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

INSTITUTO DE CULTURA Y TURISMO DE SAN GIL

VIGENCIA 2020-2023

1. OBJETIVO

Realizar un análisis y valoración de los riesgos de seguridad de la información en cuanto al impacto y la probabilidad de ocurrencia para el Instituto Municipal de Cultura y Turismo de San Gil.

2. ALCANCE

El Análisis de Riesgos de Seguridad y Privacidad de la Información provee los mecanismos necesarios para identificar, analizar, evaluar y tratar de manera adecuada los riesgos asociados a los activos de información del Instituto Municipal de Cultura y Turismo de San Gil.

3. ÁMBITO DE APLICACIÓN

La presente Guía aplica para el Sistema Integrado de Gestión del Instituto Municipal de Cultura y Turismo de San Gil.

4. GLOSARIO

- **Riesgo:** se puede definir como la posibilidad de sufrir un daño por la exposición a un peligro.

- **Análisis de riesgo:** es el proceso cuantitativo o cualitativo que permite evaluar los riesgos.

- **Amenaza:** Son aquellas acciones que pueden ocasionar consecuencias negativas en la operación normal de la entidad. Generalmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc.

- **Vulnerabilidades:** son ciertas condiciones congénitas a los activos o presentes en su entorno que facilitan que las amenazas se materialicen y causen que los activos puedan ser vulnerables. Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.

- **Activos:** Los activos a reconocer son aquellos relacionados con sistemas de información. Ejemplos típicos son los datos, el hardware, el software, servicios, edificios y recursos humanos.

- **Impactos:** Son las consecuencias que se presentan cuando ocurre una amenaza.

- **5. DESCRIPCIÓN DE LA ORGANIZACIÓN**

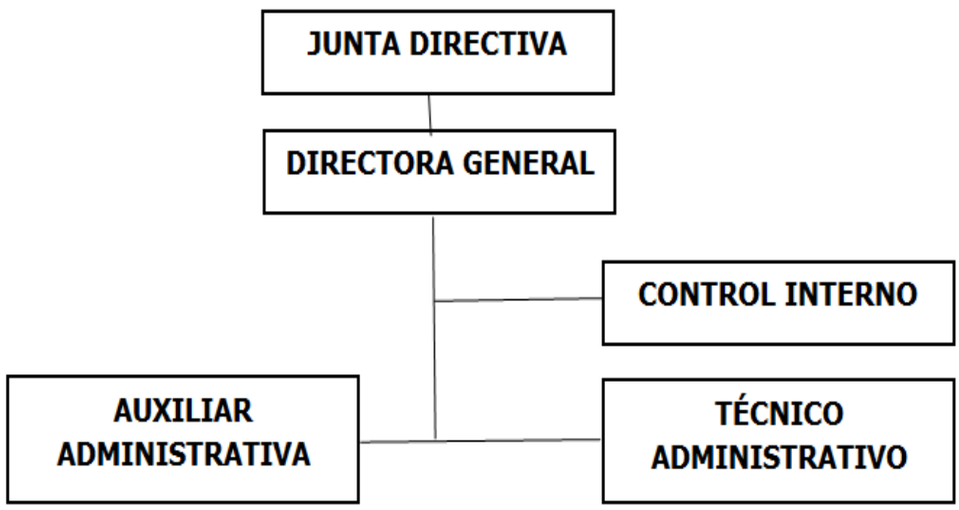
5.1. Misión

Impulsar, fomentar, y promover el desarrollo de las expresiones culturales del municipio de San Gil y áreas de influencia, asi como promover y articular iniciativas generadoras de atracción turística propias del municipio de San Gil, a través de políticas públicas generadoras de valor agregado, en coordinación con el sector social y privado.

5.2. Visión

Ser la institución municipal líder en prácticas de innovación para la promoción de expresiones culturales locales y atracción turística en San Gil, que posicionen al municipio como una marca de referencia internacional en cultura y turismo, a través de herramientas tecnológicas de vanguardia, en coordinación con el sector social y privado.

5.3. Organigrama del instituto



6. SITUACION ACTUAL

El análisis de la situación actual, tiene como base la información histórica de la Entidad, además de la recolección de la información, la observación de los procesos y las necesidades establecidas.

