PLAN GENERAL PARA EL TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE LA INFORMACIÓN

2023

OFICINA DE TECNOLOGIA DE INFORMACIÓN

Elaborado:

Ing. Carlos Alberto Rodríguez

Tabla de Contenido

Pág.

Lista de Tablas.

Pág.

Lista de Graficas

Pág.

1. INTRODUCCIÓN.

Hoy día, las exigencias de la comunidad locales y la normativa internacional, impulsa a que las empresas estén inmersas en una revolución digital, pues la información tiene un principal protagonismo en todos los procesos productivos, por tanto, la importancia de tener su información adecuadamente identificada y protegida y enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

La institución decide entonces vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información, y como medio o herramienta para el logro de los objetivos de mantener la información de la Institución confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

- Confidencialidad: Propiedad que la información sea concedida únicamente a quien esté autorizado
- Integridad: Propiedad que la información se mantenga exacta y completa.
- Disponibilidad: Propiedad que la información sea accesible y utilizable en el momento que se requiera.

2. Marco de Referencia

2.1 Marco Normativo

Los recursos informáticos y de telecomunicaciones de la Institución son administrados por la oficina de Tecnologías de Información y Comunicaciones (DTIC) adscrita a la Rectoría de la UNIAJC. Esta oficina contribuye en la gestión de actividades académicas, investigativas y administrativas de la Institución a través del diseño, el desarrollo y la prestación de servicios de informática y telecomunicaciones, alineado con el objetivo estratégico de "modernizar la infraestructura física y tecnológica que garantice el adecuado servicio educativo" y con los objetivos estratégicos por área de desempeño de "infraestructura y equipamiento", y cumplir con los objetivos de las políticas gubernamentales como lo son la política del gobierno digital, las directrices del Conpes (3701, 3854, 2018 incluyendo la directriz 2021, 2022) que incentiva la confianza en el comercio electrónico y la interoperabilidad de datos entre las instituciones.

Un listado de las diferentes leyes que son el punto de partida para la elaboración de planes, guías y documentos organizacionales

2020	**LEY 2069 DE 2020**	**Por medio de la cual se impulsa el emprendimiento en Colombia; Art. 82 Par. 2l.**
	LEY 2066 DE 2020	Por medio de la cual se establecen condiciones especiales para la normalización de cartera por única vez para los concesionarios de los servicios de radiodifusión sonora de interés público y comunitario y para los operadores del servicio de televisión comunitaria.
	LEY 2063 DE 2020	Por la cual se decreta el presupuesto de rentas y recursos de capital y ley de apropiaciones para la vigencia fiscal del 1 de enero al 31 de diciembre de 2021; arts. 52, 105.
	LEY 2056 DE 2020	Por la cual se regula la organización y el funcionamiento del Sistema General de Regalías; Art. 35.
	LEY 2055 DE 2020	Por medio de la cual se aprueba la "convención interamericana sobre la protección de los derechos humanos de las personas mayores", adoptada en Washington, el 15 de junio de 2015.
	LEY 2052 DE 2020	Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y-o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones.
	LEY 2050 DE 2020	Por medio de la cual se modifica y adiciona la Ley 1503 de 2011 y se dictan otras disposiciones en seguridad vial y tránsito; Art. 4o.
	LEY 2047 DE 2020	Por la cual se prohíbe en Colombia la experimentación, importación, fabricación y comercialización de productos cosméticos, sus ingredientes o combinaciones de ellos que sean objeto de pruebas con animales y se dictan otras disposiciones; Art. 7o.
	LEY 2043 DE 2020	Por medio de la cual se reconocen las prácticas, laborales como experiencia profesional y-o relacionada y se dictan otras disposiciones; Art. 1o.

