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

IMPLEMENTACIÓN ESTRATEGIA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

TABLA DE CONTENIDO

GLOSARIO

Seguridad informática: Se ocupa de la implementación técnica y de la operación para la protección de la información.

Seguridad de la información: Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.

Amenazas: Cualquier evento, persona, situación o fenómeno que pueda causar daño.

Vulnerabilidades: Falla o debilidad en un sistema que puede ser explotada por quien la conozca.

Riesgo: Probabilidad de ocurrencia de una amenaza.

Controles: Conjunto de mecanismos que regulan el funcionamiento de un sistema.

ISO: Organización Internacional de Normalización es una organización para la creación de estándares internacionales.

Activo: Bienes, recursos o derechos que tenga valor para una organización.

Activo de Información: Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.

Análisis de brechas: es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.

Análisis de Riesgo: Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.

Gestión del Riesgo Informáticos: Actividades empleadas para mitigar los riesgos informáticos.

Incidente de seguridad informática: daño que puede comprometer las operaciones de la entidad.

Evento: Acción que puedo haber causado daño, pero fue controlado**.**

Información: Conjunto de datos que tienen un significado.

Probabilidad: Posibilidad de que una amenaza se materialice

Impacto: Daño que provoca la materialización de una amenaza.

SGSI: Sistema de Gestión de seguridad de la Información

MSPI: Modelo de seguridad y privacidad de la información

PHVA: Planear, hacer, verificar, actuar.

INTRODUCCION

La norma ISO 27005:2011 es un estándar internacional diseñado para la gestión del riesgo en la seguridad de la información dentro de un sistema de gestión de seguridad de la información. Contiene diferentes procedimientos y directrices, que permiten establecer los riesgos que enfrenta una organización y poder mitigarlos de la mejor manera. Se realiza la identificación, el análisis, la evaluación de los riesgos, las políticas y controles que permiten reaccionar ante una posible materialización del riesgo mediante el plan de tratamiento de riesgos.

El no contar con una buena gestión de la seguridad de la información, para el Instituto Departamental de Cultura del Meta puede traer consecuencias graves, como pérdida fuga o robo de información, alteración de documentos, negación de servicios etc.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Detallar el plan de tratamiento de riesgos institucional, de tal forma que se definen y aplican los controles con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información en el Instituto Departamental de Cultura del Meta. De esta forma se busca que tanto los funcionarios, contratista y la comunidad tengan mayor confianza en el tratamiento de la información que se almacena y maneja.

1.2 OBJETIVOS ESPECÍFICOS

Identificar la ubicación y propietarios de los activos de información a través del inventario del mismo.
Categorizar y valorar los activos de información.
Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.

2. MARCO TEORICO

2.1 SEGURIDAD INFORMÁTICA

La seguridad Informática y la seguridad de la información son métodos y técnicas físicas y documentales empleadas para mantener siempre la confidencialidad, integridad y disponibilidad de la información.

Ilustración 1: Pilares de la seguridad informática.

2.2 NORMA ISO 27001

La norma ISO 27001 es un estándar internacional que describe cómo implementar el Sistema de gestión de seguridad de la información de una empresa. Investiga como salvaguardar la información mediante una serie de estándares, lineamientos y procesos que facilitan la identificación de los riesgos.

2.3 NORMA ISO 27005

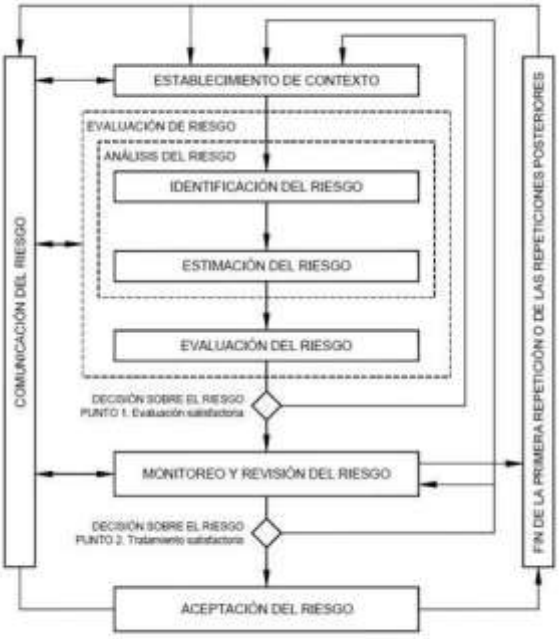
La norma ISO 27005 es un soporte a la norma (ISO 27001) la cual proporciona directrices para la gestión de riesgos de seguridad de la información, es aplicable a todos los tipos de organización y no proporciona ni recomienda una metodología específica.

