PLAN

DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VERSIÓN 1.0

ELABORÓ	REVISÓ	APROBÓ
ANDRÉS LEONARDO JIMÉNEZ CARRILLO YASMIN LANCHEROS ZAMBRANO	JENNIFER ADRIANA MEJÍA AMAYA	YENNY RUBIELA MANCERA CAMELO
PROFESIONALES UNIVERSITARIOS	ASESOR PLANEACIÒN GESTIÓN DE CALIDAD Y COMUNICACIONES	CONTRALORA DEPARTAMENTAL DEL META
FECHA	FECHA	FECHA
06/03/2019	06/03/2019	06/03/2019

DE USO EXCLUSIVO PARA LA CONTRALORÌA DEPARTAMENTAL DEL META

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La información que se crea y gestiona durante todo su ciclo de vida en la Contraloría Departamental del Meta, es de suma importancia para su funcionamiento y de los objetivos estratégicos, es allí donde cobra importancia la seguridad y privacidad de la información como atributos indispensables para evitar cualquier posibilidad de alteración, mal uso, pérdida, entre otros eventos, que puedan significar una alteración para el normal desarrollo de la gestión misional y administrativa de la entidad.

Dentro del Modelo de Seguridad y Privacidad de la información –MSPI- del Ministerio de las TIC, se incorpora la Gestión de riesgos. Es por esto que la Contraloría Departamental del Meta adopta la metodología en mención.

La entidad acoge la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, maximizar rendimientos y cuidar la seguridad de la información.

2. OBJETIVO

2.1. OBJETIVO GENERAL

Crear y gestionar un plan para mitigar los riesgos asociados a los procesos existentes en la Contraloría Departamental del Meta, con el fin de proteger los activos de información, el control de acceso y la gestión de los usuarios contra la materialización de amenazas que vulneren la seguridad de la información.

2.2. OBJETIVOS ESPECÍFICOS

1. Desarrollar un plan de trabajo para la implementación del plan de tratamiento de riesgos de seguridad y privacidad de la información.

2. Actualizar los principales activos a proteger en la entidad.

3. Realizar la evaluación de los riesgos informáticos existentes en la Contraloría Departamental del Meta.

4. Establecer controles que permitan mitigar las causas que originan los riesgos.

3. ALCANCE

El plan de tratamiento de riesgos tiene alcance para los procesos de la Contraloría Departamental del Meta, en concordancia con el alcance Manual de Seguridad de la Información.

3.1. TÉRMINOS Y DEFINICIONES

Confidencialidad. Un atentando contra la confidencialidad es cuando una persona que no es el destinatario, tiene acceso a los datos.

Integridad. Mientras la información se transmite a través del protocolo de comunicación, un atacante podría interceptar el mensaje y realizar cambios en determinados bits del texto cifrado con la intención de alterar los datos del criptograma.

Disponibilidad. En este caso, un atacante podría utilizar los recursos de la organización, como el ancho de banda de la conexión DSL para inundar de mensaje el sistema víctima y forzar la caída del mismo, negando así los recursos y servicios a los usuarios legítimos del sistema.

Gestión del Riesgo. La Gestión del Riesgo es un proceso cuya función principal es mantener un ambiente seguro. Consiste en identificar los factores que podrían dañar o revelar datos y crear medidas que implementen una solución para mitigar o reducir el riesgo. Todo el proceso de gestión del riesgo es utilizado para desarrollar e implementar estrategias de seguridad de la información, las cuales buscan reducir el riesgo y soportar la misión de la organización.

Riesgos Informáticos. El riesgo informático se define como "la probabilidad de que una amenaza en particular expone a una vulnerabilidad que podría afectar a la organización", o como "la posibilidad de que algo pueda dañar, destruir o revelar datos u otros recursos". El riesgo va inherente a una serie de términos que se deben comprender para poder tener una mejor concepción de su significado en el contexto de la seguridad de la información.

Activo: Representa el objetivo directo o indirecto de un evento. El resultado siempre tiene una consecuencia directa el cual es aplicado al activo. Un activo es algo valioso para una organización y en el contexto de seguridad informática están constituidos por el software, el hardware, las aplicaciones, las bases de datos, las redes, copias de seguridad e incluso las personas.

Probabilidad: Posibilidad o frecuencia de que un evento ocurra sobre un activo.