De acuerdo con lo anterior, se agrupa la información y se presenta una breve descripción de los elementos identificados, en relación con los siguientes elementos:

6.1. Equipos Tecnológicos

El Instituto de Cultura y Turismo de San Gil actualmente cuenta con los siguientes equipos tecnológicos:

GRUPO	DETALLE	Cantidad de Equipos Tecnológicos				
		Más de 5 Años	Entre 3 y 4 Años	Entre 1 y 2 Años	Menos de 1 Año	TOTAL
	PC's	6	0	0	0	6
	Impresoras	3	0	0	0	3
	Escáneres	1	0	0	0	1
	Portátiles	1	0	0	0	1
	TOTAL	**11**	**0**	**0**	**0**	**11**

6.2. Software

ITEM	SISTEMA DE INFORMACION	MODULOS QUE LE COMPONEN	AREA ENCARGADA
1	Sistema Financiero (GD / DELFIN)	Complementarios	Financiera y Contable

6.3. Recurso Humano

El Instituto de Cultura y Turismo de San Gil no cuenta con un departamento o área de sistemas, por lo tanto, no existe personal formado en TIC.

En caso de fallas técnicas en los equipos o software, el instituto contrata servicios externos.

7. Análisis de Riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- ✓ Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- ✓ Determinar a qué amenazas están expuestos aquellos activos.
- ✓ Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- ✓ Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

7.1. Clasificación de inventario de activos de información

Los activos se clasificarán de acuerdo a la siguiente tabla de clasificación de activos

TIPO DE ACTIVOS	DESCRIPCIÓN
Activos Esenciales / **Datos Información**	Datos importantes o vitales para la Administración de la Entidad: Aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios. Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). Datos Clasificados o Calificados: Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014). 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.
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: Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Dispositivos Móviles, Equipos de Respaldo, Impresoras, Escáneres, Módems,

Servicios	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).
Soportes Información	Dispositivos físicos electrónicos o no que permiten almacenar información de forma permanente o durante largos periodos de tiempo. Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.
Claves Criptográficas	Esenciales para garantizar el funcionamiento de los mecanismos criptográficos. Ejemplo: Claves de Cifrado, Claves de Firma, Protección de Comunicaciones (Claves de Cifrado de Canal), Cifrado de Soportes de Información, Certificados Digitales, Certificados de Claves, Claves de Autenticación.
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.
Instalaciones	Lugares donde albergan los sistemas de información y comunicaciones.

A continuación se detallan los campos que se establecen en el instrumento para realizar el levantamiento de activos de información:

- **ID:** Digitar el consecutivo con el cual se puede llevar el conteo de los activos de información.

- **Nombre del activo de información:** El activo de información se define como el elemento de información que el instituto recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes. Se debe indicar entonces el nombre específico del activo de información, es decir, la palabra o frase con la que se da a conocer el asunto de la información.

- **Descripción del activo de información:** se debe incluir una breve descripción del contenido del activo de información. Responder la pregunta: ¿de qué se trata la información? Cuando se trate de activos de información consistentes en información física o información digital, se deberán tener en cuenta las definiciones del banco de términos de la entidad.

- **Tipo de activo:** se debe seleccionar el tipo de activo de acuerdo a la tabla de clasificación de activos.

- **Idioma:** Indicar el idioma, lengua o dialecto en que se encuentra la información. Se debe tener en cuenta que el idioma oficial de Colombia es el castellano y las lenguas y dialectos de los grupos étnicos son también oficiales en sus territorios.

- **Medio de conservación y/o soporte:** es el medio en que se encuentra la información, es decir, donde reposa la información. Se debe escoger alguno de los siguientes medios de conservación y/o soporte: físico o electrónico.