"Las secciones contenidas en la norma ISO 27005 son[5]:

- Prefacio
- Introducción
- Referencias normativas
- Términos y definiciones
- Estructura
- Fondo
- Descripción general del proceso de ISRM
- Establecimiento de contexto

- Evaluación de riesgos de seguridad de la información (ISRA)
- Tratamiento de riesgos de seguridad de la información
- Seguridad de la información Aceptación del riesgo
- Seguridad de la información Comunicación de riesgos
- Seguridad de la información Monitoreo y revisión de riesgos
- Anexo A: Definición del alcance del proceso
- Anexo B: Valoración de activos y evaluación de impacto
- Anexo C: ejemplos de amenazas típicas
- Anexo D: Vulnerabilidades y métodos de evaluación de vulnerabilidad[1]
- Anexo E: enfoques ISRA"

En la siguiente figura se muestra el procedimiento de la guía 7 que propone el departamento administrativo de la función pública (DAFP) junto con el ministerio de la tecnología de información y comunicación (MinTIC) para la gestión de riesgos informáticos.



.

Ilustración 2: Tomada de NTC-ISO/IEC 27005 Gestión de Riesgos

The ISO 27000 Directory, Introduction To ISO 27005 (ISO27005), 2008 [en línea], [consultado el 15, Enero, 2018]. Disponible en Internet: http://www.27000.org/iso-27005.htm

Modelo de Seguridad Y Privacidad de la Información (MSPI) 2017 [en línea], [consultado el 15, Enero, 2018]. Disponible en Internet:http:// http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

2.4 ISO 27001. ORIGEN E HISTORIA

1901 – Nacen en Inglaterra las Normas "BS": La British Standards Institution publica normas con el prefijo "BS" con carácter internacional.

1995- Se escribe la norma BS 7799-1:1995 por el Departamento de Comercio e Industria del Reino Unido (DTI), Mejores prácticas para la gestión de la seguridad de la información.

1998 –Se hace una revisión de la anterior norma BS 7799-2:1999 que establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información certificable.

2000 - La Organización Internacional para la Estandarización (ISO) tomó la norma británica BS 7799-1 que dio lugar a la llamada ISO 17799, sin experimentar grandes cambios dando como resultado la norma ISO/IEC 17799:2000:

– ISO/IEC 27001:2005 e ISO/IEC17799:2005: Aparece el estándar ISO 27001 como norma internacional certificable y se revisa la ISO 17799 dando lugar a la ISO 27001:2005.

- BS 7799-3:2006 proporciona una guía para soportar los requisitos establecidos por ISO/IEC 27001:2005 con respecto a todos los aspectos que debe cubrir el ciclo de análisis y gestión del riesgo en la construcción de un sistema de gestión de la seguridad de la información (SGSI).

[5] *ISOTools Excellence ,SGSI Blog Especializado en Sistema de Gestión de Seguridad de la Información, ISO 27001:2013 Origen e Historia.[en línea].(Diciembre 2013). [Consultado 25 de agosto de 2017]. Disponible en internet: http://www.pmg-ssi.com/2013/12/iso27001-origen/*

[6]*Giovanni Zuccardi /Juan David Gutiérrez. ISO-27001:2005 Evolución del Estándar. [en línea] (Septiembre 2016). Disponible en internet: http://pegasus.javeriana.edu.co/~edigital/Docs/ISO27001/ISO27001v0.1.pdf*

2007 –Se renombra la norma ISO 17799: y pasa a ser la ISO 27002:2005

–Se publica la nueva versión de la norma ISO/IEC 27001:2007:

– nace la guía para la Implantación (bajo desarrollo) ISO 27003:2008.[2]

2008 -ISO 27004:2008 Métricas e Indicadores (bajo desarrollo).

–se crea la norma ISO 27005:2008 para la Gestión de Riesgos (BS 7799-3:2006)

– Se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M: 2009.

2011 – ISO 27005:2011: Se publica la nueva versión.

