración de los riesgos en términos de sus consecuencias e impacto para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

5.1.1 Criterios de evaluación de riesgo de seguridad de la información

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso para la Universidad del Atlántico.
- La criticidad de los activos de información involucrados.
- Los requisitos normativos, legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la Universidad del Atlántico.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la Universidad del Atlántico.

5.1.2 Criterios de impacto

Los criterios de impacto se especificarán en términos de grado, daño o de los costos para la Universidad, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados.
- Brechas en la seguridad de la información (perdida de la confidencialidad, integridad y/o disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceros)
- Pérdida del negocio o del valor financiero.
- Alteración de planes o fechas límites.
- Daños en la reputación.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

5.1.3 Criterios de aceptación

Los criterios de aceptación dependerán de las políticas, metas y objetivos de la Universidad del Atlántico y de las partes interesadas. Se deben establecer de manera dinámica e iterativa unas escalas de aceptación del riesgo de forma periódica.

5.2 Valoración de los riesgos de seguridad de la información

Antes de realizar la valoración de los riesgos de seguridad de la información, se debe determinar si es relevante identificar un inventario de activos de información de los procesos, el cual será la base del enfoque de la valorización de los riesgos de seguridad de la información.

Se deberán identificar, describir cuantitativa o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Universidad.

Esta fase consta de las siguientes etapas:

- Análisis del riesgo: Identificación y estimación del riesgo.
- Evaluación del riesgo

5.2.1 Identificación del riesgo

Para la evaluación de riesgos de seguridad de la información, como primera medida se deberán identificar los activos de información por proceso evaluado.

Los activos de información se clasifican en:

- **Primarios:**

Procesos o subprocesos y actividades del negocio: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

Información: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los

objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

Actividades y procesos del negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la Universidad, los necesarios para el cumplimiento legal o contractual, etc.

- **De Soporte**

Hardware: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).

Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)

Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (equipos de comunicación, cableado, puntos de acceso, etc.)

Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

Sitio: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)

Estructura organizativa: responsables, áreas, contratistas, etc.

Luego de ser identificados y relacionados todos los activos, pasaremos a conocer las amenazas que pueden causar daño a la información, los procesos y soportes. Identificar dichas amenazas y la valoración de los daños que estas pueden producir, se puede obtener mediante la indagación a los dueños de los activos, a los usuarios, a expertos, etc.

El siguiente paso, luego de identificar el listado de activos, las amenazas relacionadas, valorar los daños y revisar las medidas que se han tomado, es revisar las **vulnerabilidades**

de las que puedan tomar ventaja las amenazas para causar daños a los activos de información de la Universidad del Atlántico.

Entre los diferentes métodos que podemos utilizar estarían:

- Realizar entrevistas con los líderes de procesos y también con los usuarios.
- Realizar inspecciones periódicas en sitio.
- Utilizar herramientas para escaneo automatizado.

Por cada **amenaza** identificada analizaremos las **vulnerabilidades** que pudiesen ser explotadas.

Como pasó final, se identificarán las **consecuencias** que no son más que la manera como estas **amenazas** y **vulnerabilidades** afectan la integridad, disponibilidad y confidencialidad de los activos de información.

5.2.2 Estimación del riesgo

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad:** La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.
- **Impacto:** Hace referencia a las consecuencias que puede ocasionar a la Agencia la materialización del riesgo; se refiere a la magnitud de sus efectos.

Lo más recomendable es realizar el análisis contando con el apoyo de las personas que se encuentren más familiarizadas con el proceso para determinar con mayor precisión el impacto y la probabilidad del riesgo y así poder clasificarlos en los rangos que sean establecidos.

Para estimar el riesgo desde el enfoque del impacto y las consecuencias, se tomarán en cuenta factores tales como: pérdidas financieras, el costo de reparar o reemplazar un activo de información, disminución del rendimiento, interrupciones en la actividad normal de la institución, multas o sanciones a consecuencia de la materialización del riesgo, daños personales, entre otros.

Además de medir las posibles consecuencias, se debe ~~tener en~~ realizar también la medición y/o estimación de la probabilidad de que ocurran las situaciones que pueden impactar los activos de información de la Universidad, alterar su normal operación o detenerla por completo.

Formato para el registro, estimación y tratamiento de los riesgos de seguridad de la información

5.2.3 Formato para el registro, estimación y tratamiento de los riesgos de seguridad de la información.

El formato utilizado por la Universidad del Atlántico para ~~la~~ registrar y dar tratamiento a los riesgos de los activos de información, es el formato **evaluación-riesgo- GT** disponible en la plataforma del sistema de gestión de la calidad

Este formato será diligenciado por los miembros de cada oficina, facultad o departamento y deberán calificar el impacto y la probabilidad de ocurrencia de cada riesgo identificado, así como también se brindan campos para determinar los planes de mitigación.