- **Formato:** identifica la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta. Cuando se trate de activos de información consistentes en información física o información digital se debe seleccionar una o varias de las siguientes opciones, según corresponda. Si es otro tipo de activo de información (software, hardware o servicios) se debe seleccionar N/A: o Texto (incluye extensiones como .doc, .txt, .rtf, .pdf) o Hoja de cálculo (incluye extensiones como .xls, .xlt, .csv) o Presentación (incluye extensiones como .ppt, .pps) documento gráfico (incluye extensiones como .jpg, .gif, .png, .tif, .tiff, .ttf) Base de datos (incluye extensiones como .mdb, .sql) o Audio (incluye extensiones como .wav, .mid, .mp3, .ogg) o Video (incluye extensiones como .mpeg, .avi, .mov) o Animación (incluye extensiones como .swf) o Compresión (incluye extensiones como .zip, .rar) o Web (incluye extensiones como .html, .htmls) o Correo electrónico o Mensajería instantánea o Documento físico.
  Si existe algún formato no contemplado en la lista, se puede agregar.

- **Lugar donde se encuentra disponible (Contenedor):** corresponde al lugar donde se encuentra disponible la información para su consulta o solicitud. Se debe diligenciar siempre que se haya seleccionado en el campo "Forma de Consulta o Acceso (Información publicada o disponible)" las opciones "Disponible" o "Disponible/Publicado", indicando el lugar donde se encuentra disponible la información. Por ejemplo: Sistemas de Información (GD, DELFIN, JANIUM, entre

otros), Archivo Gestión Documental, Archivo dependencia, Servidores de Almacenamiento Oficiales (por ejemplo carpetas compartidas). Si la información únicamente ha sido publicada se debe indicar N/A. En las ubicaciones que se indiquen no se deben incluir nombres propios de los colaboradores del instituto.

- **Responsable de la producción de la Información:** corresponde al área, dependencia o unidad interna, o al nombre de la entidad externa que creó la información. Indicar el nombre de la dependencia que creo la información, en caso de corresponder a un grupo interno de trabajo deberá precisarse su nombre. En el evento que el productor de la información no sea una dependencia deberá indicarse el nombre de la instancia creadora de la información.

  No se deben incluir nombres propios de los colaboradores del instituto.

  La opción "entidad externa que creó la información", se debe usar cuando se efectúen o se hayan efectuado transferencias documentales al institutp por parte de otras entidades.

- **Responsable de la Información o Custodio:** corresponde al nombre del área, dependencia o unidad encargada de la custodia o control de la información para efectos de permitir su acceso. Para los activos consistentes en información física se debe escoger entre las siguientes opciones: Gestión Documental: cuando la información se ha transferido para su custodia y control de acceso a Gestión Documental.
  - Grupo Interno de Gestión de Talento Humano: cuando se trata de historias laborales.
  - Para el caso de los activos de información de Información digital, Software, Hardware y Servicios se deben atender las siguientes reglas:
    - Gestión de Tecnologías de la Información: Cuando el activo de Información Hardware, Software y Servicios.
    - En sistemas de información: El acceso lo otorga el que genera la información dentro del sistema.
    - Para el caso de activos de información diferentes a documentales es el propietario quien otorga el acceso.

- **Evaluación del activo:** Se evalúan los datos que contienen los activos de información de la siguiente manera.

Público: es el dato que ha sido calificado como tal por los mandatos de ley o por la Constitución política y todos aquellos que no tengan la condición de dato semiprivado, dato privado o dato sensible (incluidos los datos personales de niños, niñas o adolescentes), según la definición que de éstos hace la ley (Ley 1266 de 2008 y Decreto 1377 de 2013) y que se explica en los campos "Dato Privado", "Dato Privado", "Dato Semiprivado", "Dato Sensible" y "Dato personal de niños, niñas o adolescentes". Por ejemplo, son considerados datos públicos, entre otros, los siguientes:

- Relativos al Registro Civil.
- La profesión u oficio o la calidad de comerciante o de ser servidor público.

- Por su naturaleza, los datos públicos pueden estar contenidos en registros públicos, gacetas y boletines oficiales, documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva.

Si un dato personal no encuadra en las categorías de datos personales privados, semiprivados, sensibles o datos personales de niños, niñas o adolescentes, que se contemplan en los siguientes campos de la matriz, debe ser identificado en este campo como dato público.