En el año 2013 se publicó la nueva versión de la ISO 27001 que trae cambios significativos en su estructura, evaluación y tratamiento de los riesgos.

Norma ISO/IEC	Título
ISO 27000	Gestión de la Seguridad de la Información: Fundamentos y vocabulario.
ISO 27001	Especificaciones para un SGSI.
ISO 27002	Código de Buenas Prácticas.
ISO 27003	Guía de Implantación de un SGSI.
ISO 27004	Sistema de Métricas e Indicadores.
ISO 27005	Guía de Análisis y Gestión de Riesgos.
ISO 27006	Especificaciones para Organismos Certificadores de SGSI.
ISO 27007	Guía para auditar un SGSI.

Tabla 1: Familia Norma ISO 27000

2.5 MODELO PHVA PARA EL SGSI

Un SGSI establece una serie de procesos y lineamientos que se deben seguir mediante la estandarización de la norma ISO 27001 para asegurar los activos de información como Bases de datos, oficios, actas etc. de una organización. El objetivo es mantener siempre la confidencialidad, integridad y disponibilidad de la información.

Ilustración 3: Ciclo PHVA de SGSI

2.6 METODOLOGÍA MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones. MAGERIT se basa en analizar el impacto que puede tener una organización al ser vulnerada, buscando identificar las amenazas que pueden llegar a afectar el funcionamiento de la compañía.

Esta metodología, guía paso a paso cómo llevar a cabo el análisis de riesgos. Está dividida en tres partes. La primera parte hace referencia al Método, donde se describe la estructura que debe tener el modelo de gestión de riesgos de acuerdo a la norma ISO 27001.

La segunda parte es el inventario activo de información que puede utilizar la empresa para enfocar el análisis de riesgo, las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles que deben tenerse en cuenta.

Por último, son las técnicas que Contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis de los riesgos.

2.7 OBJETIVOS DE LA METODOLOGÍA MAGERIT

Concientizar a los funcionarios y responsables de la información, los riesgos que enfrentan y como mitigarlos.
Establecer el tratamiento de los riesgos para evitar que los mismos se materialicen.
Proyectar a las organizaciones para la auditoria y certificación de la Norma ISO 27001.

ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO APAS DEL PROYECTO

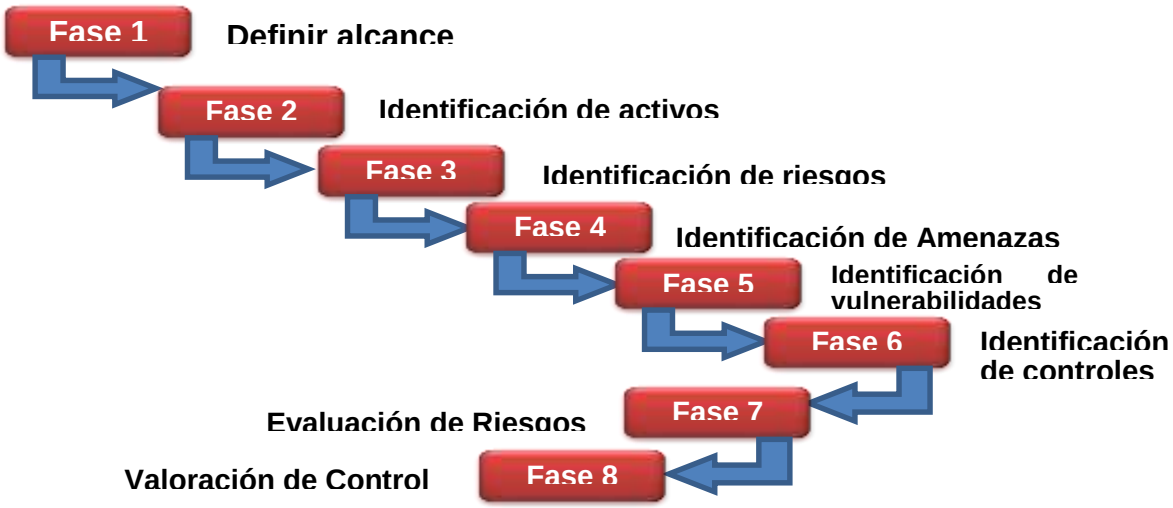


Ilustración 6: Guía para el Desarrollo.

3. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO APAS DEL PROYECTO

3.1 DEFINIR EL ALCANCE

En esta fase se establece los objetivos, justificación del procedimiento que se va a realizar, los funcionarios implicados y el contexto de seguridad informática con el que cuenta el Instituto Departamental de Cultura del Meta.

3.2 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACION

El principal activo de una organización es la información en sí, la cual puede estar en forma física como documentos impresos o escritos a mano, en medios electrónicos almacenados en Discos Duros Externos, Memorias USB o en forma digital, en los equipos de cómputo o en la Nube. Toda esta información requiere ser analizada para su protección. (Un activo es todo aquello que genera valor para una empresa u organización.)

3.3 CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN:

Nivel del Criterio

Confidencialidad / Se evalúa con los siguientes valores

Nivel	Descripción Criterio de Confidencialidad	Denominación
0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la entidad o no	Publico
1	Información que puede ser conocida y utilizada por todos los empleados del Instituto y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la entidad, el Sector Público Nacional o terceros.	Reservada – Uso Interno
2	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la entidad o a terceros.	Reservada - Confidencial
3	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del Instituto, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo o a terceros.	Reservada Secreta

Tabla 2: Evaluación de la confidencialidad

Integridad / / Se evalúa con los siguientes valores

Nivel	Descripción Criterio de Integridad
0	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del Instituto.
1	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para la entidad o terceros
2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la entidad o terceros.
3	Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al Instituto o a terceros.

Tabla 3: Evaluación de Integridad

3.3 IDENTIFICACIÓN DEL RIESGO

El objetivo de la identificación de riesgos es conocer lo incidentes o eventos que pueden causar pérdidas o alteración en el funcionamiento del Instituto Departamental de Cultura del Meta y pueden afectar la confidencialidad, integridad y disponibilidad de la información.

La identificación de los riegos se realiza con observación directa, ingeniería social y con el análisis a los equipos de seguridad perimetral. Por confidencialidad del Instituto Departamental de Cultura del Meta se presenta la identificación de riesgos general.

RIESGOS INFORMÁTICOS	CAUSAS	EFECTO
Perdida Robo o Fuga de Información	-Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de la misma. -Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de IT -No contar con acuerdos de confidencialidad con los	-Afectación parcial o total de la continuidad de las operaciones de los servicios del Incumplimiento normativo -Vulneración de los sistemas de seguridad operando

	empleados y terceros -Falta de autorización para la extracción de información generada por requerimientos. -Ingreso a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad -Habilitación de puertos USB en modo lectura y escritura para medios de almacenamiento -Ataques cibernéticos internos o externos -Empleados no capacitados en los temas de riesgos informáticos. -Desconocimiento del riesgo. -Prestar los equipos informáticos a personal no autorizado. -No cerrar sesión cuando se desplaza del puesto. -Acceso no autorizado a las dependencias. -Conectar dispositivos externos a los equipos. -Falta de implementación de la política escritorio limpio	actualmente -Mala imagen, multas, sanciones y pérdidas económicas -Generación de consultas, funcionalidades o reportes con información sensible de los clientes -Pérdida o fuga de información

Nivel	Descripción Criterio de Disponibilidad
0	Información cuya inaccesibilidad no afecta la operatoria de la entidad.
1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para el Instituto o terceros.
2	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la entidad o a terceros.
3	Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas a la entidad o a terceros.

Tabla 5: Identificación de Riesgos Informáticos.

3.4 IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza se identifica como un evento, persona, situación o fenómeno que pueda causar daño a los activos de la organización. Las amenazas pueden ser de origen Humano o Ambientales.

AMENAZA	TIPO
Polvo, Corrosión	Evento Naturales
Inundación	Evento Naturales
Incendios	Evento Naturales
Fenómenos Sísmicos	Evento Naturales
Fenómenos Térmicos	Evento Naturales y Daños físicos
Perdida en el suministro de energía	Daño Físico
Espionaje remoto	Acciones no autorizadas
Ingeniería Social	Acciones no autorizadas
Intrusión	Acciones no autorizadas
Accesos forzado al sistema	Acciones no autorizadas
Manipulación del Hardware	Acciones no autorizadas
Manipulación con Software	Acciones no autorizadas
Fallas del equipo	Fallas técnicas
Saturación del sistema de información	Fallas técnicas

Tabla 6: Identificación de Amenazas

3.5 IDENTIFICACIÓN DE LAS VULNERABILIDADES

Las vulnerabilidades son las Fallas o debilidades en un sistema, que puede ser explotada por quien la conozca. Cuando la amenaza encuentra la vulnerabilidad es cuando se crea el riesgo. Por eso es necesario conocer la lista de amenazas y el inventario de activos de información.