Vulnerabilidad: Es una falla o debilidad en los procedimientos, diseño, implementación o controles internos en un sistema de seguridad. Es cualquier ocurrencia potencial que pueda causar un resultado indeseado para una organización o para un activo en específico

Amenaza: Es el potencial que un intruso o evento explote una vulnerabilidad específica.

4. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la gestión del riesgo depende de diversos factores, aun así, la participación de la alta dirección en este caso del (la) contralor(a), Asesores, Contralores Auxiliares y jefes de proceso permite que el plan se desarrolle con mayor fluidez y efectividad, es por ello, que en la identificación de los roles no solo se observa el equipo técnico que hará las labores de análisis y tratamiento del riesgo si no que se incluye al Comité Institucional de Gestión y Desempeño.

El Comité Institucional de Gestión y Desempeño muestra su compromiso y apoyo en el diseño, implementación y mantenimiento del Plan de Tratamiento de Riesgos a través de la asignación de recursos, la definición de la política de administración del riesgo, los lineamientos de seguridad y el establecimiento del Gobierno de seguridad, cuya conformación y responsabilidades se describen a continuación:

Rol	Objetivo
Comité Institucional de Gestión y Desempeño	• Aprobar los lineamientos estratégicos en cuanto a seguridad de la información, garantiza los recursos y la toma de decisiones orientadas al cumplimiento de la estrategia por ellos definida. • Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la entidad. • Supervisa la aplicación de los requisitos definidos por gobierno digital en lo relacionado con la seguridad de la información.
Líder de seguridad de la información	• Tiene la responsabilidad de guiar y realizar el seguimiento de la implementación de los planes de seguridad definidos.
Líderes de procesos	• Tienen la responsabilidad de dar la cobertura de los lineamientos de seguridad a cada uno de sus procesos estratégicos, misionales o de apoyo.

5. ANÁLISIS DE RIESGOS DE LA CONTRALORÍA DEPARTAMENTAL DEL META

5.1. INVENTARIO DE ACTIVOS

La Contraloría Departamental del Meta está comprometida con preservar la confidencialidad, integridad y disponibilidad de la información que en ella se gestiona, incluyendo medidas que la pueden soportar y fortalecer, se realiza la clasificación de los activos de información basados en la metodología de riesgos MAGERIT Libro II catálogo de elementos que los clasifica de la siguiente manera:

- **Servicios**: Satisface una necesidad de los usuarios, los servicios prestados por el sistema:
- **Datos/Información:** activo abstracto que es almacenado de manera física y virtual pueden estar agrupados en ficheros y base de datos.
- **Aplicaciones Informáticas:** activo software que sirve para procesar, gestionar, transportar y transformar los datos.
- **Equipos Informáticos:** hardware que soporta las aplicaciones y los datos informáticos.
- **Soportes de Información:** son los dispositivos físicos con los cuales se pueden almacenar información.
- **Redes de Comunicaciones:** son los medios de transporte de la información.
- **Equipamiento auxiliar:** otro tipo de activo que sirven de soporte para los equipos informáticos sin estar directamente relacionado con los datos.
- **Instalaciones/Personal:** los lugares donde está la información y el personal que la administra.

En razón a que se tiene acceso total al proceso de gestión documental de la entidad se hace una identificación de los activos y se clasifica de acuerdo al tipo.

5.1.1. Servicios

Son todos aquellos activos encargados de satisfacer las necesidades de los funcionarios de la dependencia entre estos tenemos.

- World wide web, el cual se encarga de ofrecerles el servicio de internet para los funcionarios.
- Correo electrónico, para la gestión de cuentas de correos electrónicos enviar y recibir correos.
- Soporte interno (a usuarios de la propia organización), en donde se ofrece la asistencia informática a los funcionarios de la entidad.
- Página web, servicio de mantenimiento de la página web.
- Mensajería interna (a usuarios de la propia organización). Servicio de mensajería Interna.

5.1.2. Datos/Información

En pocas palabras son el eje central de la oficina de gestión de recursos informáticos ya que el diseño del sistema de gestión de seguridad gira en torno a esta, es un tipo de activo abstracto a diferencia de los demás activos.

- Ficheros, contratos suscritos con los proveedores
- Copias de respaldo, archivo de copias de seguridad de la información

5.1.3. Aplicaciones Informáticas

Hace referencia al software encargado de gestionar el activo datos mediante operaciones informáticas.

