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

ESE UNIVERSITARIA DEL ATLÁNTICO

TABLA DE CONTENIDO

1. GENERALIDADES

La **Empresa Social del Estado Universitaria del Atlántico,** en adelante la Entidad, se compromete a proteger la seguridad y la privacidad de la información que maneja, en cumplimiento con las normativas vigentes y las mejores prácticas del sector. La gestión adecuada de los datos es fundamental para garantizar la confianza de nuestros usuarios, colaboradores y la comunidad en general. Este Plan se fundamenta en un análisis exhaustivo de las amenazas y vulnerabilidades que pueden afectar la confidencialidad, integridad y disponibilidad de los datos, así como en la implementación de controles que aseguren un manejo responsable y ético de la información.

El Modelo Integrado de Planeación y Gestión (MIPG), actúa como un marco de referencia que orienta a las entidades y organismos públicos en la dirección, planificación, ejecución, seguimiento, evaluación y control de sus actividades. Su objetivo es producir resultados que respondan a los planes de desarrollo y aborden las necesidades y problemas de los ciudadanos, garantizando integridad y calidad.

MIPG se convierte en una herramienta fundamental para el desarrollo e implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Entidad al proporcionar un marco que ayuda a alinear el Plan con los objetivos estratégicos de la entidad. Esto garantiza que las acciones a implementar estén en consonancia con las prioridades institucionales y las necesidades de los ciudadanos. Así mismo, se pueden establecer objetivos claros y medibles relacionados con la seguridad y la privacidad de la información. También resalta la importancia de integrar la identificación y evaluación de riesgos en la planificación. Esto implica reconocer las amenazas y vulnerabilidades desde el comienzo, permitiendo una gestión proactiva en lugar de reactiva.

MIPG promueve la ejecución de acciones concretas y su seguimiento constante estableciendo indicadores que permitan evaluar la eficacia de las medidas de seguridad y privacidad implementadas fomenta la toma de decisiones basada en datos y evidencias, lo que es crucial para gestionar adecuadamente los riesgos asociados con la información. Incluye además un enfoque de mejora continua, que permite a la Entidad revisar y ajustar su plan de tratamiento de riesgos de manera regular. Finalmente, facilita la transparencia en la gestión de riesgos, promoviendo una cultura de rendición de cuentas y confianza entre los ciudadanos y la Entidad.

A través de este documento, la Entidad, asegura que las acciones emprendidas sean efectivas, coherentes y alineadas con las metas de desarrollo de la organización, reafirmando su compromiso con la seguridad de la información y la protección de datos, garantizando que se implementen las medidas necesarias para salvaguardar la confianza de nuestros usuarios y cumplir con las expectativas de la sociedad.

2. INTRODUCCIÓN

La información que forma parte de una entidad pública es fundamental para su adecuado funcionamiento en el marco de la política pública y su conexión con los ciudadanos. No importa la naturaleza específica de la información manejada por la entidad; esta juega un papel esencial en el logro de sus objetivos. Por esta razón, proteger toda la información contra cualquier amenaza potencial, como alteraciones, mal uso o pérdida, entre

otros eventos, se convierte en una medida crucial. Este resguardo no solo actúa como una salvaguarda, sino que también respalda el desarrollo normal de las actividades de la entidad o del Estado en su conjunto.

En el Marco de Seguridad del Modelo de Seguridad y Privacidad de la Información (MSPI),el cual imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), un aspecto fundamental es la Gestión de Riesgos, la cual desempeña un papel crucial en la toma de decisiones. En este contexto, dado que las entidades del Estado son el enfoque principal del MSPI, se adopta la metodología de la " Guía para la Administración del Riesgo y el diseño de controles en entidades públicas" proporcionada por la Dirección de Gestión y Desempeño Institucional de la Función Pública. La intención es integrar esta guía con lo que se ha implementado previamente dentro de la Entidad en términos de otros modelos de gestión, aprovechando así el trabajo previo realizado en la identificación de riesgos para complementarlos con los riesgos específicos de seguridad de la información.

El proceso de gestión del riesgo es importante que se estructure en etapas fundamentales sobre las cuales se apoyen las actividades destinadas a lograr una administración de riesgos alineada con las necesidades de la Entidad. En primera instancia, se encuentra el compromiso de la alta y media dirección. Este compromiso se erige como un factor primordial, ya que el auténtico respaldo de los directivos asegura en gran medida el éxito de cualquier iniciativa. La necesidad de contar con la aprobación de la dirección en cada fase del proceso se presenta como un requisito ineludible, consolidando así una gestión del riesgo eficaz.

En segunda instancia, la conformación de un equipo MECI o de un grupo interdisciplinario presenta la idea de abordar integralmente los riesgos implica la necesidad de contar con un equipo que represente diversas áreas de la Entidad. Esta diversidad permite obtener una visión completa de la Entidad al analizar un mismo proceso. Es crucial incorporar los riesgos de seguridad durante el análisis del MECI o del modelo de Gestión de Calidad, alineando así los objetivos del MSPI.

Finalmente, la capacitación en la metodología, aunque es necesaria para que el equipo interdisciplinario pueda analizar los riesgos de seguridad, es vital que este equipo esté integrado por miembros del proyecto MSPI. Esto garantiza un conocimiento profundo del contexto organizacional en todos los aspectos del desarrollo del MSPI, permitiendo una implementación efectiva y coherente con los objetivos establecidos.

Con la creciente digitalización y el uso de tecnologías de la información, es imperativo establecer un marco robusto que permita anticipar y responder a los riesgos emergentes. Por ello, este Plan no solo busca proteger los activos informáticos, sino también fomentar una cultura de seguridad y privacidad entre todos los integrantes de la Entidad, asegurando así que la información se maneje con el respeto y la responsabilidad que merece.

3. ALCANCE

Este documento comenzará con el proceso de identificación de los riesgos de información asociados a las operaciones y servicios de la Entidad. A lo largo de su desarrollo, se abordará de manera integral la evaluación

y clasificación de estos riesgos. Finalmente, culminará con la implementación del Plan diseñado específicamente para mitigar y gestionar eficazmente dichos riesgos.

4. OBJETIVOS

4.1. GENERAL

Desarrollar e implementar un plan integral que permita identificar, evaluar, gestionar y mitigar los riesgos relacionados con la seguridad y la privacidad de la información en la Empresa Social del Estado Universitaria del Atlántico, garantizando así la protección de los datos, la confianza de los usuarios y el cumplimiento de las normativas vigentes, contribuyendo a la mejora continua de los procesos y servicios ofrecidos por la misma.

4.2. ESPECÍFICOS

- Realizar un inventario exhaustivo de los activos de información, identificando sus características, así como las amenazas y vulnerabilidades asociadas.