Privado: Es el dato que por su naturaleza intima o reservada sólo es relevante para su titular y cuyo tratamiento no se puede hacer sin autorización de su titular. Los datos privados pueden ser objeto de tratamiento (cualquier operación o conjunto de operaciones sobre datos personales como la recolección, almacenamiento, uso, circulación o supresión), pero siempre se requiere contar con la autorización previa e informada de su titular, regulada por el artículo 9 de la Ley 1581 de 2012. Existen unos casos excepcionales en los que no se requiere de autorización, por ejemplo: casos de urgencia médica o sanitaria, cuando la información sea requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos. Son datos privados por ejemplo:

- Los libros y papeles del comerciante, entre otros, los libros de contabilidad.
- Las historias clínicas.
- La información extraída del domicilio de las personas (que solo pueden ser obtenidos por orden de autoridad judicial en el cumplimiento de sus funciones).
- La información cobijada bajo la reserva bancaria.
- La información tributaria respecto de las bases gravables y la determinación privada de los impuestos que figuren en las declaraciones tributarias.
- El número telefónico cuando se asocia al nombre de una persona, no contentivo en un Directorio telefónico.

Cuando se identifique la existencia de un dato personal privado en un activo de información, el activo debe ser considerado como **PÚBLICO CLASIFICADO** en lo que tiene ver con el dato personal privado exclusivamente (excepción parcial), con base en los "Objetivos legítimos de la excepción" contemplados en el artículo 18, literales a), b) o c) de la Ley 1712 de 2014, según se considere que sea la causal aplicable (derecho a la intimidad, a la vida, la salud, la seguridad, los secretos comerciales, industriales o profesionales, etc.) , y como "Fundamento constitucional o legal" incluir: artículo 3, literal h) de la Ley 1266 de 2008 (definición de dato privado), artículo 4, literal h), de la Ley 1581 de 2012 (principio de confidencialidad en el tratamiento de datos personales no públicos)

y además los específicos que puedan existir en el caso concreto, según se considere pertinente.

Semiprivado: Es el dato que no tiene naturaleza íntima o reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular, si no a cierto sector o grupo de personas o a la sociedad en general. Su tratamiento no se encuentra prohibido, pero sí requiere de autorización previa y expresa del titular del dato. Son datos personales semiprivados, por ejemplo:

- Los datos financieros, crediticios, comerciales y de servicios y la proveniente de terceros países, referidos al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen (artículo 3, literales g) y h) de la Ley 1266 de 2008).

Cuando se identifique la existencia de un dato personal semiprivado en un activo de información, el activo debe ser considerado como **PÚBLICO CLASIFICADO** en lo que tiene que ver con el dato personal semiprivado exclusivamente (excepción parcial), con base en los "Objetivos legítimos de la excepción" contemplados en el artículo 18, literales a) y/o b) y/o c) de la Ley 1712 de 2014, según se considere que sea la causal aplicable (derecho a la intimidad, vida, salud, seguridad, secreto comercial, profesional, etc.) , y como "Fundamento constitucional o legal" incluir: artículo 3, literal g) (definición de dato semiprivado) y artículo 4, literal g), de la Ley 1266 de 2008 (principio de confidencialidad en el tratamiento de datos personales) y además los específicos que puedan existir en el caso concreto, según se considere pertinente.

Sensible: Es aquel que afecta la intimidad de su titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, orientación política, las convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos. El tratamiento de datos sensibles está prohibido por el artículo 6 de la Ley 1581 de 2012 (salvo que su titular haya dado autorización), excepto en los siguientes eventos: cuando por ley no se requiera autorización; cuando su tratamiento sea necesario para salvaguardar el interés vital del titular y éste se encuentre física o jurídicamente incapacitado; cuando el tratamiento sea efectuado en el curso de actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa, sindical, siempre que se refieran a las personas que mantienen contactos regulares por razón de su finalidad con dichas organizaciones; cuando el tratamiento sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial y, cuando el tratamiento tenga una finalidad histórica, estadística o científica. Son datos personales sensibles por ejemplo:

- Origen racial o étnico.
- Orientación política.
- Convicciones religiosas o filosóficas.
- Orientación sexual.