- Sysman, Sistema de Información administrativo
- GLPI Sistema de Información para solicitar asistencia
- Nod 32, antivirus.

5.1.4. Equipos informáticos

Se trata de los dispositivos hardware encargados de soportar las aplicaciones y los datos.

- Grandes equipos, servidor de bases de datos, servidores de dominio e internet
- Informática personal, computadores de la entidad
- Conmutadores de la entidad
- Central telefónica, planta telefónica
- Impresoras, medios de impresión

5.1.5. Soportes de Información

- Discos, discos duro extraíbles de respaldo de la información

5.1.6. Redes de Comunicaciones

- Red local, Lan de la entidad

5.1.7. Equipamiento Auxiliar

- Mobiliario, muebles, estantes de la entidad.

5.1.8. Instalación y Personas

- Rack, Rack de Comunicaciones
- Administradores de sistemas, Profesional Universitario de Sistemas, Proveedores

5.2. VALORACIÓN CUALITATIVA DE LOS ACTIVOS

Para realizar la valoración de los activos se tuvo en cuenta que no a todos se les debe generar el mismo peso, toda vez que cada uno cumple una función diferente y el riesgo de amenaza varía en razón de la misma, por lo tanto el impacto ante la materialización de una amenaza es diferente, se realiza la valoración cuantitativa en razón de las cinco dimensiones confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad de acuerdo a la siguiente tabla:

Criterios de valoración

Valor		Criterio
10	Extremo	Daño Extremadamente Grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Efectos prácticos

Dimensiones Activos

De acuerdo al activo se asignan unas dimensiones que sirven para darle un valor conforme a las consecuencias frente a la materialización de amenazas.

Dimensión	Código
Disponibilidad	D
Integridad	I
Confidencialidad	C
Autenticidad	A
Trazabilidad	T

Valoración Cualitativa Servicios

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión				
				C	I	A	D	T
[www]	World wide web	[S_Internet]	Servicio de internet para los funcionarios	6	6	6		
[email]	Correo electrónico	[S_correo]	Gestión de cuentas de correos electrónicos	6	6	7		
[int]	interno (a usuarios de la propia organización)	[S_U_soporte]	Asistencia informática a los funcionarios de la entidad.	6	6	6		
[anon]	anónimo (sin requerir identificación del usuario)	[S_U_página_web]	Servicio de mantenimiento de la página web.			6	7	
[int]	interno (a usuarios de la propia organización)	[S_U_spark]	Servicio de mensajería Interna			5	7	

Valoración Cualitativa Datos/Información

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión				
				C	I	A	D	T
[files]	Ficheros	[D_contratos]	Contratos suscritos con los proveedores	6	4	7		

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión				
				C	I	A	D	T
[Backus]	Copias de Respaldo	[D_Copias de Seguridad]	Archivo de copias de seguridad de la información	5			5	

Valoración Cualitativa Aplicaciones Informáticas

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión				
				C	I	A	D	T
[sub]	desarrollo a medida (subcontratado)	[A_Sysman]	Sistema de Información administrativo		6	6	7	
[std]	estándar (off the shelf)	[A_GLPI]	Sistema de Información para solicitar asistencia		5	5	6	
[av]	anti virus	[A_antivirus]	Nod 32 instalación en la nube				6	

Valoración Cualitativa Equipos informáticos

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión				
				C	I	A	D	T
[host]	Grandes equipos	[E_servidor]	Servidor de bases de datos, servidores de dominio e internet	6	6		6	
[pc]	Informática personal	[E_computadores]	Computadores de la entidad	6	6		6	
[switch]	Conmutadores	[E_switch]	Conmutadores de la entidad				5	

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión				
				C	I	A	D	T
[pabx]	Central telefónica	[E_planta]	Planta telefónica		5		5	
[print]	medios de impresión	[E_impresoras]	impresoras				5	

Valoración Cualitativa Soportes de Información

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión				
				C	I	A	D	T
[disk]	discos	[S_copias]	Discos duro extraíbles de respaldo de la información		6		6	

Valoración Cualitativa Redes de Comunicaciones

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión				
				C	I	A	D	T
[LAN]	Red local	[R_lan]	Lan de la entidad				6	

Valoración Cualitativa Equipamiento Auxiliar

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión				
				C	I	A	D	T
[Furniture]	Mobiliario	[M_mobiliario]	Muebles, estantes de la entidad.		5		6	