- Establecer procesos y procedimientos bien definidos para abordar cualquier evento de seguridad que pueda impactar la disponibilidad de los recursos informáticos críticos, asegurando que existan instrucciones claras y eficaces para manejar situaciones de seguridad, con el fin de garantizar la continuidad de los servicios informáticos esenciales, priorizando aquellos que requieren atención inmediata.

- Diseñar e implementar estrategias y controles específicos para mitigar los riesgos identificados, asegurando la protección de la información y la privacidad de los datos.

- Desarrollar programas de capacitación y sensibilización para todos los que hacen parte de la Entidad sobre la importancia de la seguridad y privacidad de la información, asegurando que comprendan sus roles y responsabilidades.

- Establecer mecanismos de monitoreo y auditoría para evaluar la efectividad de las medidas de seguridad implementadas y garantizar el cumplimiento de las políticas y procedimientos establecidos.

- Crear un plan de respuesta a incidentes que defina claramente los procedimientos a seguir en caso de una violación de la seguridad o un incidente de privacidad, incluyendo roles y responsabilidades.

- Implementar un proceso de revisión y actualización regular del Plan de Tratamiento de Riesgos, asegurando que se adapte a los cambios en el entorno de amenazas y a las normativas vigentes.

- Promover una cultura organizacional que valore la seguridad y privacidad de la información, incentivando la participación de todos los miembros de la entidad en la gestión de riesgos.

5. APLICABILIDAD

Este documento tiene una aplicabilidad integral que abarca todos los ámbitos de operación de la Entidad. Su alcance incluye no solo los procesos estratégicos y misionales, que son fundamentales para la consecución de los objetivos institucionales, sino también los procesos de apoyo que sustentan eficientemente las actividades clave. Además, se extiende a los procesos de evaluación, garantizando que las prácticas de identificación y tratamiento de riesgos se integren de manera coherente en todos los niveles y funciones de la E.S.E.

6. MARCO LEGAL Y NORMATIVO

- Decreto 1360 de 1989 Presidencia de Colombia. "*Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor".*
- Ley 572 de 1999 Congreso de la República Comercio Electrónico, Firmas Digitales, Intercambio electrónico de datos.
- Documento Conpes 3072 de 2000 Conpes Agenda de Conectividad.
- Decreto 3816 de 2003 Presidencia de Colombia. *"Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública".*
- Ley 1273 de 2009 Congreso de la República*. "Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".*
- Conpes 3701 de 2011. Lineamientos de política para la Ciberseguridad y Ciberdefensa.
- Ley 1581 de 2012 Congreso de la República. *"Por el cual se dictan disposiciones generales para la protección de datos personales".*
- Ley 1712 de 2014 Congreso de la República. *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".*
- Ley 2294 de 2023 Congreso de la República. *"Por el cual se expide el plan nacional de desarrollo 2022-2026 "Colombia potencia mundial de la vida".*
- Decreto 1078 de 2015 Presidencia de Colombia. *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".*
- Decreto 415 de 2016 Departamento Administrativo de la Función Pública. Se modifica el Decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.
- Decreto 728 de 2017 Ministerio de las Tecnologías de la Información y las Comunicaciones. *"Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de las zonas de acceso público a internet inalámbrico".*
- Resolución 2710 de 2017 Ministerio de las Tecnologías de la Información y las Comunicaciones. *"Por la cual se establecen lineamientos para la adopción del protocolo IPv6".*
- Decreto 1008 de 2018 Ministerio de las Tecnologías de la Información y las Comunicaciones. "*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de*

Tecnologías de la Información y las Comunicaciones Circular 2 de 2018 Ministerio de las Tecnologías de la Información y las Comunicaciones Cumplimiento legal y normativo respecto a seguridad de la información".

- Conpes 3920 de 2018 Conpes Big Data, la política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales. Guía 6 de 2019 Ministerio de las Tecnologías de la Información y las Comunicaciones Guía para la construcción del Plan Estratégico de Tecnologías de Información PETI. Ley 1955 del 2019 Presidencia de Colombia Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Conpes 3975 de 2019. Conpes Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
- Decreto 612 de 2018. "*Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del Estado".*

7. MARCO CONCEPTUAL Y TEÓRICO

7.1. DEFINICIONES

- **Acceso a la información pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo:** En el contexto de la seguridad de la información, se hace referencia a cualquier dato o componente vinculado con su manejo (sistemas, dispositivos de almacenamiento, instalaciones, personal, entre otros) que posea importancia para la organización, según la norma ISO/IEC 27000. En términos más específicos, un Activo de Información se define en el ámbito de la seguridad de la información como cualquier dato o componente que tiene valor para los procesos de la organización.
- **Amenazas:** Se refiere a una circunstancia que podría desencadenar un evento no deseado y, como consecuencia, ocasionar perjuicios a un sistema o a la organización. Esta definición se encuentra en concordancia con la norma ISO/IEC 27000.
- **Administración del riesgo:** Se refiere a un conjunto de mecanismos de control que, al interactuar entre sí, proporcionan a la entidad la capacidad para tomar las medidas necesarias. Esto permite gestionar eventos que podrían tener impactos negativos en el logro de los objetivos institucionales y proteger a la entidad de los efectos derivados de su ocurrencia.
- **Auditoría:** Procedimiento planificado y organizado de manera sistemática, independiente y debidamente registrado. Su propósito es obtener pruebas de auditoría con el fin de evaluar hasta qué

punto se cumplen los criterios de auditoría establecidos. Este enfoque sigue las pautas de la norma ISO/IEC 27000.

- **Causa:** Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes 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.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Datos abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).
- **Disponibilidad:** Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).
- **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- **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.
- **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo. Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados. Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).
- **Información:** Conjunto de datos que tienen un significado.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **Modelo Integrado de Planeación y Gestión -MIPG:** En su versión actualizada se define como un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.
- **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 control o las diferentes auditorías de los sistemas integrados de gestión.
- **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.
- **Probabilidad:** Posibilidad de que una amenaza se materialice.

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL (Gobierno en Línea - Decreto 1151 de 2008) la correlativa obligación.
- **Proceso:** Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
- **Procedimiento:** Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Riesgo de seguridad de la información**: se refiere a la posibilidad de que una amenaza específica pueda explotar una vulnerabilidad, resultando en la pérdida o daño de un activo de información. Estos daños se manifiestan en la afectación de la confidencialidad, integridad o disponibilidad de la información.
- **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 de los controles de seguridad de la información sobre cada uno de los procesos.
- **Seguridad de la Información**: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.
- **Tratamiento del Riesgo:** Proceso para modificar el riesgo (Icontec Internacional, 2011).
- **Valoración del Riesgo**: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos. Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

8. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

8.1. CONDICIONES GENERALES

Este Plan se propone realizar un análisis exhaustivo de los riesgos, abarcando desde la documentación hasta el diseño de recomendaciones, procedimientos y controles de seguridad en el ámbito del acceso a la información, tanto interna como externa. Es crucial destacar que no se establece un límite máximo o mínimo en la identificación de riesgos. La Entidad se compromete a identificar cualquier riesgo que pueda afectar el

logro de los objetivos de los procesos, sistemas de gestión, estándares, grupos de estándares y/o ejes trazadores de acreditación trazados.