7.2. Dimensiones de valoración

La Valoración del Activo de Información se realiza mediante la identificación del impacto para el Instituto de Cultura y Turismo de San Gil por la pérdida de las propiedades, principios o fundamentos de la Seguridad de la Información, teniendo en cuenta la siguiente tabla de criterios:

Criterio	Valor
Crítico	= 5
Alto	= 3 y < 5
Medio	= 1 y < 3
Bajo	= 0 y < 1

7.2.1. Confidencialidad

Impacto que tendría para el Instituto de Cultura y Turismo de San Gil, la pérdida de confidencialidad sobre el activo de información, es decir, que sea conocido por personas no autorizadas:

¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización.

- **5. Crítico:** Es la existencia de información más crítica (Calificada, Vital o Esencial) a nivel de pérdida de su confidencialidad que cualquier otra y que por ende debe tener una mayor protección. A la información (Calificada, Vital o Esencial) sólo pueden tener acceso las personas que expresamente han sido declaradas usuarios legítimos de esta información, y con los privilegios asignados. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente al instituto.
- **4. Alto:** Es la información que es utilizada por los funcionarios del instituto para realizar sus labores en los procesos y que no puede ser conocida por terceros sin autorización del propietario del activo. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente al instituto.
- **3. Medio:** Es la información que es utilizada por los funcionarios del instituto para realizar sus labores en los procesos y que puede ser conocida por terceros con la autorización del propietario del activo. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente al instituto.
- **2. Bajo:** Es la información que ha sido calificada como de conocimiento público. Esta información puede ser entregada o publicada con ciertas restricciones dadas por el propietario del activo a los funcionarios o a cualquier persona sin que implique daños a terceros ni a las actividades y procesos del instituto. El conocimiento o divulgación no autorizada de la información que gestiona este activo no tiene ningún impacto negativo para el instituto.
- **1. Mínimo:** Es la información que ha sido calificada como de conocimiento público. Esta información puede ser entregada o publicada sin restricciones a los funcionarios o a cualquier persona sin que implique daños a terceros ni a las actividades y procesos del instituto. El conocimiento o divulgación no autorizada de la información que gestiona este activo no tiene ningún impacto negativo en el instituto.
- **0. Nulo:** Es la información que ha sido calificada como de conocimiento público y su divulgación no implica impacto negativo para el instituto.

7.2.2. Integridad

Impacto que tendría la pérdida de integridad, es decir, si la exactitud y estado completo de la información y métodos de procesamiento fueran alterados.

¿Qué importancia tendría que los datos fueran modificados fuera de control?

Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización.

- **5. Crítico:** La pérdida de exactitud y estado completo del activo impacta negativamente la prestación de servicios de tecnología y de información en el instituto.
- **4. Alto:** La pérdida en la exactitud de algún dato o estado del activo impacta negativamente la prestación de servicios de tecnología y de información en el instituto.
- **3. Medio:** La pérdida posible en la exactitud de algún dato o estado completo del activo puede impactar negativamente al proceso que gestiona la información y/o a otros procesos en el instituto.
- **2. Bajo:** La pérdida posible de en la exactitud de algún dato o estado completo del activo puede tener algún impacto negativo en los procesos en el instituto.
- **1. Mínimo:** La pérdida de exactitud y estado completo activo no tiene ningún impacto negativo en los procesos en el instituto.
- **0. Nulo:** La pérdida de exactitud y estado no genera situación negativa alguna en los procesos en el instituto.

7.2.3. Disponibilidad

Impacto que tendría la pérdida de disponibilidad, es decir, si los usuarios autorizados no tuvieran acceso a los activos de información en el momento que lo requieran.

¿Qué importancia tendría que el activo no estuviera disponible?

Un activo tiene un gran valor desde el punto de vista de disponibilidad cuando si una amenaza afectara a su disponibilidad, las consecuencias serían graves.

- **5. Crítico:** La falta o no disponibilidad de la información que posea el activo de información o el mismo impacta negativamente la prestación de servicios de tecnología y de información en el instituto.
- **4. Alto:** La falta o no disponibilidad parcial de la información que posea el activo de información o el mismo impacta negativamente la prestación de servicios de tecnología y de información en el instituto.
- **3. Medio:** La falta o no disponibilidad de algún dato que posea el activo de información o el mismo impacta negativamente al proceso que gestiona la información y/o a otros procesos en el instituto.
- **2. Bajo:** La falta o no disponibilidad del activo de información en su componente puede tener algún impacto negativo en los procesos en el instituto.