Valoración Cualitativa Instalación y Personas

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión				
				C	I	A	D	T
[local]	cuarto	B_rack	Rack de Comunicaciones		5		6	
[adm]	administradores de sistemas	B_sistemas	Profesional Universitario de Sistemas				6	
[prov]	proveedores	B_proveedores	Proveedores				6	

5.3. IDENTIFICACIÓN DE AMENAZAS

Para realizar la identificación y valoración de amenazas se tiene en cuenta la frecuencia con las que estas ocurren, las 5 dimensiones de seguridad que denota Magerit y la escala de rango porcentual de impactos en los activos.

Escala de rango de frecuencia de amenazas

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	Se presentó en el último día	100
Frecuencia alta	Se presentó en la última Semana	70
Frecuencia media	Se presentó en el último mes	50
Frecuencia baja	Se presentó en los últimos 6 meses	10
Frecuencia muy baja	No Se presentó en el último año.	5

Dimensiones de Seguridad

Dimensiones de Seguridad	Código
Confidencialidad	C
Autenticidad	A
Integridad	I
Disponibilidad	D
Trazabilidad	T

Escala de rango porcentual de impactos en los activos para cada dimensión de seguridad

Impacto	Valor Cuantitativo
Muy Alto	100%
Alto	70%
Medio	50%
Bajo	20%
Muy bajo	5%

En la siguiente tabla se identifica las amenazas para el inventario de activos realizado, de igual manera, el impacto ante la materialización de la amenaza.

Identificación amenazas e impacto

Nombre grupo de activo Magerit	Nombre activo CDM	Amenaza	Frecuencia de la Amenaza	Impacto para cada dimensión de seguridad %				
				C	I	A	D	T
World wide web	Servicio de internet para los funcionarios	Fallo de servicios de comunicaciones	50				**75%**	
		Caída del sistema por sobrecarga	50				**75%**	
		Desastres industriales	5				75%	
Correo electrónico	Gestión de cuentas de correos electrónicos	Errores de mantenimiento / actualización de programas (software)	5		20%		5%	
		Fuga de información	5	75%				
Interno (a usuarios de la propia organiza-ción)	Asistencia informática a los funcionarios de la entidad	Indisponibilidad del personal	70		20%		75%	
		Ingeniería social	5	75%				

Nombre grupo de activo Magerit	Nombre activo CDM	Amenaza	Frecuencia de la Amenaza	Impacto para cada dimensión de seguridad %				
				C	I	A	D	T
Anónimo (sin requerir identificación del usuario)	Servicio de mantenimiento de la página web	Denegación de servicio	10		50%		100%	5%
		Acceso no autorizado	5	75%	50%	75%		
		Fallo de servicios de comunicaciones	50				100%	
Interno (a usuarios de la propia organización)	Servicio de mensajería Interna	Errores del administrador	50		50%		100%	
		Acceso no autorizado	5			75%		
		Fallo de servicios de comunicaciones	50				75%	
Ficheros	Contratos suscritos con los proveedores	Degradación de los soportes de almacenamiento de la información	5		50%		50%	
		Datos incompletos de los usuarios	5		20%			20%
Copias de respaldo	Archivo de copias de seguridad de la información	Degradación de los soportes de almacenamiento de la información	5		20%		75%	
		Acceso no autorizado	5	20%	20%	50%	20%	
Desarrollo a medida (subcontratado)	Sistema de Información administrativo	Acceso no autorizado	5	20%	75%	100 %		20%
		Errores del administrador	50		50%		75%	

Nombre grupo de activo Magerit	Nombre activo CDM	Amenaza	Frecuencia de la Amenaza	Impacto para cada dimensión de seguridad %				
				C	I	A	D	T
Estándar (off the shelf)	Sistema de información para solicitar asistencia	Errores del administrador	5		50%		75%	
		Acceso no autorizado	5	20%	20%	50%	20%	
Anti virus	ESET Nod 32	Errores del administrador	5		20%		50%	
Grandes equipos	Servidor de bases de datos, servidores de dominio e internet	Pérdida de equipos	5				100%	
		Corte del suministro eléctrico	50		50%		50%	
Informática personal	Computadores de la entidad	Pérdida de equipos	5				100%	
		Corte del suministro eléctrico	50		50%		50%	
Conmuta-dores	Conmuta-dores de la entidad	Fuego	5				20%	
		Pérdida de equipos	5				50%	
Central telefónica	Planta telefónica	Errores del administrador	5		20%		20%	
		Corte del suministro eléctrico	50		50%		50%	
Medios de impresión	Impresoras	Corte del suministro eléctrico	50		50%		50%	
		Pérdida de equipos	5				50%	
Discos	Discos duro extraíbles de respaldo de la información	Degradación de los soportes de almacenamiento de la información	5		50%		100%	
Red local	Lan de la entidad	Desastres naturales	5				50%	