La identificación se llevará a cabo de manera objetiva para garantizar una evaluación precisa. La toma de decisiones estratégicas será fundamental en la gestión efectiva de riesgos, considerando opciones como la aceptación del riesgo con acciones para reducir su probabilidad o impacto, la transferencia a terceros, la eliminación mediante la interrupción de actividades causantes del riesgo, y la implementación de controles para mitigar riesgos identificados. Además, la Entidad implementará procesos de formación y capacitación para desarrollar competencias en gestión del riesgo, fortaleciendo así la capacidad del personal para afrontar y mitigar eficazmente los riesgos.

8.2. PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Este proceso está adaptado a las necesidades específicas de la Entidad y debe ser un esfuerzo constante para garantizar la seguridad y privacidad de la información.

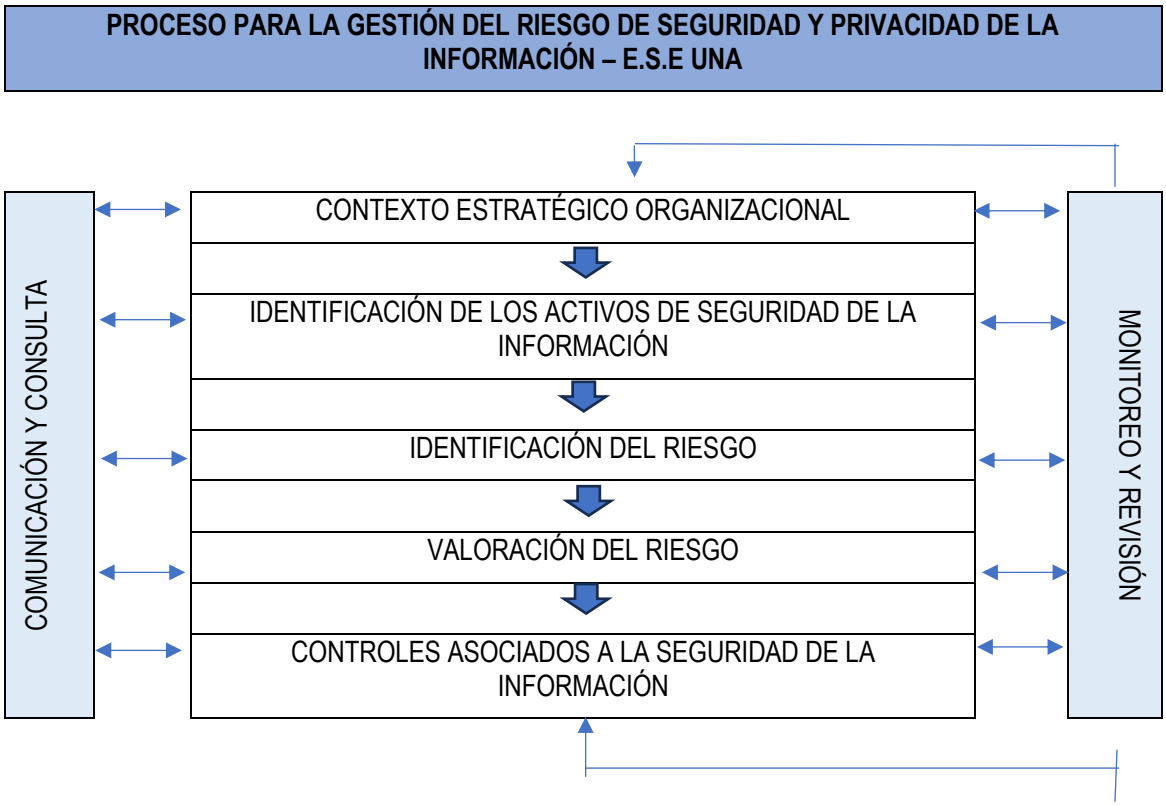


Gráfico 1. *Proceso para la gestión del riesgo de seguridad y privacidad de la información E.S.E UNA.*

Basado en lo anterior, se describe cada etapa del proceso a continuación.

8.2.1. Establecimiento del Contexto para la Gestión del Riesgo de Seguridad y Privacidad de la Información

Implica obtener una comprensión integral de los riesgos que podrían afectar el logro de los objetivos en estas áreas específicas. Este proceso implica una evaluación detallada de:

- La estructura organizacional.
- El modelo de operación por procesos
- El cumplimiento de planes y programas
- Los recursos físicos y tecnológicos disponibles

Para llevar a cabo este análisis, es esencial definir criterios específicos que permitan evaluar y cuantificar los riesgos asociados a la seguridad y privacidad de la información. Estos criterios actúan como marco de referencia para identificar, medir y gestionar los riesgos de manera efectiva en consonancia con los objetivos organizacionales y los estándares de seguridad y privacidad.

CRITERIOS

Criterios Generales

Estos criterios abordan aspectos generales relacionados con la naturaleza y magnitud del riesgo. Pueden incluir consideraciones sobre la probabilidad de ocurrencia, el impacto potencial y la tolerancia de la organización hacia ciertos niveles de riesgo.
Aspectos Legales y Reglamentarios: Los criterios de aceptación del riesgo pueden estar influenciados por el cumplimiento de requisitos legales y reglamentarios. Si un riesgo no contraviene normativas establecidas, podría ser aceptado en ciertos contextos.

Operaciones: Se considera la viabilidad de las operaciones frente al riesgo. Si un riesgo no impide de manera significativa las operaciones diarias y no afecta críticamente los procesos clave, podría ser aceptado.

Tecnología: Los criterios relacionados con la tecnología abordan la capacidad de los sistemas y tecnologías de la organización para mitigar o gestionar el riesgo. Si los sistemas existentes pueden tolerar o compensar el riesgo de manera efectiva, podría ser aceptado.

Finanzas: Los aspectos financieros son esenciales en la toma de decisiones sobre la aceptación del riesgo. Se evalúa si la organización tiene recursos financieros para mitigar el riesgo o si es más viable aceptarlo sin incurrir en costos significativos.

Factores Sociales y Humanitarios: Este criterio considera los aspectos sociales y humanitarios relacionados con la aceptación del riesgo. Puede incluir la evaluación de posibles impactos negativos en la comunidad, en la fuerza laboral y en otros grupos de interés.

Este criterio proporciona a la E.S.E. UNA, una guía clara para decidir cuándo un riesgo puede ser aceptado sin la necesidad de implementar medidas adicionales de mitigación.