	LEY 2040 DE 2020	Por medio de la cual se adoptan medidas para impulsar el trabajo para adultos mayores y se dictan otras disposiciones; Art. 8o.
	LEY 2016 DE 2020	Por la cual se adopta el Código de Integridad del Servicio Público Colombiano y se dictan otras disposiciones; Art. 3 Par.
2021	LEY 2153 DE 2021	Por la cual se crea un sistema de información, registro y monitoreo que permita controlar, prevenir y evitar el tráfico ilegal de fauna y flora silvestre en el territorio nacional y se dictan otras disposiciones; Art. 3 Inc. 2
	LEY 2132 DE 2021	Por medio del cual se establece el Día Nacional de la Niñez y Adolescencia Indígena colombiana y se dictan otras disposiciones; Art. 5
	LEY 2127 DE 2021	Por medio de la cual se erigen los municipios de Pisba, Paya y Labranza grande - departamento de Boyacá, como "Triángulo de la Libertad" en reconocimiento del Bicentenario de Independencia y se dictan otras disposiciones; Art. 5
	LEY 2126 DE 2021	Por la cual se regula la creación, conformación y funcionamiento de las Comisarías de Familia, se establece el órgano rector y se dictan otras disposiciones; Art. 30 Par. 2
	LEY 2108 DE 2021	Ley de internet como servicio público esencial y universal" o por medio de la cual se modifica la ley 1341 de 2009 y se dictan otras disposiciones
	LEY 2101 DE 2021	Por medio de la cual se reduce la jornada laboral semanal de manera gradual, sin disminuir el salario de los trabajadores y se dictan otras disposiciones.
	LEY 2097 DE 2021	Por medio de la cual se crea el registro de deudores alimentarios morosos (redan) y se dictan otras disposiciones.
	LEY 2089 DE 2021	Por medio de la cual se prohíbe el uso del castigo físico, los tratos crueles, humillantes o degradantes y cualquier tipo de violencia como método de corrección contra niñas, niños y adolescentes y se dictan otras disposiciones; Art. 5.
	LEY 2085 DE 2021	Por medio de la cual se adopta la figura de la Depuración Normativa, se decide la pérdida de vigencia y se derogan expresamente normas de rango legal; Art. 7 Inc. 3.
	LEY 2080 DE 2021	Por medio de la cual se reforma el código de procedimiento administrativo y de lo contencioso administrativo -ley 1437 de 2011- y se dictan otras disposiciones en materia de descongestión en los procesos que se tramitan ante la jurisdicción; arts. 1, 8, 9, 10, 12 a 15.

Fuente: (MinTIC, 2021)

3. OBJETIVO.

Brindar a la institución un marco aplicado a la Infraestructura tecnológica, con un enfoque sistemático que proporcione las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información, a través de métodos que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y expedición de políticas así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo.

3.1 OBJETIVOS ESPECÍFICOS.

En beneficio del apoyo y cumplimiento de los propósitos de la política estratégica de seguridad de la información en la UNIAJC, se declaran los siguientes objetivos específicos:

- Brindar lineamientos y principios que propendan por la unificación de criterios para la administración de los riesgos de seguridad de la información.
- Fortalecer el sistema de gestión de riesgos de la Institución incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo de la Institución.
- Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas.
- Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información, y su mitigación.
- Reducir toda posibilidad de que una brecha o evento produzca determinado impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.
- Lograr y mantener a través de la implementación de medidas de control el nivel de probabilidad e impacto residual de los riesgos al nivel aceptable por parte de la Alta Gerencia.

4. ALCANCE.

La gestión de riesgos de seguridad de la información y su tratamiento, podrá será aplicada sobre cualquier proceso de la UNIAJC, a cualquier sistema de información o aspecto particular de control de la Institución, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

5. TÉRMINOS Y DEFINICIONES.

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información, en beneficio de unificar criterios dentro de la Agencia.

- Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la institución 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.
- 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.
- 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.
- Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evalúa.
- Control: Medida que modifica el riesgo.
- Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una institución 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.

