1. OBJETIVO

Establecer los criterios para la identificación, análisis, valoración, acciones y seguimientos a los riesgos potenciales que afecten la confiabilidad, disponibilidad e integridad de la información de la institución.

2. ALCANCE

Las políticas definidas el presente documento aplican a toda la comunidad Universitaria de la Institución Universitaria Antonio José Camacho.

3. DEFINICIONES Y TERMINOS

Entiéndase para el presente documento los siguientes términos:

IES: Instituto de Educación Superior

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

Información: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Ataque cibernético: intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

Brecha de seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en si misma, sea o no protegida por reserva legal.

4. REFERENCIAS NORMATIVAS

Norma NTC-ISO-IEC 27001

Guía No. 7, MINTIC, Guía de gestión de riesgos, Seguridad y privacidad de la información

5. DOCUMENTOS ASOCIADOS

RFT-O-2 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

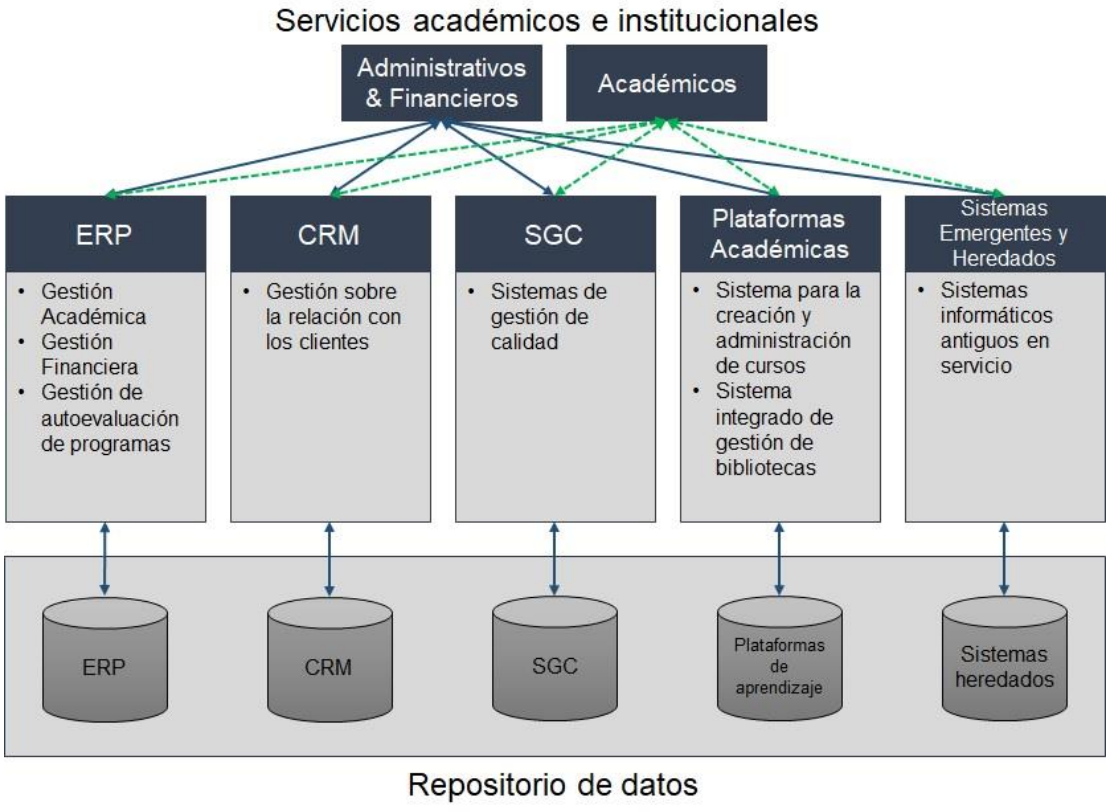
DIR-F-7 MAPA DE RIESGO GESTION DE INFRAESTRUCTURA

6. TRATAMIENTO E IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Permite conocer los riesgos que pueden afectar confidencialidad, integridad y disponibilidad de la información en los diferentes procesos de la organización, estas causas pueden ser internas o externas.