Criterios de Evaluación del Riesgo

Los criterios de evaluación del riesgo en seguridad de la información constituyen un enfoque integral para determinar los riesgos a los que se enfrenta la E.S.E. Universitaria del Atlántico. Se consideran diversos aspectos clave:

- **Valor Estratégico del Proceso de Información:** Este criterio implica analizar la importancia estratégica del proceso de información en el contexto general de la E.S.E.UNA. Se evalúa cómo la seguridad de la información impacta directamente en los objetivos y metas estratégicas de la organización.
- **Criticidad de los Activos de Información:** La criticidad de los activos de información involucrados en el proceso es un factor crucial. Se examina la importancia de los datos y recursos específicos que son esenciales para el funcionamiento y la continuidad de las operaciones de la organización.
- **Requisitos Legales y Reglamentarios, así como Obligaciones Contractuales:** Este criterio aborda el cumplimiento de los requisitos legales y reglamentarios aplicables, así como las obligaciones contractuales relacionadas con la seguridad de la información. Se busca garantizar que la E.S.E. UNA cumpla con las normativas y acuerdos contractuales establecidos.
- **Importancia de la Disponibilidad, Confidencialidad e Integridad de la Información:** La evaluación de la importancia de la disponibilidad, confidencialidad e integridad de la información destaca la relevancia de preservar estos principios fundamentales de la seguridad de la información para asegurar el buen funcionamiento de las operaciones y la integridad de la E.S.E. UNA.
- **Expectativas y Percepciones de las Partes Interesadas:** Se considera la perspectiva de las partes interesadas, evaluando sus expectativas y percepciones en relación con la seguridad de la información. Esto asegura que se tenga en cuenta la satisfacción y confianza de los involucrados en la toma de decisiones.
- **Consecuencias Negativas para el Buen Nombre y la Reputación de la E.S.E. UNA:** Este criterio destaca la importancia de proteger la reputación y el buen nombre de la E.S.E. UNA. Se evalúan las posibles consecuencias negativas que podrían surgir en caso de incidentes de seguridad que afecten la percepción pública.

La inclusión de estos criterios en la evaluación del riesgo brinda una perspectiva completa, permitiendo a la E.S.E. UNA tomar decisiones informadas sobre las medidas de mitigación y control necesarias para salvaguardar la seguridad de la información y mantener una reputación sólida.

Criterios de Impacto del Riesgo

Los criterios de impacto del riesgo son parámetros específicos que se definen en función del grado de daño o de los costos que la E.S.E. UNA podría experimentar como consecuencia de un evento de seguridad de la información. Estos criterios consideran diversos aspectos clave para evaluar el impacto potencial:

- **Nivel de Clasificación de los Activos de Información de los Procesos:** Este criterio se enfoca en la importancia y clasificación de los activos de información asociados a los procesos de la E.S.E. UNA. La pérdida o compromiso de información clasificada conlleva un mayor impacto en la seguridad.
- **Brechas en la Seguridad de la Información:** Se evalúa el impacto de las brechas en la seguridad, como la pérdida de confidencialidad, integridad o disponibilidad de la información. Estas brechas pueden tener consecuencias significativas en la operación y reputación de la E.S.E. UNA.
- **Operaciones Deterioradas:** Se considera el impacto en las operaciones cotidianas de la E.S.E. UNA. Interrupciones o deterioro en las operaciones pueden afectar la eficiencia y la capacidad de cumplir con sus funciones.
- **Pérdida de la Misión y del Valor Financiero**: Este criterio evalúa cómo un evento de seguridad podría comprometer la misión de la entidad y afectar su valor financiero. La pérdida de la misión puede tener consecuencias a largo plazo en la identidad y objetivos de la organización.
- **Alteración de Planes y Fechas Límites**: Se examina cómo un evento de seguridad podría alterar los planes estratégicos y las fechas límites establecidas por la entidad. Cambios en la planificación pueden tener implicaciones en la consecución de objetivos.
- **Daños para la Reputación**: Este criterio evalúa el impacto en la reputación de la E.S.E. UNA. Daños a la reputación pueden resultar en pérdida de confianza por parte de clientes, socios y partes interesadas, afectando las relaciones comerciales y la percepción pública.
- **Incumplimiento de Requisitos Legales**: Se considera el impacto de un evento de seguridad en el cumplimiento de requisitos legales y reglamentarios. El incumplimiento puede dar lugar a sanciones legales y multas, afectando la posición legal de la entidad.

La definición precisa de estos criterios proporciona una base sólida para la evaluación del impacto del riesgo, permitiendo a la Entidad tomar decisiones informadas en la gestión de la seguridad de la información y la mitigación de posibles consecuencias adversas.

Criterios de Aceptación del Riesgo

Son pautas establecidas para determinar en qué condiciones un riesgo puede ser aceptado sin implementar medidas adicionales de mitigación. Estos criterios pueden variar según la expectativa de duración del riesgo.

8.2.2. Identificación de los Activos de Seguridad de la Información Activos

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:

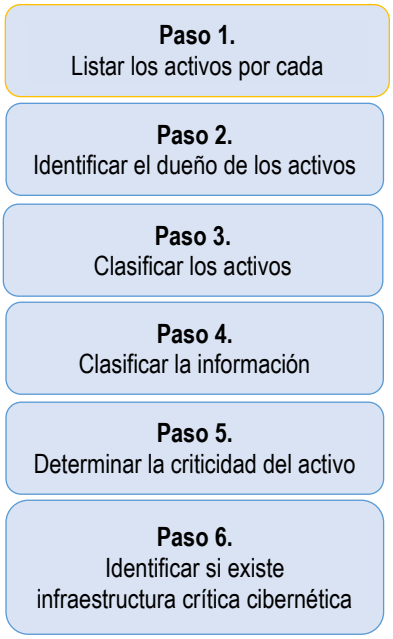
- Aplicaciones de la organización
- Servicios web
- Redes -Información física o digital
- Tecnologías de información TI
- Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital

¿POR QUÉ IDENTIFICAR LOS ACTIVOS?

Facilita la identificación de los activos más críticos de la Entidad y sus procesos tienen, ya sean bases de datos, archivos, servidores web o aplicaciones esenciales para la prestación de sus servicios.

Así las cosas, la identificación de los activos de seguridad de la información, se refiere al proceso de reconocer y catalogar todos los elementos de valor para la Entidad. En el contexto de la seguridad de la información, según la norma ISO 27001:2013, un activo es cualquier cosa que posea valor y requiera protección. Esta identificación debe llevarse a cabo con un nivel de detalle suficiente para proporcionar la información necesaria para la evaluación de riesgos.