Nombre grupo de activo Magerit	Nombre activo CDM	Amenaza	Frecuencia de la Amenaza	Impacto para cada dimensión de seguridad %				
				C	I	A	D	T
Mobiliario	Muebles, estantes de la entidad.	Fuego	5				50%	
Cuarto	Rack de Comunica-ciones	Desastres naturales	5				50%	
		Fuego	5				50%	
		Ingeniería social	5				50%	
Administra-dores de sistemas	Profesional Universitario de Sistemas	Extorsión	5				50%	
		Ingeniería social	5				50%	
Proveedo-res	Proveedo-res	Extorsión	5				50%	

De acuerdo con los resultados de la identificación de las amenazas y el impacto que tiene para la dependencia, la materialización de una de ellas y la frecuencia con la que ocurren, se decide a través de los siguientes controles mitigar las amenazas con alto riesgo como lo son:

- Fallo de servicios de comunicaciones
- Caída del sistema por sobrecarga
- Indisponibilidad del personal
- Errores del administrador

5.4. CONTROLES DE SEGURIDAD

5.4.1. Salvaguardas

Una vez se han identificado los activos de la entidad y las amenazas que estos representan a su seguridad, se definen salvaguardas con el fin de reducir el riesgo teniendo en cuenta los activos que se van a proteger.

Clasificación Salvaguardas

Efecto	Tipo

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acortan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Tipo de Activo	Nombre grupo de activo Magerit	Código Activo CDM	Nombre activo CDM	Tipo de Protección	Des Salvaguarda
Servicios	World wide web	[S_Internet]	Servicio de internet para los funciona-rios	[MN] de monitorización	Registro de descarga
				[PR] preventivas	Políticas de seguridad
				[RC] recuperativas	Canal redundante
				[AW] de concienciación	Capacitación al personal en el manejo de la información.
				[AD] administrativas	Puesta en marcha del Plan Director
	Correo electróni-co	[S_correo]	Gestión de cuentas de correos electróni-cos	[MN] de monitorización	Registro de descarga
				[PR] preventivas	Políticas de seguridad
				[RC] recuperativas	Canal redundante
				[AW] de concienciación	Capacitación al personal en el manejo de la información.
				[AD] administrativas	Puesta en marcha del Plan Director
	Interno (a usuarios de la propia organizaci ón)	[S_U_soport e]	Asistencia informática a los funciona-rios de la entidad.	[PR] preventivas	Políticas de seguridad
				[RC] recuperativas	Canal redundante
				[AW] de concienciación	Capacitación al personal en el

Tipo de Activo	Nombre grupo de activo Magerit	Código Activo CDM	Nombre activo CDM	Tipo de Protección	Des Salvaguarda
					manejo de la información
				[AD] administrativas	Puesta en marcha del Plan Director
	Anónimo (sin requerir identifica-ción del usuario)	[S_U_página_web]	Servicio de manteni-miento de la página web.	[MN] de monitorización	Registro de descarga
				[PR] preventivas	Políticas de seguridad
				[RC] recuperativas	Canal redundante
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[AD] administrativas	Puesta en marcha del Plan Director
				[RC] recuperativas	Canal redundante
Servicios	Interno (a usuarios de la propia organizaci ón)	[S_U_spark]	Servicio de mensajería Interna	[MN] de monitorización	Registro de Accesos
				[PR] preventivas	Políticas de seguridad
				[RC] recuperativas	Canal redundante
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[AD] administrativas	Puesta en marcha del Plan Director
Datos / Informa-ción	Ficheros	[D_contratos]	Contratos suscritos con los proveedo-res	[PR] preventivas	Políticas de seguridad
				[RC] recuperativas	Canal redundante
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[AD] administrativas	Puesta en marcha del Plan Director