VULNERABILIDADES	DESCRIPCIÓN
Fácil acceso al Instituto Departamental de Cultura del Meta.	No existe un control para el acceso de las personas no autorizadas al Instituto.
Falta de dispositivos de seguridad biométrica para acceso.	El dispositivo de seguridad biométrica reduce el riesgo de robo de información o equipos electrónicos por fácil acceso.
Falta de organización y limpieza (escritorio Limpio).	Mantener el escritorio limpio, es importante para que los funcionarios no dejen expuestos: documentos, equipos electrónicos u objetos de valor, sobre los escritorios, que pueden ser robados fácilmente.
Falta de máquina trituradora de papel	La máquina trituradora de papel, evita que las personas arrojen documentos importantes con información personal a la basura, que puedan ser usados para crear perfiles de ataque.
Falta de Capacitación de los funcionarios en temas de seguridad Informática.	El eslabón más débil en términos de seguridad informática en una organización son los funcionarios.

Tabla 7: Identificación de Vulnerabilidades

3.6 IDENTIFICACIÓN DE CONTROLES EXISTENTES

La identificación de los controles existentes permite realizar la evaluación de riesgos. Los controles garantizan que al momento de la materialización de un riesgo se reduzcan o mitiguen los riesgos informáticos y la organización funcionen correctamente. Pero se debe tener en cuenta que nunca se va a estar 100% seguros.

Dada la importancia de los controles, con que cuenta el Instituto Departamental de Cultura del Meta no es adecuado exponerlos en el proyecto, por lo que se pueden crear perfiles de ataque.

3.7 EVALUACIÓN DE RIESGO

La evaluación de riesgo se realiza con enfrentamiento entre la probabilidad de ocurrencia y el impacto que genera el riesgo en los activos de información, dado por la matriz de calificación, evaluación y respuestas a los riesgos.

TABLA DE PROBABILIAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**	**FRECUENCIA**
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
3	posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	probable	El evento probablemente ocurra en la mayoría de las circunstancias	Al menos una vez en el último año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

Tabla 8: Probabilidad de riesgo

TABLA DE IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efecto mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

Tabla 9: Impacto del riesgo

PROBABILIDAD	IMPACTO				
	Insignificante(1)	Menor(2)	Moderado(3)	Mayor(4)	Catastrófico(5)
Raro(1)	B	B	M	A	A
improbable(2)	B	B	M	A	E
posible(3)	B	M	A	E	E
probable(4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B:Zona de Riesgo Baja: Asumir el riesgo

M:Zona de Riesgo Moderada: Asumir el riesgo, Reducir el riesgo

A:Zona de Riesgo Alta: Reducir ,Evitar, Compartir o Transferir

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

Tabla 10: Matriz de calificación, evaluación y respuestas a los riesgos.

ANÁLISIS DE RIESGOS					
RIESGO	CALIFICACIÓN		TIPO DE IMPACTO	EVALUACIÓN	MEDIDAS DE RESPUESTAS
	PROBABILIDAD	IMPACTO		ZONA DE RIESGO	
Perdida, Robo o fuga de información	3	5	Disponibilidad, integridad y confidencialidad de la información	Extrema	Reducir el riesgo, Evitar o Transferir

Tabla 11: Ejemplo de análisis de riesgo

PROBABILIDAD	IMPACTO				
	Insignificante(1)	Menor(2)	Moderado(3)	Mayor(4)	Catastrofico(5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B:Zona de Riesgo Baja:Asumir el riesgo

M:Zona de Riesgo Moderada:Asumir el riesgo,Reducir el riesgo

A:Zona de Riesgo Alta:Reducir ,Evitar,Compartir o Transferir

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

Tabla 12: Ejemplo de valoración del riesgo

3.8 VALORACION DE CONTROLES

La valoración de controles, evalúa los controles existentes en la organización y la efectividad para mitigar la exposición al riesgo.
Se emplea una tabla para la valoración de control donde se establecen 2 parámetros con 5 criterios, dependiendo del puntaje y si el control se ejecuta con la probabilidad, con el impacto o ambos, se genera un desplazamiento del valor del riesgo.