PASOS PARA IDENTIFICAR LOS ACTIVOS



Fuente: *Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018. Tomado de Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6, Función Pública.*

TIPOS DE ACTIVOS

TIPO DE ACTIVO	DESCRIPCIÓN
Bases de Datos	Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, puede ser utilizada en un formato de motor ya sea SQL, SQL Server, MySQL o en formato Excel. Ejemplos: Bases de datos con información personal o con datos relevante para algún proceso (bases de datos de nóminas, Base de datos Aprendices, Listado de proveedores, estados financieros) entre otros.
Datos / Información	Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. Ejemplo: Copias de Respaldo, Ficheros, Datos de Gestión Interna, Datos de Configuración, Credenciales (Contraseñas), Datos de Validación de Credenciales (Autenticación), Datos de Control de Acceso, Registros de Actividad (Log), Matrices de Roles y Privilegios, Código Fuente, Código Ejecutable, Datos de Prueba, Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, formatos o formularios físicos o digitales.
Equipos Auxiliares	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos. Ejemplo: Fuentes de alimentación, generadores eléctricos, equipos de climatización, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, equipos de destrucción de soportes de información, mobiliarios, armarios, cajas fuertes.
Hardware / Infraestructura	Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Dispositivos Móviles, Equipos de Respaldo, Periféricos, Dispositivos Criptográficos, Dispositivos Biométricos, Servidores de Impresión, Impresoras, Escáneres, Equipos Virtuales (host), Soporte de la Red (Network), Módems, Concentradores, Conmutadores (switch), Encaminadores (router), Pasarelas (bridge), Firewall, Central Telefónica, Telefonía IP, Access Point.
Instalaciones	Lugares donde albergan los sistemas de información y comunicaciones.

Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.
Redes de Comunicaciones	Infraestructuras dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro. Ejemplo: Red Telefónica, Red Inalámbrica, Telefonía Móvil, Satelital, Red Local (LAN), Red Metropolitana (MAN), Internet, Radio Comunicaciones, Punto a Punto, ADSL, Red Digital (RDSI).
Servicios	Funciones que permiten suplir una necesidad de los usuarios del servicio (internos o externos) Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, Gestión de Identidades (altas y bajas de usuarios del sistema), Gestión de Privilegios, Intercambio electrónico de datos, PKI (Infraestructura de Clave Pública). o servicios relacionados con la misión de la Entidad, servicios relacionados con los prestados por la Entidad hacia los grupos de valor, servicios relacionados para el desarrollo de las funciones de grupos de interés
Software / Aplicaciones Informáticas	Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. Ejemplo: Aquellos utilizados para la enseñanza, para el desarrollo de aplicaciones, para la gestión o administración de bases de datos, para la gestión o administración de documentos, para la gestión del correo electrónico, para la navegación web, para el desarrollo de aplicaciones propias, para la gestión de respaldos de información, para la prevención de virus o infecciones informáticas, para conexiones o trabajos remotos, entre otros.
Soportes de Información	Dispositivos físicos o electrónicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo y que posteriormente permiten recuperar la información contenida en ellos. Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.

CLASIFICACIÓN VALORACIÓN DE LOS ACTIVOS

CRITICIDAD RESPECTO A SU CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

VALOR	CONFIDENCIALIDAD

ALTO	**Pública Reservada / Confidencial:** Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica. Por lo tanto, cuando un activo de información realice tratamiento de datos personales privados o sensibles el activo de Información deberá ser calificado como activo de información pública confidencial (ALTO).
MEDIO	**Pública Clasificada / Uso Interno**: Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario. Por lo tanto, cuando un activo de información realice tratamiento de datos personales semiprivados, el activo de Información deberá ser calificado por lo menos como un activo de información pública de uso interno (MEDIO).
BAJO	**Pública / Pública:** Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
SIN CLASIFICAR	**SIN CLASIFICAR**: Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de Información Pública Reservada. (Alta).
VALOR	**INTEGRIDAD**
ALTO	**ALTO**: información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones o generar pérdidas de imagen severas de la Entidad.
MEDIO	**MEDIO**: información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado para la Entidad.
BAJO	**BAJO**: información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la Entidad o entes externos.
SIN CLASIFICAR	**SIN CLASIFICAR**: Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.
VALOR	**DISPONIBILIDAD**
ALTO	**ALTO**: La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.

MEDIO	**MEDIO**: La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
BAJO	**BAJO**: La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
SIN CLASIFICAR	**SIN CLASIFICAR**: Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

MATRIZ DE IDENTIFICACIÓN DE ACTIVOS DE PROCESOS

Proceso	Nombre del Activo	Descripción del Activo	Dueño del Activo	Tipo de Activo	Ley 1712 de 2014 - clasificación de la información	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	BAJA	BAJA	BAJA	BAJA

Tabla 1. *Ejemplo identificación activos del proceso. Tomado de Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6, Función Pública.*

8.2.3. Identificación del Riesgo

Los riesgos asociados al uso de tecnologías de información y comunicaciones que podrían impactar de manera total o parcial en el adecuado funcionamiento de los sistemas y servicios informáticos de la E.S.E. Universitaria del Atlántico resaltan la necesidad de identificar los procesos críticos dentro de la entidad. Este enfoque implica reconocer las operaciones y funciones más vitales para el E.S.E. UNA, con el propósito de establecer procedimientos alternos que aseguren la continuidad en la operación informática ante posibles interrupciones. La identificación de estos procesos críticos permite implementar medidas específicas de resiliencia y contingencia, garantizando que, incluso en situaciones adversas, la entidad pueda mantener sus funciones esenciales y preservar la integridad de los servicios informáticos críticos.

La identificación del riesgo tiene como objetivo principal discernir los posibles eventos que podrían ocasionar una pérdida potencial. Este proceso busca comprender en detalle el cómo, dónde y por qué podría materializarse dicha pérdida. En esencia, se trata de anticipar y reconocer cualquier circunstancia o evento que tenga el potencial de generar consecuencias adversas para la organización. La identificación del riesgo implica

un análisis exhaustivo para determinar escenarios posibles, sus causas subyacentes y la naturaleza de las pérdidas que podrían derivarse, lo que proporciona una base sólida para la gestión y mitigación efectiva de los riesgos identificados.

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, es necesario vincular el grupo de activos o los activos concretos del proceso, y analizar en conjunto las amenazas y vulnerabilidades que podrían llevar a su realización.

DETERMINACIÓN DE ÁREAS DE RIESGO INFORMÁTICO

La identificación de áreas de riesgo informático en la Entidad se centrará en las tecnologías de información y comunicaciones esenciales para el cumplimiento de su misión. Las áreas principales de riesgo incluyen las bases de datos, servicios de información y administrativos, y la seguridad informática (comunicaciones), que están estrechamente interrelacionadas.

IDENTIFICACIÓN DE LAS AMENAZAS: Implica reconocer y evaluar las posibles fuentes de peligro que podrían causar daños a los activos de la Entidad, incluyendo información, procesos y sistemas. Estas amenazas pueden surgir tanto de eventos naturales como de acciones humanas, y pueden ser accidentales o intencionales. Es crucial identificar todos los posibles orígenes de amenazas, ya sean accidentales o deliberados, para tener una comprensión completa de los riesgos a los que se enfrenta la entidad. Es recomendable clasificar las amenazas de manera genérica y por tipo, por ejemplo, acciones no autorizadas, daño físico o fallas técnicas.