Tipo de Activo	Nombre grupo de activo Magerit	Código Activo CDM	Nombre activo CDM	Tipo de Protección	Des Salvaguarda
	Copias de respaldo	[D_Copias de Seguridad]	Archivo de Copias de seguridad de la información	[PR] preventivas	Políticas de seguridad
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[AD] administrativas	Puesta en marcha del Plan Director
Aplicacio-nes Informáti-cas	Desarrollo a medida (subcon-tratado)	[A_Sysman]	Sistema de Información administra-tivo	[PR] preventivas	Políticas de seguridad
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[RC] recuperativas	Copias de Seguridad
Aplicacio-nes Informáti-cas	Estándar (off the shelf)	[A_GLPI]	Sistema de Información para solicitar asistencia	[PR] preventivas	Políticas de seguridad
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[RC] recuperativas	Copias de Seguridad
	Anti virus	[A_antivirus]	NOD 32	[AW] de concienciación	Capacitación al personal en el manejo de la información
				[MN] de monitorización	Registro de Uso y Descarga
				[EL] eliminatorias	Desinstalar licencias vencidas
				[PR] preventivas	Políticas de seguridad
Equipos informáti-cos	Grandes equipos	[E_servidor]	Servidor de bases de datos, servidores de dominio e internet	[PR] preventivas	Políticas de seguridad
				[AW] de concienciación	Capacitación al personal en el manejo de la información

Tipo de Activo	Nombre grupo de activo Magerit	Código Activo CDM	Nombre activo CDM	Tipo de Protección	Des Salvaguarda
				[RC] recuperativas	Copias de Seguridad
	Informáti-ca personal	[E_computa-dores]	Computado res de la entidad	[PR] preventivas	Políticas de seguridad
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[RC] recuperativas	Copias de Seguridad
Equipos informáti-cos	Conmu-tadores	[E_switch]	Conmutado res de la entidad	[PR] preventivas	Políticas de seguridad
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[RC] recuperativas	Copias de Seguridad
	Central telefónica	[E_planta]	Planta telefónica	[PR] preventivas	Políticas de seguridad
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[RC] recuperativas	Copias de Seguridad
	Medios de impresión	[E_impreso-ras]	impresoras	[PR] preventivas	Políticas de seguridad
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[RC] recuperativas	Copias de Seguridad
Soportes de Informa-ción	discos	[S_copias]	Discos duros extraíbles de respaldo de la información	[PR] preventivas	Políticas de seguridad
				[AW] de concienciación	Capacitación al personal en el manejo de la información

Tipo de Activo	Nombre grupo de activo Magerit	Código Activo CDM	Nombre activo CDM	Tipo de Protección	Des Salvaguarda
				[AD] administrativas	Puesta en marcha del Plan Director

Tipo de Activo	Nombre grupo de activo Magerit	Código Activo CDM	Nombre activo CDM	Tipo de Protección	Des Salvaguarda
Redes de Comunicaciones	Red local	[R_lan]	Lan de la entidad	[PR] preventivas	Políticas de seguridad
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[AD] administrativas	Puesta en marcha del Plan Director
Equipa-miento Auxiliar	Mobiliario	M_mobiliario	Muebles, estantes de la entidad.	[PR] preventivas	Políticas de seguridad
				[AW] de concienciación	Capacitación al personal en el manejo de la información
				[AD] administrativas	Puesta en marcha del Plan Director
Instala-ción y Personas	Cuarto	B_rack	Rack de Comunica-ciones	[DC] de detección	Detección de Incendios
	Adminis-tradores de sistemas	B_sistemas	Profesional Universitario de Sistemas	[AW] de concienciación	Capacitación al personal en el manejo de la información
				[AD] administrativas	Puesta en marcha del Plan Director
	Proveedores	B_proveedores	Proveedo-res	[AW] de concienciación	Capacitación al personal en el manejo de la información