6.1 IDENTIFICACIÓN DEL ACTIVO

Se identifican varios conjuntos de activos, relacionados a continuación:



Fuente: Elaboración propia con base a los sistemas de información de los diferentes servicios de la institución

6.1.1 Servicios académicos e institucionales

Los servicios académicos e institucionales ofrecen el soporte imprescindible para garantizar el buen funcionamiento de la institución. Estos servicios se pueden describir como:

- Servicios administrativos y financieros: Servicios de apoyo a los procesos organizacionales, de dirección y control para el buen funcionamiento de la institución; procesos como contratación docente, cualificación de personal, contables y de tesorería, entre otros.
- Servicios académicos: Servicios de apoyo a las actividades académicas de estudiantes relacionadas con inscripciones, admisiones, matriculas, programas académicos, notas, entre otros.

6.1.2 Aplicaciones

Una institución cuenta con un número considerable de aplicaciones para diferentes propósitos académicos y administrativos, siendo estas de uso comercial, software libre, aplicaciones emergentes o programas descontinuados pero siguen siendo utilizados para la consulta. Dentro de este conjunto de aplicaciones se cuenta con las siguientes herramientas:

- Sistemas de gestión académica: Herramienta modulares para el manejo de los procesos académicos relacionados con inscripciones, registro de estudiantes, carga académica, registro de notas, entre otros. Estas plataformas son una de las más importantes del campus ya que en ella reside toda la información relacionada con la gestión estudiantil. El nivel de maduración de una plataforma académica crece con trayectoria de la institución y se aprecia su potencial para desarrollos que apunten a estos sistemas que beneficiaran la gestión universitaria.
- Sistema de administración de la relación con el cliente: Sistemas de apoyo para fortalecer las estrategias de negocio que ubica a los estudiantes como el centro de las actividades empresariales a través de seguimientos enfocados en el comportamiento del cliente, en su satisfacción en cada punto estratégico de servicio.
- Sistema de gestión de la calidad: Contribuye a la administración, automatización y mantenimiento de los procesos de calidad, brindando a la institución soportes para la gestión de documentación, visualización de procesos, gestión del talento humano y gestión y administración de equipos, entre otros.
- Sistema de autoevaluación de programas: Plataforma que permite realizar procesos de autoevaluación a programas de la institución bajo los lineamientos del CNA. Este sistema suelen estar compuestos por

módulos: modulo administrativo de configuración y gestión de procesos de autoevaluación, y módulos de acceso web para la recolección de información.

- Sistema integrado de gestión de bibliotecas: Sistemas que brindan a toda la comunidad académica y docente acceso a los recursos bibliográficos y bases de datos para que sean consultados física y electrónicamente; estas herramientas facilita toda la gestión bibliotecaria, desde el manejo de inventario de libros como su disponibilidad, reservas, préstamos, entre otros.
- Sistema evaluación docente: Sistema de apoyo a la institución y profesorado que busca mejorar las prácticas en el aula tomando como base la opinión del estudiante.
- Sistemas de para la gestión financiera: Sistemas para soportar procesos administrativos, contables y financieros la institución. Estas aplicaciones son integradas por módulos que a su vez son alimentados en línea por las diferentes áreas.
- Aplicativo de Contratación Docente: Dentro de los procesos administrativos, para facilitar la realización de contratos surgen desarrollos que apoyan estos procesos. Esta herramienta es utilizada en general por la oficina de Gestión Humana, encargada de la elaboración de estos contratos en base a la información suministrada por las diferentes decanaturas en los procesos de carga académica, cantidad de cursos, si es de tiempo completo, o temporal.
- Aplicativo de Generación de Facturas y cuentas de cobro: Son aplicativos emergentes de apoyo a la gestión para para la sistematización, centralización y gestión cuentas de facturas y cuentas de cobro por servicios suministrados por parte de la institución a terceros, o servicios que la institución presta a empresas.
- Aplicaciones para el aprendizaje: Para el apoyo a la enseñanza presencial como a distancia, se cuentan con plataformas como herramienta para la creación y administración de cursos. Los cursos virtuales son ofrecidos en modo B-learning, el cual cuenta con las herramientas necesarias para llevarlos a cabo a entera satisfacción permitiendo un seguimiento y control, eliminado fronteras dado que se puede trabajar en esta modalidad desde cualquier lugar si cuenta con una conexión a internet. Los cursos virtuales en modalidad presencial, están orientados a complementar procesos de aprendizaje del aula.