Para la estimación de los riesgos se utilizarán los siguientes criterios:

TABLA 1: CRITERIOS PARA CALIFICAR LA PROBABILIDAD

PROBABILIDAD			
CLASIFICACIÓN	**VALOR**	**DESCRIPCIÓN**	**FRECUENCIA**
~~Casi~~ Seguro	5	Se espera su ocurrencia en la mayoría de las circunstancias	Más de 1 vez en al año
Probable	4	El evento probablemente ocurriría en la mayoría de las circunstancias	Al menos 1 vez en el último año
Posible	3	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
Improbable	2	Es poco probable que el evento se presente	Al menos 1 vez en los últimos 5 años
Rara Vez	1	El evento puede ocurrir solo en circunstancias excepcionales	No ha ocurrido en los últimos 5 años

Adaptado para la Universidad del Atlántico de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP, 2018.

TABLA 2: CRITERIOS PARA CALIFICAR EL IMPACTO

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.
MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento	- Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Demora en la información, ocasionando retrasos en la atención a los usuarios.

	en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR	- Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Adaptado para la Universidad del Atlántico de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP, 2020

TABLA 3: CRITERIOS PARA CALIFICAR EL IMPACTO-RIESGOS DE SEGURIDAD DE LA INFORMACION.

NIVEL		CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL

	VALOR DEL IMPACTO	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	-Afectación ≤ 2% de la población. -Afectación ≤ 1% del presupuesto anual de la entidad. No hay afectación medioambiental.	-Sin afectación de la integridad. -Sin afectación de la disponibilidad. -Sin afectación de la confidencialidad. -Sin afectación a la reputación.
MENOR	2	-Afectación ≤ 10% de la población. -Afectación ≤ 2% del presupuesto anual de la entidad. -Afectación leve del medio ambiente requiere de ≤ 8 días de recuperación.	-Afectación leve de la integridad. -Afectación leve de la disponibilidad. -Afectación leve de la confidencialidad. -Sin afectación a la reputación.
MODERADO	3	-Afectación ≤ 20% de la población. -Afectación ≤ 5% del presupuesto anual de la entidad. -Afectación leve del medio ambiente requiere de ≤ 8 semanas de recuperación.	-Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la Confidencialidad de la información debido al interés particular de los empleados y terceros. -Afectación moderada de la reputación.
MAYOR	4	-Afectación ≤ 30% de la población. -Afectación ≤ 20% del presupuesto anual de la entidad. -Afectación importante del medio ambiente que requiere de ≥6 meses de recuperación.	-Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. -Afectación grave de la reputación.

CATASTRÓFICO	5	-Afectación ≥ 30% de la población. -Afectación ≥ 20% del presupuesto anual de la entidad. -Afectación muy grave del medio ambiente que requiere de ≥1 años de recuperación.	-Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. -Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. -Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. -Afectación muy grave de la reputación.

Adaptado para la Universidad del Atlántico de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP, 2018.

5.2.4. Determinación del Riesgo Inherente y Residual

El análisis de riesgo determinado por su probabilidad e impacto nos permite tener una primera evaluación del riesgo inherente y ver el grado de exposición al riesgo que tiene la Universidad del Atlántico. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede observar gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita un primer análisis gráfico. De esta manera podemos analizar de manera global los riesgos según su ubicación en cada zona, facilitando la organización de prioridades para el tratamiento y la implementación de planes de acción.

PROBABILIDAD		IMPACTO				
		INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
RARA VEZ	1	Zona1 de riesgo bajo-asumir el riesgo	Zona4 de riesgo bajo-asumir el riesgo	Zona8 de riesgo moderada Asumir el riesgo reducir el riesgo	Zona15 de riesgo Alta Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona17 de riesgo Alta Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo
IMPROBABLE	2	Zona2 de riesgo bajo-asumir el riesgo	Zona5 de riesgo bajo-asumir el riesgo	Zona9 de riesgo moderada Asumir el riesgo reducir el riesgo	Zona16 de riesgo Alta Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona22 de riesgo Extrema Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo
POSIBLE	3	Zona3 de riesgo bajo-asumir el riesgo	Zona7 de riesgo moderada Asumir el riesgo reducir el riesgo	Zona13 de riesgo Alta Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona19 de riesgo Extrema Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona23 de riesgo Extrema Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo
PROBABLE	4	Zona6 de riesgo moderada Asumir el riesgo reducir el riesgo	Zona11 de riesgo Alta Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona14 de riesgo Alta Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona20 de riesgo Extrema Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona24 de riesgo Extrema Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo
CASI SEGURO	5	Zona10 de riesgo Alta Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona12 de riesgo Alta Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona18 de riesgo Extrema Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona21 de riesgo Extrema Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo	Zona25 de riesgo Extrema Reducirir el riesgo Evitar el riesgo Compartir o trasladar el riesgo

ZONA	NIVEL DE RIESGO
ZONA RIESGO BAJA	Z-1
	Z-2
	Z-3
	Z-4
	Z-5
ZONA DE RIESGO MODERADO	Z-6
	Z-7
	Z-8
	Z-9
ZONA DE RIESGO ALTA	Z-10
	Z-11
	Z-12
	Z-13
	Z-14
	Z-15
	Z-16
	Z-17
ZONA DE RIESGO EXTREMA	Z-18
	Z-19
	Z-20
	Z-21
	Z-22
	Z-23
	Z-24
	Z-25

Esquema general de la Matriz de Riesgos Institucional y zonas de riesgo Institucional para la Universidad del Atlántico-Adaptado para la Universidad del Atlántico de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP, 2018.