6. MAPA DE RIESGOS GESTION TIC

IDENTIFICACIÒN DEL RIESGO					VALORACION DEL RIESGO (PRIMERA LINEA DE DEFENSA)										
#	TIPO DE RIESGO	CAUSA	RIESGO	CONSECUENCIA	RIESGO INHERENTE			CONTROLES EXISTENTE	RIESGO RESIDUAL			ACCIONES ASOCIADAS AL CONTROL			
					PROBABILIDAD	IMPACTO	NIVEL DE RIESGO		PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	ACCIONES	PERIODO DE EJECUCION	RESPONSABLE	REGISTRO
R 1	Corrupción	1. No se han procedimentado las actividades de mantenimiento de controles al acceso de información 2. No se han identificado los activos de información con sus respectivas amenazas y vulnerabilidades	Acceso no autorizado, alteración, eliminación y/o extracción de información no publica	1. Reclamaciones o quejas de los usuarios. 2. Sanción por parte del ente de control u otro ente regulado. 3. Pérdida de Información crítica para la entidad que no se puede recuperar. 4. Perdida de la imagen institucional	Rara vez	MAYOR	Zona de Riesgo Alta	No existen controles	Rara Vez	Mayor	Zona de Riesgo Alta	1Establecer y publicar la política de seguridad y privacidad de la información 2. Identificar y valorar los activos de información con sus respectivas amenazas y vulnerabilidades	1. 30 de abril de 2019 2. 31 de junio de 2019	Profesional universitario de Sistemas	1. Política aprobada y publicada 2.Listado de activos de información aprobado
R 2	Interno	1. Falta de mantenimiento a las UPS para mitigar ausencias de energía 2. Equipos obsoletos	Pérdida de disponibilidad de la información	1. Retrasos y reprocesos 2. Demandas, sanciones y hallazgos de entes de control	Casi Seguro	Moderado	Zona de Riesgo Extrema	1. Actualización del servidor, copias mensuales de seguridad 2. Suscripción de mantenimiento preventivo	Rara Vez	Moderado	Zona de Riesgo Moderada	1. Incluir en el proceso contractual de mantenimiento preventivo, las UPS 2. Oficiar a la Secretaria General la necesidad de adquisición de equipos de computo	1. 30 de junio de 2019 2. 30 de marzo de 2019	Profesional universitario de Sistemas	1. Cronograma de mantenimiento 2. Oficio de necesidades

IDENTIFICACIÒN DEL RIESGO					VALORACION DEL RIESGO (PRIMERA LINEA DE DEFENSA)										
#	TIPO DE RIESGO	CAUSA	RIESGO	CONSECUENCIA	RIESGO INHERENTE			CONTROLES EXISTENTE	RIESGO RESIDUAL			ACCIONES ASOCIADAS AL CONTROL			
					PROBABILIDAD	IMPACTO	NIVEL DE RIESGO		PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	ACCIONES	PERIODO DE EJECUCION	RESPONSABLE	REGISTRO
R 3	Interno	Falta de conciencia de los funcionarios en cuanto a las consecuencias de revelar la información confidencial.	Pérdida de confidencialidad de la información	1. Reclamaciones o quejas de los usuarios. 2. Sanción por parte del ente de control u otro ente regulado. 3. Pérdida de la imagen institucional 4. Beneficios a terceros	Rara vez	Moderado	Zona de Riesgo Moderada	Política de uso de los recursos informáticos	Rara Vez	Moderado	Zona de Riesgo Moderada	Sensibilización de la política de operación de uso de los recursos informáticos.	30 de abril de 2019 31 de agosto de 2019 31 de diciembre de 2019	Profesional universitario de Sistemas Profesional de Comunicaciones	Constancia de envío del mensaje
R 4	Seguridad Digital	1. No actualización del Antivirus	Infección por virus que afecta la funcionalidad del Software	Daño del software	Casi Seguro	Menor	Zona de Riesgo Alta	Política de operación del uso de recursos informáticos Antivirus	Posible	Insignificante	Zona de Riesgo Baja	1. Divulgar el Plan/Manual de Seguridad y Privacidad de la Información (600.01.101) 2. Actualizar la política de operación del uso de los recursos informáticos (socializada) 3. Continuar con el control existente- Antivirus	1. Trimestre II /2019 2. Trimestre II /2019 3. Trimestre II / 2019	Profesional de Comunicaciones Profesional Universitario Sistemas	1. Spark socialización 2. Actualización de Política y boletín interno 3.implementación plataforma antivirus

IDENTIFICACIÒN DEL RIESGO					VALORACION DEL RIESGO (PRIMERA LINEA DE DEFENSA)			
#	TIPO DE RIESGO	CAUSA	RIESGO	CONSECUENCIA	RIESGO INHERENTE	CONTROLES EXISTENTE	RIESGO RESIDUAL	ACCIONES ASOCIADAS AL CONTROL