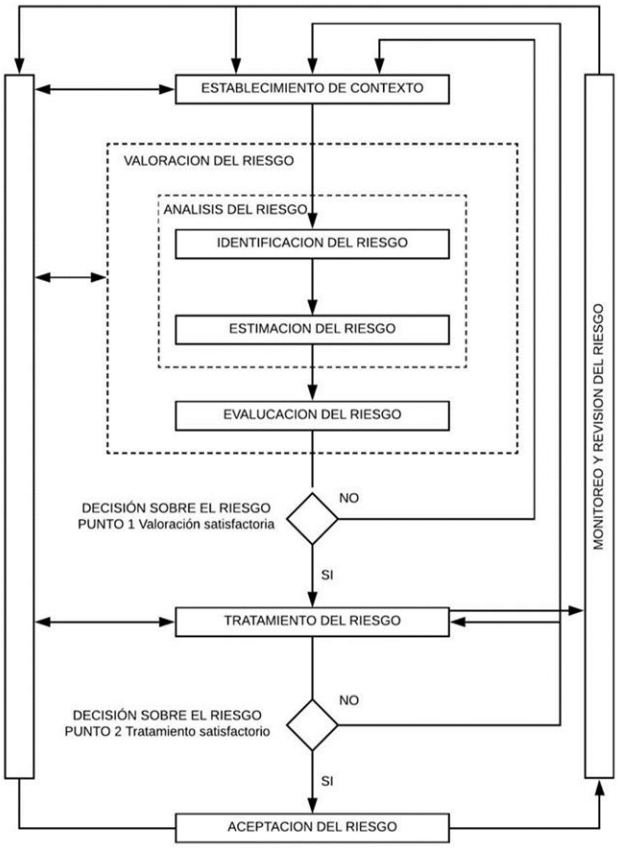
- Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar 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 institución.
- 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.
- 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 institución con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

- Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
- Riesgo Inherente: Es el nivel de riesgo 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: Efecto de la incertidumbre sobre los objetivos.
- Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupo de activos causando así daño a la organización.
- 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.
- Seguimiento: Mesa de trabajo semestral, en la 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.
- 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: 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.

6. VISIÓN GENERAL DEL PROCESO DE GESTIÓN DE RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN.

La seguridad de la información, es un ciclo repetitivo de actividades que se conectan unas con otras, cada actividad debe resolverse para no dejar vulnerabilidades en el proceso, la imagen siguiente representa una visión general del proceso.

Ilustración 1 Diagrama de flujo del riesgo



Adaptado para la UNIAJC de la Guía de Riesgos DAFP, 2013.

7. Política de Seguridad de la Información

Propósito: Proteger la información estratégica de la Institución y formar sus niveles de acceso y confidencialidad.

Exposición de la política

- Los dueños de la información nominados por autoridad competente deben ser funcionarios que estén completamente familiarizados con el segmento de información que les corresponde, así como con todos los procesos que interactúan con esta información.
- Los dueños de la información serán los responsables de verificar que existan procedimientos y procesos de seguridad para asegurar el manejo y la integridad de la información que reside en medios magnéticos o en documentos.
- El uso de los recursos lógicos de la institución deberá ser destinados para uso exclusivo de la UNIAJC.
- Toda información que viaje en un ambiente público deberá ser previamente encriptada.
- Los permisos de acceso a todos los sistemas de información, sean estos aplicativos del ERP y/o tendrán un tiempo de expiración de tres meses como mínimo y máximo cuatro meses.
- Se debe aplicar estándares y buenas prácticas de seguridad sobre el manejo de un modelo seguro de datos.
- Toda alta o baja del archivo maestro de personal debe ser oportuna y adecuadamente informado para una correcta administración de las claves de acceso.
- La entrega y/o acceso a la información de la institución, así como el acceso a su infraestructura tecnológica por parte de terceros, se realizará en base a la suscripción de convenios de confidencialidad o a la existencia de cláusulas de confidencialidad en los contratos u órdenes de trabajo respectivos.
- Todos los funcionarios que manejan información sensible de la compañía deberán firmar un acuerdo de confidencialidad.
- Será responsabilidad de la Oficina de tecnologías de la información, mantener vigente y actualizado el licenciamiento de software para la institución, tal como antivirus, licencias de firewall, destinados a proteger las instalaciones y activos informáticos de la Institución, así como también procurar una operación sin sobre cargas en la red de datos.