6.2 ACCESO A LA INFORMACIÓN

Todos los funcionarios públicos, contratistas, IES, que laboran para la Institución Universitaria Antonio José Camacho deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la Institución Universitaria Antonio José Camacho, Los jefes de cada proceso responsables de generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

Todas las prerrogativas para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Entidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Entidad.

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

6.3 ADMINISTRACION DE CAMBIOS

Todo cambio (creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración del mismo, al nivel de jefe inmediato o a quienes estos formalmente deleguen. El responsable de la administración de los accesos tendrá la facultad de aceptar o rechazar la solicitud.

Para la administración de cambios se efectuará el procedimiento correspondiente definido por la Institución Universitaria Antonio José Camacho, de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

6.4 SEGURIDAD DE LA INFORMACION

Los funcionarios públicos, contratistas, IES y pasantes de la Institución Universitaria Antonio José Camacho son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios públicos, contratistas, IES y pasantes no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas.

Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

6.5 SEGURIDAD PARA LOS SERVICIOS INFORMATICOS

El sistema de correo electrónico, grupos de charla y utilidades asociadas de la entidad debe ser usado únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los contratistas y pasantes.

La entidad se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito.

Para este efecto, el funcionario o contratista autorizará a la entidad para realizar las revisiones y/o auditorias respectivas directamente o a través de terceros.

Los funcionarios públicos, contratistas IES y pasantes que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.

En cualquier momento que un trabajador publique un mensaje en un grupo de discusión de Internet, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la entidad.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la oficina de Servicios informáticos, no utilizar el computador y desconectarlo de la red.

El intercambio electrónico de información se realizará con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacionales, y utilizando mecanismos criptográficos de clave pública que garanticen la integridad, confidencialidad, autenticidad y aceptación de la información. Cuando se considere necesario, los servicios de intercambio de información también incluirán garantías de "no repudio".

6.7 SEGURIDAD EN RECURSOS INFORMATICOS

Los recursos informáticos deben cumplir como mínimo con lo siguiente:

- Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los recursos informáticos. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.
- Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre el Administración de usuarios.
- Las puertas traseras: Las puertas traseras son entradas no convencionales a los sistemas operacionales, bases de datos y

aplicativos. Es de suma importancia aceptar la existencia de las mismas en la mayoría de los sistemas operacionales, bases de datos, aplicativos y efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan.

- El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.
- Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos, contratistas IES, y pasantes de la Institución Universitaria Antonio José Camacho son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.
- Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.
- Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.
- Antes de que un nuevo sistema se desarrolle o se adquiera, los jefes de oficina, en conjunto con el Director de la oficina de servicios informáticos, deberán definir las especificaciones y requerimientos de seguridad necesarios.
- Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

7. CALIFICACIÓN DE LA INFORMACIÓN[1]

La Información es un recurso vital producido por los sistemas de información de la institución, esta debe ser protegida apropiadamente contra accesos no autorizados, alteración, modificación, propagación, perdida o destrucción de las mismas, independientemente de los medios de almacenamiento donde esta reside.

[1] GUÍA PARA LA CALIFICACIÓN DE LA INFORMACIÓN DE ACUERDO CON SUS NIVELES DE SEGURIDAD [En línea]. Colombia: Presidencia de la Republica. Disponible en Internet: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/G-GD-02-calificacion-informacion.pdf

7.1 INSTAURAR CALIFICACIÓN DE LA INFORMACIÓN

La calificación asignada a la categoría de información determina los controles requeridos de seguridad y privacidad contemplando los siguientes aspectos:

7.1.1 INFORMACIÓN PÚBLICA

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (Artículo 5 Ley 1712 de 2014)
- **Información clasificada:** Es toda aquella que al ser divulgada puede llegar a causar daño a algunos derechos individuales de personas naturales o jurídicas por contener información relacionada con la intimidad y privacidad de éstas. (Artículo 18 Ley 1712 de 2014)
- **Información reservada:** Información reservada: Su divulgación indebida puede afectar bienes o intereses públicos. (Artículo 19 Ley 1712 de 2014). Es necesario establecer el plazo para la clasificación de la reserva, es decir el tiempo en que se considera debe limitarse el acceso a la información el cual según la Ley solo puede durar un máximo de 15 años desde la creación del documento.