IDENTIFICACIÓN DE LAS VULNERABILIDADES: La identificación de vulnerabilidades es el proceso sistemático de reconocer y catalogar debilidades, fallos o puntos susceptibles en los sistemas, procesos, procedimientos, recursos humanos y tecnológicos de una organización que podrían ser explotados por amenazas para causar daño o pérdida. Este proceso implica analizar exhaustivamente diversos aspectos, como la infraestructura tecnológica, las prácticas organizativas, las configuraciones de sistemas y la capacitación del personal, con el objetivo de identificar áreas donde la seguridad puede ser comprometida.

Es importante mencionar que, la sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

AMENAZA	VULNERABILIDAD
	Controles de acceso a centros de datos inadecuados

MEDIO AMBIENTE E INFRAESTRUCTURA	Suministro eléctrico inestable
	Desastres naturales
	Desastres causados por el hombre
	Inadecuado sistema de prevención de atención de desastres
RECURSO HUMANO	Contratación inadecuada
	Ausentismo
	Roles y responsabilidades inadecuados – Falta de conciencia alrededor de la seguridad informática
	Falta de capacitación
	Falta de procedimientos oficiales
	Desastres ocasionados por el hombre
SOFTWARE	Falta de conciencia alrededor de la seguridad informática.
	Software malicioso
	Exposición de contraseñas de acceso a servicios informáticos
	Exposición de contraseñas de acceso a servicios informáticos
HARDWARE	Daño
	Degradación
	Plan de mantenimiento inapropiado
	Suministro eléctrico inestable
COMUNICACIONES	Falta de esquemas de alta disponibilidad (respaldo)
	Administración de red inadecuada
DATOS (INFORMACIÓN)	Inadecuada clasificación de activos
	Software malicioso
	Protección inadecuada de bases de datos
	Falta de plan de procedimientos y software de respaldo

IDENTIFICACIÓN DE LAS CONSECUENCIAS: La identificación de las consecuencias implica un proceso integral que requiere dos elementos clave: una lista de activos de información y su relación con los procesos de la entidad, así como una lista de amenazas y vulnerabilidades en relación con esos activos y su relevancia. Es crucial reconocer que las consecuencias pueden abarcar desde la pérdida de eficacia y condiciones adversas de operación hasta daños en la reputación. En este proceso, se deben identificar las consecuencias operativas de los posibles escenarios de incidentes, considerando factores como el tiempo necesario para la

investigación y reparación, la pérdida de tiempo operacional, oportunidades, riesgos para la salud y seguridad, costos financieros y el impacto en la imagen y reputación de la entidad. Esta evaluación detallada permite una comprensión holística de las repercusiones potenciales, facilitando así la implementación de medidas preventivas y correctivas efectivas.

Riesgo	Activo	Descripción del Riesgo	Amenaza	Tipo	Causa/Vulnerabilidad	Consecuencias
Base de datos de Nómina	Pérdida de la integridad	La falta de políticas de seguridad, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la perdida de la integridad de la base de datos de nómina	Modificación no autorizada	Seguridad digital	✓ Falta de políticas de seguridad digital ✓ Ausencia de políticas de control de acceso ✓ Contraseñas sin protección ✓ Autenticación débil	Retraso en el pago de nómina

Tabla 3. *Formato de descripción del riesgo de seguridad de la información. Tomado de Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6, Función Pública.*

8.2.4. Valoración del Riesgo

En la valoración se evalúan tanto la probabilidad de ocurrencia como el impacto en caso de que ocurran. Este proceso permite priorizar los riesgos y determinar cuáles requieren una atención inmediata, se parte del contexto estratégico de la Entidad, que implica reconocer tanto las situaciones de riesgo internas como externas.

Al considerar los factores internos y externos, se determinan los agentes generadores de riesgo en el ámbito de la seguridad y privacidad de la información. Se analizan las causas subyacentes y las posibles consecuencias, que pueden incluir pérdida, daño, perjuicio o detrimento. Este enfoque integral permite una comprensión profunda de los riesgos asociados, lo que facilita la toma de decisiones informadas y la implementación de medidas adecuadas para gestionar y mitigar dichos riesgos.

ANÁLISIS DE RIESGOS

El análisis de riesgos es un proceso detallado que implica evaluar las posibles consecuencias o efectos derivados de la ocurrencia de riesgos, tomando en consideración los objetivos específicos de la Entidad. Estas consecuencias pueden manifestarse en diversas formas, ya sea afectando a personas, bienes materiales o aspectos intangibles como la imagen y el prestigio corporativo. Durante este análisis, se examinan

minuciosamente los posibles escenarios de riesgo y se cuantifican sus impactos en relación con los objetivos institucionales y los activos críticos. Este enfoque permite una comprensión más profunda de las repercusiones potenciales, lo que facilita la toma de decisiones informadas sobre la gestión y mitigación de riesgos para garantizar la continuidad operativa y la protección integral de la Entidad.

Para realizar el análisis se utiliza las siguientes tablas para evaluar la probabilidad y el impacto:

CRITERIOS PARA CLASIFICAR LA PROBABILIDAD DE OCURRENCIA DEL RIESGO

CALIFICACIÓN	VARIABLE
REMOTA	Improbable que ocurra (no ha ocurrido en los últimos 5 años)
RARO	Posible que ocurra en algún momento (puede ocurrir al menos una vez en los últimos 5 años)
OCASIONAL	Probablemente ocurrirá (puede suceder al menos una vez en los últimos dos años)
FRECUENTE	Probablemente ocurrirá en la mayoría de las circunstancias (al menos una vez en el último año)
CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias (más de una vez al año)

CRITERIOS PARA LA CALIFICACIÓN DEL IMPACTO DEL RIESGO

CALIFICACIÓN	VARIABLE
INSIGNIFICANTE	Las consecuencias de los riesgos, si ocurren no afectan a ningún proceso de la Entidad
MENOR	Las consecuencias de los riesgos, si ocurren, afectan levemente a la Entidad y pueden pasar desapercibidas para el paciente y no afectan la prestación del servicio ni la imagen institucional. En equipos o instalaciones daños por cuantía menor a 150 SMLMV.
MODERADO	Las consecuencias de los riesgos pueden afectar parcialmente los procesos y servicios de la Entidad, pero las pérdidas y daños son menores y no afectan la imagen institucional. En equipos o instalaciones daños por cuantía de 150 a 450 SMLMV.
MAYOR	Las consecuencias de los riesgos pueden afectar de manera importante los procesos y servicios de la Entidad y afectarse igualmente la imagen institucional. En equipos o instalaciones daños por cuantía de 450 a 1500 SMLMV

CATASTROFICO	Las consecuencias pueden afectar totalmente a la E.S.E UNA produciendo daños recuperables y afectarse la imagen institucional de manera grave. En equipos o instalaciones daños por cuantía superior a 1500 SMLMV.