7.1 Políticas de manejo de cuentas de correo y uso de la red

Propósito: Para el manejo del uso de red se ha establecido las siguientes políticas:

- La instalación de puntos de red LAN Y WAN se realizará con contratación externa y/o personal directo de la Institución Universitaria Antonio José Camacho.
- La Oficina de tecnologías de la información y Comunicaciones, tendrá la responsabilidad de llevar un control de inventario de los puntos de red instalados en

todos los edificios y oficinas de la Institución. Esto incluye la certificación, rotulación de los mismos de acuerdo al estándar previamente establecido, y el uso de un sistema informático de control de este inventario.

- Todas las unidades de la institución que tengan necesidad de instalar puntos de red deberán canalizar y sustentar sus requerimientos ante su correspondiente responsable de área. Encontrar justificada la necesidad, cada responsable deberá hacer llegar a DTIC para ser atendidos.

Para el manejo del correo electrónico y el internet la UNIAJC ha establecido las siguientes políticas:

- Para la utilización de los diferentes servicios de red a través de las cuentas creadas, se deben acatar las normas obligatorias, cuyo incumplimiento acarreará sanciones de acuerdo con el reglamento interno de trabajo, según sea el caso.
- La cuenta electrónica es personal e intransferible. El usuario es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre. La Institución Universitaria Antonio José Camacho no se hace responsable por lo que se haga o diga en nombre de una cuenta particular y por lo tanto, está prohibido el uso de cuentas por personas ajenas a su titular.
- La UNIAJC podrá suspender o cancelar cuentas por mal manejo, sin perjuicios de imponer las sanciones correspondientes, según la gravedad de la falla.

Se consideran como conductas de mal manejo de las cuentas personales: Usos inaceptables tales como:

- Exceder los servicios para la cual se creó la cuenta.
- Intentar apoderarse de claves de acceso de otros usuarios, acceder y/o modificar archivos de otro usuario y en especial los pertenecientes a la UNIAJC.
- Enviar mensajes para la difusión de mensajes o correos electrónicos sin identificar plenamente a su autor o enviar anónimos.
- Usar los servicios de red para propósitos no investigativos o usuarios para propósitos fraudulentos, comerciales o publicitarios o para propagación de mensajes destructivos u obscenos.
- Difundir cadena de mensajes.
- Perturbar el trabajo de los demás enviando mensajes que pueden interferir con su trabajo.
- Violar o intentar violar los sistemas de seguridad de la red y servidores académicos y administrativos a los cuales se tenga acceso de manera local o externamente.
- Violar los derechos de privacidad de terceras partes.
- Violación de los derechos de propiedad intelectual de terceras partes.
- Usar la red para propósitos recreativos.
- Violar las reglas y restricciones impuestas por el administrador de red y la política de seguridad de la información de cualquier equipo que tenga una conexión a la red.

- No hacer uso racional del ancho de banda, espacio en disco, memoria, disco duro y unidades de almacenamiento.
- No salirse de una cuenta ajena cuando por circunstancia accidental se conecte a una.

Se consideran como conductas de buen manejo de las cuentas personales: Usos aceptables:

- Uso para propósitos educativos y de investigación.
- Uso para propósitos de administración de la infraestructura educativa y para investigación.
- Uso para acceso a bibliotecas.
- Uso para desarrollar proyectos de instituciones educativas o de un sector privado de proyectos de investigación.

7.2 Custodia y tenencia de activos informáticos.

• Los activos informáticos corporativos y centralizados serán custodiados por DTIC En caso de que se requiere equipo especializado, estos serán custodiados por el área donde se encuentre la operación.

• Los activos informáticos de usuarios finales (Mouse, Teclado y Diademas, sonido), serán custodiados por el responsable de su operación.

• Los custodios deberán ser funcionarios nombrados por la institución, a quienes se asignan los activos informáticos y son responsables pecuniariamente de su buen uso e integridad. Los usuarios son quienes utilizan para su labor diaria o eventual el activo informático y pueden ser empleados regulares de la institución o no (empleados de outsourcing, contratistas externos, consultores, entre otros).

• Cuando el usuario es un empleado regular de la institución, es a su vez un custodio. Cuando el usuario no es un empleado regular, el equipo debe estar a cargo de un funcionario nombrado de la Institución.