- **1. Mínimo:** La falta o no disponibilidad del activo de información no tiene ningún impacto negativo en los procesos en el instituto.
- **0. Nulo:** La falta o no disponibilidad de algún dato que posea el activo de información no afecta los procesos en el instituto.

Una vez evaluado el activo en los tres componentes de confidencialidad, integridad y disponibilidad, se procederá a obtener el grado de importancia del activo para la entidad, así:

VALOR			CRITERIO
3	Mínimo uno de los componentes integridad, confidencialidad o disponibilidad tiene una calificación de **crítico** ó **alto**	Alto	De gran importancia a la entidad
2	Ninguno de los componentes integridad, confidencialidad o disponibilidad tiene una calificación de **crítico** ó **alto**, y alguno de los componentes tiene una calificación de **medio.**	Medio	De importancia a la entidad
1	Ninguno de los componentes integridad, confidencialidad o disponibilidad tienen una calificación de **crítico**, **alto** o **medio.**	Bajo	De menor importancia a la entidad

7.3. Identificación de amenazas

Se determinan las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

7.3.1. Tipos de amenazas a determinar

- **De origen industrial** Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

- **Ataques intencionados** Fallos deliberados causados por las personas.

7.3.2. Valoración de las amenazas

Una vez identificadas las amenazas se procede a realizar una valoración sobre los impactos que estas tienen sobre los activos. Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía. Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

- **Degradación:** cuán perjudicado resultaría el activo
- **Frecuencia:** cada cuánto se materializa la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera, esta degradación se medirá de la siguiente manera:

VALOR		CRITERIO
3	Alto	Daño grave
2	Medio	Daño importante
1	Bajo	Daño menor

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable. La frecuencia se medirá de la siguiente manera:

VALOR		CRITERIO
3	Alto	Bastante frecuente
2	Medio	Frecuente
1	Bajo	Poco frecuente

7.4. Determinación del impacto

El impacto se considera como la medida del daño sobre el activo procedente de la materialización de una amenaza. Una vez tengamos el valor de un activo para la organización y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. El impacto se calculará así:

VALOR			CRITERIO	
	Grado importancia del activo	Degradación		
3	Alto	Alto	Alto	Alto impacto
	Alto	Medio		
	Medio	Alto		
2	Alto	Bajo	Medio	Impacto moderado
	Medio	Medio		
	Bajo	Alto		
1	Medio	Bajo	Bajo	Bajo impacto
	Bajo	Bajo		
	Bajo	Medio		

7.5. Determinación del riesgo

El riesgo es la medida del daño posible sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, podemos calcular el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

VALOR			CRITERIO	
	Impacto	Frecuencia		
3	Alto	Alto	Alto	Alto riesgo
	Alto	Medio		
	Medio	Alto		
2	Alto	Bajo	Medio	Riesgo moderado
	Medio	Medio		
	Bajo	Alto		
1	Medio	Bajo	Bajo	Bajo riesgo
	Bajo	Bajo		
	Bajo	Medio		

7.6. Identificación de controles

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas

7.6.1. Evaluación de los controles

Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad de la siguiente manera:

¿El control está documentado, incluye el responsable y la frecuencia de aplicación?	¿El control se está aplicando?	¿El control es efectivo (sirve o cumple su función?

- Para la primera pregunta califique de 0 a 25.
- Para la segunda pregunta califique de 0 a 25.
- Para la tercera pregunta califique de 0 a 50

8. Desarrollo práctico – Valoración

En el formato Identificación y evaluación de controles, se deben identificar y documentar los controles asociados al riesgo y calificar de acuerdo con las preguntas descritas en el formato; finalmente, se debe hacer la sumatoria de los resultados de calificación por control.

IDENTIFICACIÓN Y EVALUACIÓN DE CONTROLES				
FECHA:				
RIESGO:				
Controles	Evaluación del control			Total
	¿El control está documentado, incluye el responsable y la frecuencia de aplicación?	¿El control se está aplicando?	¿El control es efectivo (sirve o cumple su función)?	