VALORACIÓN DE CONTROL		
PARAMETROS	**CRITERIOS**	**PUNTAJE**
HERRAMIENTAS PARA EJERCER EL CONTROL	Posee una herramienta para ejercer el control.	15
	Existen manuales, Instructivos o procedimientos para el manejo de la herramienta.	15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.	30
SEGUIMIENTO AL CONTROL	Están definidos los responsables de la ejecución del control y del seguimiento.	15
	La frecuencia de ejecución del control y seguimiento es adecuada.	25
TOTAL		100

Tabla 13: Valoración de los controles

RANGOS DE CALIFICACION DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO, DESPLAZA EN LA MATRIZ DE CALIFICACION,EVALUACION Y RESPUESTA A LOS RIESGOS	
	CUADRANTES A DISTRIBUIR EN LA PROBABILIDAD	CUADRANTES A DISTRIBUIR EN EL IMPACTO
ENTRE 0-50	0	0
ENTRE 51-75	1	1
ENTRE 76-100	2	2

Tabla 14: Evaluación de los controles

ANÁLISIS DE RIESGOS							
RIESGO	CALIFICACIÓN		CONTROL	TIPO DE CONTROL	PUNTAJE Herramienta para ejercer el control	PUNTAJE Seguimiento al Control	PUNTAJE FINAL
	PROB	IMPACTO					
Perdida, Robo o fuga de información	3	5	Reservado	PROBABILIDAD E IMPACTO	60	40	100

Tabla 15: Ejemplo de análisis de riesgos con evaluación de controles

De acuerdo con el análisis anterior, el riesgo reduce dos puntos en Probabilidad, y dos en impacto, de acuerdo a las calificaciones de los controles, como se muestra en la siguiente ilustración:

PROBABILIDAD	IMPACTO				
	Insignificante(1)	Menor(2)	Moderado(3)	Mayor(4)	Catastrofico(5)
Raro(1)	B	B	M	A	A
improbable(2)	B	B	M	A	E
posible(3)	B	M	A	E	E
probable(4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B:Zona de Riesgo Baja:Asumir el riesgo

M:Zona de Riesgo Moderada:Asumir el riesgo,Reducir el riesgo

A:Zona de Riesgo Alta:Reducir ,Evitar,Compartir o Transferir

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

Tabla 16: Matriz probabilidad impacto

3.9 SOCIALIZACIÓN DE LA IMPORTANCIA DE LA GESTIÓN DE RIESGOS INFORMÁTICOS Y SEGURIDAD DE LA INFORMACIÓN

Debido a que los funcionarios de una entidad, son el eslabón más débil de la seguridad informática, se realiza una presentación sobre seguridad informática y seguridad de la información que permite a los funcionarios, conocer la importancia de la gestión de riesgos informáticos y conocer los riesgos que enfrentan para poder mitigarlos.

4. RESULTADOS Y DISCUSIÓN

La gestión de Riesgos informáticos permitió conocer las vulnerabilidades, las amenazas y los riesgos informáticos del Instituto Departamental de Cultura del Meta. Este Análisis permite a la entidad fortalecer la estructura de la seguridad de la información y prepararse para cualquier evento o incidente.

4.1 RECOMENDACIONES

Concientizar constantemente al Director y Funcionarios del Instituto Departamental de Cultura del Meta, sobre la importancia de cumplir con la política de seguridad de la información.
Aplicar correctivos o Sanciones a los funcionarios que no cumplan con la política de seguridad de la información establecida.
Mantener actualizada la política de seguridad de la información
Realizar Auditorías periódicas de Seguridad Informática.
Capacitar frecuentemente a los funcionarios de la entidad en temas de seguridad informática.
Establecer un responsable de la seguridad informática en el Instituto

5. ANEXOS

Ver documento anexo

6. ELABORACIÓN, REVISIÓN Y APROBACIÓN

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE	SEPAD S.A.S Contratista	Natalia Alexandra Leyva Quijano	Comité Institucional de Gestión y Desempeño
CARGO		Subdirectora General	
FIRMA			

7. CONTROL DE CAMBIOS

Revisión	Versión No.	Fecha	Cambio
N/A	01	02-05-2019	Creación del Documento