Con el propósito de facilitar la calificación y evaluación de los riesgos, se utiliza una matriz que aborda un análisis cualitativo. Esta matriz proporciona una representación visual de la magnitud de las posibles consecuencias (impacto) y la probabilidad de que ocurran (probabilidad). Al emplear este enfoque, se logra una comprensión más clara y estructurada de la importancia relativa de los riesgos, permitiendo una toma de decisiones informada para priorizar la gestión y mitigación de los riesgos identificados.

		IMPACTO *¿Qué tan severos serían los resultados si ocurriera el riesgo?*				
PROBABILIDAD ¿Cuál es la probabilidad de que ocurra el riesgo?		**INSIGNIFICANTE**	**MENOR**	**MODERADO**	**ALTO**	**CATASTRÓFICO**
	CASI SEGURO	**A**	**A**	**E**	**E**	**E**
	FRECUENTE	**M**	**A**	**A**	**E**	**E**
	OCASIONAL	**B**	**M**	**A**	**E**	**E**
	RARO	**B**	**B**	**M**	**A**	**E**
	REMOTA	**B**	**B**	**M**	**A**	**A**

B: Zona de riesgo baja: Asumir el riesgo

M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo

A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir

E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir

Riesgo	**Activo**	**Amenaza**	**Causa/Vulnerabilidad**	**Probabilidad**	**Impacto**	**Zona de Riesgo**
Perdida de la confidencialidad	Base de datos de nómina	Modificación no autorizada	✓ Ausencia de políticas de control de acceso ✓ Contraseñas sin protección ✓ Autenticación débil	Ocasional	Alto	Extremo

Tabla 4. *Ejemplo valoración del riesgo. Tomado de Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6, Función Pública.*

TRATAMIENTO DEL RIESGO

El tratamiento de riesgos es el proceso integral que sigue a la identificación y se centra en la toma de decisiones para mitigar o gestionar los riesgos identificados. En este contexto, se lleva a cabo un análisis detallado de las posibles acciones a emprender, asegurándose de que sean factibles y efectivas. Estas acciones pueden incluir la implementación de políticas, la definición de estándares, la optimización de procesos y procedimientos, así como cambios físicos, entre otras medidas. La esencia del tratamiento de riesgos radica en la capacidad de tomar decisiones informadas y estratégicas basadas en los resultados obtenidos durante la identificación y análisis de riesgos.

El objetivo final es reducir la probabilidad de ocurrencia o el impacto de los riesgos, garantizando así la seguridad y la continuidad efectiva de las operaciones de la entidad.

ACEPTACIÓN DEL RIESGO: En algunos casos, la Entidad puede decidir aceptar ciertos riesgos cuando los costos asociados con la mitigación son desproporcionados en comparación con el beneficio esperado. Sin embargo, esta aceptación debe ser informada y documentada adecuadamente.

ZONAS O NIVELES DE CRITICIDAD E INTERVENCIÓN DEL RIESGO		TRATAMIENTO
RIESGO BAJO	Dada su baja probabilidad de presentación, es posible asumir el riesgo, pero deben planearse acciones para reducirlo en caso de que se presente.	Asumir el riesgo
RIESGO MODERADO	Evaluada la probabilidad e impacto es posible asumir el riesgo, pero siempre acompañado de acciones para reducirlo y evitarlo en lo posible.	Asumir el riesgo, reducir el riesgo
RIESGO ALTO	En esta zona de riesgo alta debe siempre evitar, reducir, compartir o transferir el riesgo.	Reducir el riesgo, evitar, compartir o transferir
RIESGO EXTREMO	En esta zona de riesgo extrema debe siempre y de manera simultánea: evitarse el riesgo, reducirlo y compartir o transferir el riesgo. Los puntos de control deben ser más estrictos.	Reducir el riesgo, evitar, compartir o transferir.

IMPACTO DE CONFIDENCIALIDAD EN LA INFORMACIÓN: El impacto de confidencialidad de la información se refiere a la pérdida o revelación de esta. Cuando se habla de información reservada institucional se hace alusión a aquella que por la razón de ser de la E.S.E. solo puede ser conocida y difundida al interior de esta; así mismo, la sensibilidad de la información depende de la importancia que esta tenga para el desarrollo de la misión de la entidad.

IMPACTO DE CREDIBILIDAD O IMAGEN: El impacto de credibilidad se refiere a la pérdida de esta frente a diferentes actores sociales o dentro de la entidad.

IMPACTO LEGAL: El impacto legal se relaciona con las consecuencias legales para una entidad, determinadas por los riesgos relacionados con el incumplimiento en su función administrativa, ejecución presupuestal y normatividad aplicable.

IMPACTO OPERATIVO: El impacto operativo aplica en la mayoría de las entidades para los procesos clasificados como de apoyo, ya que sus riesgos pueden afectar el normal desarrollo de otros procesos.

8.2.5. Controles Asociados a la Seguridad de la Información

Una vez identificados y valorados los riesgos, se implementan estrategias para manejarlos. Esto incluye decidir cómo mitigar, transferir, aceptar o evitar los riesgos. Se desarrollan e implementan medidas de control y se establece un plan para gestionar los riesgos de manera efectiva.

La identificación de controles existentes se refiere al proceso de reconocer y evaluar las medidas de seguridad y salvaguardias ya implementadas en la Entidad. Este procedimiento busca evitar redundancias y gastos innecesarios, como la duplicidad de controles, al tiempo que garantiza la eficacia de los controles identificados. Además de simplemente identificarlos, se recomienda realizar una verificación para asegurarse de que los controles existentes funcionen correctamente.

Citamos algunos ejemplos relevantes de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI).

PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	**OBJETIVO: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información**
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de

	procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Tabla 5. *Controles para riesgos de seguridad de la información. Tomado de Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6, Función Pública.*

8.2.6. Comunicación del Riesgo

La comunicación efectiva es esencial en la gestión del riesgo. Se deben establecer canales de comunicación claros para informar a todas las partes interesadas sobre los riesgos identificados, las estrategias de tratamiento y los resultados de la gestión del riesgo.

Para ello la Entidad empleara una comunicación continua con:

- ✓ **Informes regulares**: Estableciendo un calendario para reportar el estado de los riesgos y tratamientos.
- ✓ **Capacitación**: Proporcionando formación a los empleados sobre la seguridad y privacidad de la información.