• La asignación de equipos de cómputo se realiza por la DTIC a los funcionarios custodios, después de la solicitud del jefe de área, una vez asignado el recurso a un funcionario este no puede asignarse a ningún otro empleado.

7.3 Productos de Software.

Los productos de software deberán cumplir los siguientes lineamientos para su adquisición e implementación:

• El uso de software para la institución provendrá de las siguientes fuentes:

a) Adquisición a terceros
b) Desarrollos propios

• El software adquirido deberá ser siempre a través del licenciamiento legal del mismo. Este tipo de software deberá incluir información para la instalación, la cual deberá ser usada por el personal de soporte técnico. Además, debe exigirse al proveedor el

entrenamiento en el uso y aplicabilidad del software para el usuario final al cual está destinado el producto.

- El software desarrollado localmente se hará dentro del ámbito de competencia de la Dirección de Tecnologías de Información y Comunicaciones. Ningún proyecto de desarrollo local se podrá realizar en otra dependencia diferente de DTIC.
- El desarrollo de software aplicación deberá cumplir con los estándares técnicos definidos por DTIC.

8. 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 Agencia 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 Agencia, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Institución 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 Institución. Como criterios para la gestión de riesgos de seguridad de la información se establecen:

8.1 Criterios de evaluación del riesgo de seguridad de la información:

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

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

8.2 Criterios de impacto.

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la agencia, 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 (pérdida de la confidencialidad, integridad y disponibilidad).
- Operaciones deterioradas (afectación a partes internas o terceras partes) Pérdida del negocio y del valor financiero.
- Alteración de planes o fecha límite Daños en la reputación.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

8.2.1 Criterios de Aceptación.

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de la UNIAJC y de Las partes interesadas, por tanto, las escalas de aceptación de riesgos de seguridad de información son fijadas por la UNIAJC.

8.3 Valoración de los riesgos de seguridad de la información

Los riesgos se deberán identificar, describir cuantitativa o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la UNIAJC, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo identificación de los riesgos.
- Estimación del riesgo.
- Evaluación del riesgo.

8.3.1 Identificación del Riesgo.

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación.

Los activos de información se clasifican en dos tipos:

a) Primarios:
   a. 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 muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.
   b. Información: información vital para la ejecución de la misión 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.
   c. Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

b) De Soporte:
   a. Hardware: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
   b. 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.).
   c. Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos

de un sistema de información (conmutadores, cableado, puntos de acceso, etc.).

d. Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.).
e. Sitio: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.).
f. Estructura organizativa: responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos, se han de conocer las amenazas que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la UNIAJC. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios, Inspección física.
- Uso de las herramientas para el escaneo automatizado.

Para cada una de las amenazas analizaremos las vulnerabilidades (debilidades) que podrían ser explotadas.

Finalmente, se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

8.3.2 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.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias, se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación de la institución.

Tabla 1 Frecuencia de eventos.

PROBABILIDAD			
CONCEPTO	**VALOR**	**DESCRIPCIÓN**	**FRECUENCIA**
Raro	1	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
Improbable	2	Es muy poco factible que el evento se presente	Al menos de 1 vez en los últimos 5 años.
Posible	3	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
Casi Certeza	5	Se espera que ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Fuente: Elaboración propia.

Tabla 2 Zonas de impacto valor.

IMPACTO		
CONCEPTO	**VALOR**	**DESCRIPCIÓN**
Insignificante	1	La materialización del riesgo puede ser controlado por los participantes del proceso, y no afecta los objetivos del proceso.
Menor	6	La materialización del riesgo ocasiona pequeñas demoras en el cumplimiento de las actividades del proceso, y no afecta significativamente el cumplimiento de los Objetivos de la Agencia. Tiene un impacto bajo en los procesos de otras áreas de la Agencia.
Moderado	7	La materialización del riesgo demora el cumplimiento de los objetivos del proceso, y tiene un impacto moderado en los procesos de otras áreas de la UNIAJC. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste Se desarrolle en forma normal.
Mayor	11	La materialización del riesgo retrasa el cumplimiento de los objetivos de la UNIAJC y tiene un impacto significativo en la imagen pública de la Agencia y/o de La Nación. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras.
Catastrófico	13	La materialización del riesgo imposibilita el cumplimiento de los objetivos de la Agencia, tiene un impacto catastrófico en la imagen pública de la Agencia y/o de La Nación. Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras.