Cada zona de riesgo viene identificada con un color distintivo que indica la severidad del riesgo de la siguiente manera:

Zona de Riesgo
B: Zona de riesgo Baja (Color Verde): 5 zonas, siendo Z- 5 la zona de mayor riesgo.
M: Zona de riesgo Moderada (color Amarillo): 4 zonas, siendo Z- 9 la zona de mayor riesgo.
A: Zona de riesgo Alta (Color Rojo): 8 zonas, siendo Z- 17 la zona de mayor riesgo.
E: Zona de riesgo Extrema (Color Vino tinto): 8 zonas, siendo la Z-25 la de más alto riesgo.

5.2.4 Evaluación de Riesgos

Luego de valorar los impactos, la probabilidad y las consecuencias de los riesgos identificados en cada escenario de incidentes, obtendremos los niveles de riesgo, los cuales compararemos en contexto para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información en aras de su impacto en la Universidad del Atlántico.

5.3 Tratamiento de los riesgos de seguridad de la información

Luego de la etapa de evaluación del riesgo, se obtiene una lista ordenada de riesgos o una matriz donde identificamos los niveles de riesgo de acuerdo a su zona y color, entonces se deberán elegir la o las estrategias de tratamiento del riesgo consecuentemente a su valoración y a los criterios establecidos en el contexto de gestión de riesgos.

Para cada nivel se deberá seleccionar la opción de tratamiento adecuada para cada riesgo identificado de forma individual. Para la toma de esta decisión, el factor costo/beneficio del tratamiento será el de mayor relevancia.

TABLA 4: RELACION COSTO BENEFICIO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

OPCION DE TRATAMIENTO	COSTO-BENEFICIO
Evitar el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)	El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios
Trasladar o **compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).	El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo
Reducir el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto	El costo y el tiempo del tratamiento es adecuado a los beneficios
Aceptar el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa	La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.

El resultado de esta fase será un plan de tratamiento de riesgos que contiene la selección y justificación de una o más opciones para cada uno de los riesgos identificados, identificando además los riesgos residuales, es decir, aquellos que continúan existiendo a pesar de las medidas tomadas.

5.4 Monitoreo y Seguimiento a los Riesgos de seguridad de la información

Se realizará la revisión periódica de los activos, vulnerabilidades, probabilidades, impactos y amenazas en busca de posibles cambios que hagan necesaria una valoración continua y constante de los riesgos de seguridad de la información.

Los riesgos cambian a medida que cambian los procesos de la Universidad del Atlántico y estos cambios pueden ocurrir de manera inesperada, por lo tanto, se debe realizar la supervisión continua para detectar: nuevos activos o modificaciones en su valor, nuevas amenazas, nuevas vulnerabilidades o cambios en las ya detectadas, cambios en la severidad de los impactos y por último nuevos incidentes en la seguridad de la información.

Se deben definir esquemas de seguimiento y medición al sistema de gestión de riesgos de seguridad de la información que permitan contextualizar la toma de decisiones de manera oportuna.

6 NORMATIVIDAD Y DOCUMENTOS DE REFERENCIA

El plan de tratamiento de riesgos de seguridad y privacidad de la información de la Universidad del Atlántico se realiza acorde a los requisitos de Gobierno en Línea, orientados con la norma ISO 27005, plan tratamiento de riesgos de la Universidad del Atlántico y en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, que contribuya a salvaguardar la disponibilidad, integridad y la confidencialidad de la información institucional.

7 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ACTIVIDAD	META	PRODUCTO
Análisis de Riesgos de Seguridad y Privacidad de la información	Identificar los riesgos de seguridad y privacidad	Matriz de riesgos de seguridad de la información Matriz de activos de seguridad de la información
	Establecer los criterios de evaluación e impacto de los eventos de seguridad de la información	
Seguimiento y control de los Riesgos	Establecer las estratégicas de evaluación acuerdo a los eventos presentados y su nivel de criticidad	Matriz de riesgos, seguimiento y controles actualizados
Mejoramiento	Identificar las oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos.	Planes de mejoramiento
Política de Seguridad y privacidad de la Información	Aprobación y publicación de la política	Acuerdo por medio del cual se aprueba la política de seguridad y privacidad de la información para la Universidad

8 CONTROL DE CAMBIOS

VER	FECHA	ELABORÓ	DESCRIPCIÓN
0	Mayo 15 del 2020	Ing. Alvaro Castellar	VERSIÓN ORIGINAL
1	Septiembre 29 del 2022	Ing. Carlos Gómez	Actualización de criterios para analizar el impacto, Adición del item 7 Plan de tratamiento riesgo de seguridad y privacidad de la información.