8.2.7. Monitoreo y Revisión del Riesgo

Este paso implica el seguimiento continuo de los riesgos identificados y las medidas de control implementadas. Se revisa periódicamente el contexto, se actualiza la valoración del riesgo y se ajustan las estrategias de tratamiento según sea necesario. La gestión del riesgo es un proceso iterativo y dinámico. El monitoreo y revisión son componentes esenciales en la gestión efectiva de riesgos, y su implementación seguirá un proceso

estructurado en la E.S.E. Universitaria del Atlántico. La supervisión iniciará con el responsable del proceso, que puede ser el Gerente o la Oficina Asesora de Planeación, quienes realizará el seguimiento inicial para asegurar la ejecución de las acciones planificadas y evaluar la eficiencia de su implementación.

En un segundo momento, el subgerente corporativo, realiza un seguimiento adicional. Este enfoque jerárquico garantiza una cobertura completa de los distintos aspectos de la Entidad.

La Oficina de Control Interno desempeñará un papel clave al comunicar y presentar los resultados y propuestas de mejora tras la evaluación. Se llevará a cabo al menos semestralmente, y se centrará en detectar situaciones que requieran tratamiento o ajuste. Además, cada responsable de proceso realiza autoevaluaciones periódicas para determinar la efectividad de los controles implementados y minimizar los riesgos. Simultáneamente, la Oficina de Control Interno emite su informe de evaluación de riesgos y controles de segundo orden. Este enfoque estructurado y jerárquico garantizará una supervisión continua y exhaustiva de la gestión de riesgos, facilitando la identificación temprana de posibles problemas y permitiendo la implementación proactiva de mejoras para fortalecer la resiliencia de la E.S.E. UNA frente a posibles riesgos.

Todo lo anterior, contribuye a un ciclo de mejora continua para perfeccionar el modelo de gestión de riesgos en seguridad de la información. Se aprovechan los resultados del monitoreo y las revisiones para ajustar y mejorar continuamente el enfoque de gestión de riesgos.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información debe ser adaptado constantemente a la realidad específica de la E.S.E. Universitaria del Atlántico, teniendo en cuenta sus activos, amenazas y vulnerabilidades particulares. Además, se solicita la participación de todas las partes interesadas en el proceso para asegurar una implementación efectiva y sostenible.

8.2.8. Acciones Ante los Riesgos Materializados

RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
RESPONSABLE	**ACCIÓN**
Líder de Proceso (director, Gerente, subgerente, jefe de Oficina)	✓ Informar a la Dirección de Planeación, como segunda línea de defensa, y a la Oficina de Control Interno, el evento o materialización de un riesgo. ✓ Proceder de manera inmediata a aplicar el plan de tratamiento de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso). ✓ Realizar los correctivos necesarios e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentando en el plan de tratamiento.
Jefe de Control Interno	✓ Informar al líder del proceso sobre el hecho encontrado y a la segunda línea de defensa en caso de detectarse en una auditoría. ✓ Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, se debe verificar que se tomen las acciones correctivas.

***Tabla 6**. Acciones ante los riesgos materializados.*

8.2.9. Plan de Trabajo

Las actividades para desarrollar dentro del Plan de Tratamiento de Riesgos y Seguridad de la Información de la E.S.E. Universitaria del Atlántico 2025 son:

Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
			Fecha Inicio	Fecha Final
Sensibilización	Socialización del Plan de Tratamiento de Riesgos y Seguridad de la Información de la E.S.E. Universitaria del Atlántico 2025	Dirección TIC	01 de Feb de 2025	01 de marzo de 2025
Actividades	**Tareas**	**Responsable de la Tarea**	**Fechas Programación Tareas**	
			Fecha Inicio	**Fecha Final**
Identificación de Activos de información	Envío de formato identificación de activos de información	Dirección TIC	01 de marzo de 2025	07 de marzo 2025
	Entrega de formato identificación de activos de información	Responsable de cada área o proceso	08 de marzo de 2025	30 de marzo 2025
	Realimentación, revisión y verificación de los activos de información (Ajustes)	Dirección TIC - Responsable de cada área o proceso	01 de abril de 2025	30 de abril de 2025
Identificación de Riesgos	Envío de formato identificación de riesgos de seguridad y privacidad de la información	Dirección TIC	01 de mayo de 2025	07 de mayo 2025
	Entrega de formato identificación de riesgos de seguridad y privacidad de la información	Responsable de cada área o proceso	08 de mayo de 2025	30 de mayo 2025
	Realimentación, revisión y verificación de los riesgos de	Dirección TIC - Responsable de	01 de junio de 2025	30 de junio de 2025

	seguridad y privacidad de la información (Ajustes)	cada área o proceso		
Valoración de Riesgos identificados y sus controles asociados	Reuniones con equipos de trabajo por área para la aceptación, aprobación de riesgos identificados y controles asociados.	Dirección TIC - Responsable de cada área o proceso	01 de julio de 2025	30 de agosto de 2025
Construcción de la Matriz de riesgos de seguridad y privacidad de la información de la Entidad	Envío de formato Matriz de riesgos de seguridad y privacidad de la información	Dirección TIC	01 de septiembre de 2025	07 de septiembre de 2025
	Entrega de formato Matriz de riesgos de seguridad y privacidad de la información	Responsable de cada área o proceso	08 de octubre de 2025	30 de octubre de 2025
Socialización de la Matriz de riesgos de seguridad y privacidad de la información	Socializar la Matriz a los colabores de la Entidad.	Dirección TIC	01 noviembre de 2025	01 de diciembre de 2025
Monitoreo y Revisión	Generación, presentación de informe sobre el proceso	Planeación - Dirección TIC	Diciembre 2025	Diciembre 2025

***Tabla 7**. Plan de trabajo.*

9. BIBLIOGRAFIA

Departamento Administrativo de la Función Pública. (2014). *Guía para la administración del riesgo*. Bogotá, Colombia.

Función Pública. (2022). *Guía para la administración del riesgo y el diseño de controles en entidades públicas* (Versión 6). Bogotá, Colombia.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). *Guía para la administración del riesgo y diseño de controles en entidades públicas* (Versión 5). Bogotá, Colombia.

Organización Internacional de Normalización (ISO). (2018). *Norma Internacional ISO 31000*. Ginebra, Suiza.

10. FICHA DE CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
01	28/01/2025	Creación del documento.

11. APROBACIÓN DEL DOCUMENTO

ELABORÓ	REVISÓ	APROBÓ
Nombre: Elena Roció El Pilar Moya Ramírez	**Nombre:** María Angélica Ahumada Figueroa	**Nombre:** Comité Institucional de Gestión y Desempeño
Cargo: Apoyo y Asesoría en la gestión de la Coordinación de Tecnologías de la Información	**Cargo:** Director(a) Tecnologías de la Información	**Cargo:** Comité Institucional de Gestión y Desempeño
Fecha: 28/01/2025	**Fecha:** 28/01/2025	**Fecha:** 31/01/2025