7.1.2 LEY DE TRANSPARENCIA[2]

La información de las diferentes aplicaciones de la institución se encuentra almacenada en los sistemas de información y contenedores de datos. Por lo tanto, es importante incorporar a la clasificación teniendo en cuenta el artículo 6 de la ley 1712 de 2014 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:

a) Información. Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen;

b) Información pública. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal;

c) Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por

[2] http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882

lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley;

d) Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley;

e) Publicar o divulgar. Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión;

f) Sujetos obligados. Se refiere a cualquier persona natural o jurídica, pública o privada incluida en el artículo 5° de esta ley;

g) Gestión documental. Es el conjunto de actividades administrativas y técnicas tendientes a la planificación, procesamiento, manejo y organización de la documentación producida y recibida por los sujetos obligados, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación;

h) Documento de archivo. Es el registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones;

i) Archivo. Es el conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura;

j) 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;

k) Documento en construcción. No será considerada información pública aquella información preliminar y no definitiva, propia del proceso deliberatorio de un sujeto obligado en su calidad de tal.

8 EVALUACIÓN DE RIESGO

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo. Dentro de estos parámetros, como lo propone la Guía de gestión de riesgos, Seguridad y privacidad de la información de MINTIC "*Esta se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada "Matriz de Calificación, Evaluación y respuesta a los Riesgos", con la cual la guía presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo*".

Para la evaluación de riesgos se cuenta con una matriz de calificación tal cual como se muestra con la siguiente imagen:

MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A RIESGOS					
PROBABILIDAD	**IMPACTO**				
	INSIGNIFICANTE (1)	**MENOR (2)**	**MODERADO (3)**	**MAYOR (4)**	**CATASTRÓFICO (5)**
CASI SEGURO (5)	**A**	**A**	**E**	**E**	**E**
PROBABLE (4)	**M**	**A**	**A**	**E**	**E**
POSIBLE (3)	**B**	**M**	**A**	**E**	**E**
IMPROBABLE (2)	**B**	**B**	**M**	**A**	**E**
RARO (1)	**B**	**B**	**M**	**A**	**A**
MEDIDAS DE RESPUESTA U OPCIONES DE MANEJO					
B: Zona de riesgo Baja:			Asumir el Riesgo		
M: Zona de riesgo Moderada:			Asumir o Reducir el Riesgo		

A: Zona de riesgo **Alta**:	Reducir, Evitar, Compartir o Transferir el Riesgo
E: Zona de riesgo **Extrema**:	Reducir, Evitar, Compartir o Transferir el Riesgo

Teniendo en cuenta los procesos y las herramientas de los documentos relacionados, se presenta a continuación el análisis de uno de los riesgos de seguridad de la información como ejemplo:

Análisis del riesgo					
Proceso: Atención al usuario					
Objetivo: Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio y de acuerdo a las disposiciones legales vigentes.					
Riesgo	**Calificación**		**Impacto**	**Evaluación**	**Respuesta**
	Probabilidad	**Impacto**	**Tipo de impacto**	**Zona de Riesgo**	**Medidas de Respuesta**
Cambio en los datos de contactos de los usuarios					

8. ANÁLISIS DEL RIESGO

Para el análisis de riesgos se cuenta con las siguientes calificaciones tal cual como se muestra a continuación:

Tabla: Análisis de riesgo

ANÁLISIS DEL RIESGO			V - 3.0 - 2015 DIR-F-3
NOMBRE DEL PROCESO:	Gestión de Infraestructura	**RESPONSABLE DEL PROCESO:**	Planeación (Infraestructura Física), DTIC, Servicios Operacionales Laboratorios académicos, Bibliotecas, Coordinación académica (Medios audiovisuales).