Fuente: Elaboración propia.

8.3.3 Determinación del riesgo inherente y residual.

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario con sin controles) y ver el grado de exposición al riesgo que tiene la institución UNIAJC. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

Tabla 3 Zonas de Impacto

PROBABILIDAD		IMPACTO				
		INSIGNIFICANTE (1)	MENOR (6)	MODERADO (7)	MAYOR (11)	CATASTRÓFICO (13)
E (RARO)	1	Pasillos (PA)				
D (IMPROBABLE)	2	Cafetería (CA)	Baños (BA)			
C (POSIBLE)	3		Aulas de clase (AC)	Oficinas (OF)	Centros de cómputo (CP)	Cuartos eléctricos e hidráulicos (CE)
B (PROBABLE)	4				Salas de cómputo y laboratorios (SL)	
A (CASI SEGURO)	5					

Fuente: Elaboración propia.

Tabla 4 Niveles de riesgo.

ZONA	NIVEL DE RIESGO
ZONA DE RIESGO BAJO	BA
	PA
	CA
ZONA DE RIESGO MODERADO	AC
	OF
ZONA DE RIESGO ALTA	CP
	SL
ZONA DE RIESGO EXTREMA	CE

Fuente: Elaboración propia.

Las zonas de riesgo se diferencian por colores de la siguiente manera:

Tabla 5 Zona de riesgo.

ZONA DE RIESGO
B: Zona de riesgo Baja (Color Verde)
M: Zona de riesgo Moderada (color Amarillo)
A: Zona de riesgo Alta (Color Rojo)
E: Zona de riesgo Extrema (Color Vino tinto)

Fuente: Elaboración propia.

8.3.4 Evaluación de los riesgos.

Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basadas en riesgos de seguridad de la información y en beneficio de reducir su impacto a la Institución.

8.4 Tratamiento de los riesgos de la seguridad de la información

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

Tabla 6 Riesgos costo beneficio.

COSTO - BENEFICIO	OPCIÓN DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios.	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 costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo.	Transferir o compartir el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el Servicio).
El costo y el tiempo del tratamiento son adecuados a los beneficios.	Reducir o Mitigar el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto.
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	Retener o aceptar el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa.

Fuente: Elaboración propia.

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

Nota: Será conveniente que para la selección de los controles se consideren posibles restricciones o limitantes que impidan su elección tales como: restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, uso, de personal o las restricciones para la integración de controles nuevos y existentes.

8.5 Monitoreo y seguimiento.

Periódicamente, se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Institución por lo tanto podrá cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte: (1) nuevos activos o modificaciones en el valor de los activos, (2) nuevas amenazas, (3) cambios o aparición de nuevas vulnerabilidades, (4) aumento de las consecuencias o impactos, (5) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

8.6 Cronograma valoración de riesgos.

La Institución definirá y mantendrá un cronograma de actividades para la realización de la valoración de los riesgos de seguridad de la información en los procesos de la organización, basado con su criticidad y su valor para el cumplimiento de la misión de la UNIAJC.

El cronograma se publicará como seguimiento periódicamente, en el siguiente formato institucional y detallando la ejecución de actividades de enero a diciembre.

Tabla 7 Tabla de seguimiento de actividades

CRONOGRAMA DE EJECUCIÓN															
		2023													
Proyectos	DESCRIPCION	01	02	03	04	05	06	07	08	09	10	11	12	Objetivo	Meta %
Gestión de cambio cobertura tecnológica	Ampliación de cobertura tecnológica de licenciamiento y herramientas académicas para el campus universitario de la UNIAJC.	12.5 %												1	30
Gestión de seguridad en riesgos	Gestión de roles, usuarios, sitios y tráfico	12.5 %												4	100
Actualización de herramientas tecnológicas	Actualización permanente de consolas de seguridad perimetral y adquisición de herramientas DLP.	12.5 %												2	40

Fuente: Elaboración propia.