OBJETIVO DEL PROCESO:	Desarrollar, mantener y mejorar la infraestructura física, tecnológica y los medios educativos institucionales, requeridos para la adecuada prestación del servicio en sus funciones académicas y administrativas.						
RIESGO ASOCIADO AL PROCESO	TIPO DE RIESGO	PROBABILIDAD DE OCURRENCIA	IMPACTO	CALIFICACIÓN DEL RIESGO		EVALUACIÓN	
				PROBABILIDAD DE OCURRENCIA	IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA
Falta de mantenimiento y daños eventuales sobre la infraestructura física, tecnológica y medios educativos.	R. Estratégico	Casi Seguro: Se espera que el evento ocurra en la mayoría de las circunstancias. Más de 1 vez al año.	CREDIBIL. o IMAGEN- Todos los funcionarios	5	2	Alta	Reducir, Evitar, Compartir o Transferir el Riesgo
Infraestructura física, tecnológica y bibliográfica insuficiente y/o inadecuada.	R. Estratégico	Probable: Es viable que el evento probablemente ocurra en la mayoría de las circunstancias. Al menos de 1 vez en el último año.	CONFID. INFORM.- Institucional	4	4	Extrema	Reducir, Evitar, Compartir o Transferir el Riesgo
Vulnerabilidad de los Sistemas de información	R. Operativo (Misional)	Probable: Es viable que el evento probablemente ocurra en la mayoría de las circunstancias. Al menos de 1 vez en el último año.	CONFID. INFORM.- Institucional	4	4	Extrema	Reducir, Evitar, Compartir o Transferir el Riesgo

Desastre natural	R. Estratégico	Posible: El evento podrá ocurrir en algún momento. Al menos de 1 vez en los últimos 2 años.	CREDIBIL. o IMAGEN- Usuarios de la ciudad	3	3	Alta	Reducir, Evitar, Compartir o Transferir el Riesgo
Peculado	R. Corrupción	Improbable: El evento puede ocurrir en algún momento. Al menos de 1 vez en los últimos 5 años.	CONFID. INFORM.- Grupo de trabajo	2	2	Baja	Asumir el Riesgo
Prevaricato	R. Corrupción	Raro: El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales). No se ha presentado en los últimos 5 años.	CONFID. INFORM.- Grupo de trabajo	1	2	Baja	Asumir el Riesgo
Vandalismo	R. Corrupción	Casi Seguro: Se espera que el evento ocurra en la mayoría de las circunstancias. Más de 1 vez al año.	OPERATIVO- Intermitencia en el servicio	5	4	Extrema	Reducir, Evitar, Compartir o Transferir el Riesgo

Tabla: Criterios de evaluación

CRITERIOS DE EVALUACION SEGÚN PROBABILIDAD DE OCURRENCIA	CALIFICACION DEL RIESGO	CRITERIOS DE EVALUACION SEGÚN IMPACTO				
		GENERAL	CONFIDENCIALIDAD DE LA INFORMACIÓN	CREDIBILIDAD O IMAGEN	LEGAL	OPERATIVO
Raro: El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	1	**Insignificante**: De presentarse el hecho, tendría consecuencias o efectos	Personal	Grupo de funcionarios	Multas	Ajustes a una actividad concreta

No se ha presentado en los últimos 5 años.		mínimos sobre la entidad.				
Improbable: El evento puede ocurrir en algún momento. Al menos de 1 vez en los últimos 5 años.	**2**	**Menor**: De presentarse el hecho, tendría bajo impacto o efecto sobre la entidad.	Grupo de trabajo	Todos los funcionarios	Demandas	Cambios en procedimientos
Posible: El evento podrá ocurrir en algún momento. Al menos de 1 vez en los últimos 2 años.	**3**	**Moderado**: De presentarse el hecho, tendría medianas consecuencias o efectos sobre la entidad.	Relativa al proceso	Usuarios de la ciudad	Investigación disciplinaria	Cambios en la interacción de los procesos
Probable: Es viable que el evento probablemente ocurra en la mayoría de las circunstancias. Al menos de 1 vez en el último año.	**4**	**Mayor**: De presentarse el hecho, tendría altas consecuencias o efectos sobre la entidad.	Institucional	Usuarios de la región	Investigación fiscal	Intermitencia en el servicio
Casi Seguro: Se espera que el evento ocurra en la mayoría de las circunstancias. Más de 1 vez al año.	**5**	**Catastrófico** : De presentarse el hecho, tendría desastrosas consecuencias o efectos sobre la entidad.	Estratégica	Usuarios del país	Intervención – Sanción	Paro total del proceso

9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La Institución evaluará el ejercicio de “tratamiento de riesgos y privacidad de la información”, por medio de seguimientos para revisar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando verificaciones al menos una vez al año o cuando sea necesario. De esta forma conlleva, dado el caso, a evidenciar todas aquellas situaciones que pueden estar influyendo en la aplicación de las acciones de tratamiento.