					PROBABILIDAD	IMPACTO	NIVEL DE RIESGO		PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	ACCIONES	PERIODO DE EJECUCION	RESPONSABLE	REGISTRO
R 5	Seguridad Digital	1. Instalación de programas y descargas de archivos sin autorización del administrador de la red. 2. Falta de conciencia de los funcionarios sobre las políticas de seguridad digital.	Vulnerabilidad ante la ingeniería social	Pérdida económica y pérdida de la información	Casi Seguro	Moderado	Zona de Riesgo Extrema	No existe	Casi Seguro	Moderado	Zona de Riesgo Extrema	1. Socialización de la política de seguridad y privacidad de la información 2. Sensibilización por medio de mensaje interno a los funcionarios sobre las políticas de seguridad digital.	1. 31 de mayo de 2019 2. 31 de julio de 2019 31 de octubre de 2019 31 de diciembre de 2019	Profesional universitario de Sistemas Profesional de Comunicaciones	1. Banner Web 2. Banner Intranet
R 6	Seguridad Digital	1. Falta de controles de acceso al servidor físico.	Acceso no autorizado al cuarto de telecomunicaciones.	Pérdida económica y pérdida de la información	Casi Seguro	Mayor	Zona de Riesgo Extrema	Señalización	Casi Seguro	Mayor	Zona de Riesgo Extrema	1. Asegurar el acceso al cuarto de telecomunicaciones	30 de abril de 2019	Secretaria General Profesional Universitario Sistemas	Registro fotográfico de la gestión adelantada

7. CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Ítem	Actividad	Responsable	Fecha
1	Crear y/o modificar política de tratamiento de riesgos de seguridad y privacidad de la información	Oficina de Gestión TI	30/04/2019
2	Actualizar listado de activos de información para proteger	Líderes de Proceso	30/04/2019
3	Identificar y/o actualizar amenazas que puedan afectar los activos	Líderes de proceso	31/05/2019
4	Actualizar la valoración de las amenazas que puedan afectar los activos incluido el riesgo	Líderes de proceso	31/05/2019
5	Implementar los controles de seguridad necesarios para mitigar el los riesgos identificados en el mapa de riesgos de Gestión TIC	Líderes de proceso	Según período de ejecución 600.02.572

8. SEGUIMIENTO Y EVALUACIÓN

En primera instancia el seguimiento se debe llevar a cabo por el responsable del proceso quien debe autoevaluarse e indicar la efectividad de sus controles para minimizar el riesgo, segundo momento de seguimiento por parte de área de sistemas y tercer momento por la Oficina de Control Interno quien dentro de la auditoría realizada al proceso de Gestión TIC entregará las propuestas de mejoramiento y tratamiento a las situaciones detectadas en ésta ámbito.

Las valoraciones integrales de toda la Entidad y particulares por proceso, proyecto o estrategia correspondiente a la disminución del nivel de vulnerabilidad, deben hacerse anualmente conforme la directriz institucional.

Cada semestre se realizará seguimiento a todo el componente de administración de riesgos articulado con el plan de seguridad y privacidad de la información y verificará aspectos como:

- Cumplimiento de las políticas y directrices para la administración del riesgo: metodología de administración del Riesgo (diseño y funcionamiento).

- Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones, lo cual se hace a través de los siguientes indicadores:

Indicador 01: AJUSTE POLÍTICA DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (Mide actividad 1 del cronograma del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información)

DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
V1. Política de tratamiento de riesgos de seguridad y privacidad de la información creada, ajustada y socializada	(V1 / V2) *100	Guía del modelo de operación del marco de seguridad y privacidad de la información
V2: Política de tratamiento de riesgos de seguridad y privacidad de la información programada para creación, ajuste y socialización		

METAS

MINIMA	75-80 %	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

OBSERVACIONES

Busca identificar el nivel de estructuración de los procesos de la entidad orientados a la seguridad de la información.

Indicador 02: CUBRIMIENTO ACTIVOS DE INFORMACIÓN (Miden actividades 2, 3 y 4 del cronograma del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información)

DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
V1. Número de activos críticos de información incluidos en el alcance de implementación del modelo, incluidos en la zona de riesgo inaceptable y la implementación del control no requiere adquisición de elementos de hardware o software.	(V1 / V2) *100	Alcance del SGSI, Inventario de Activos de información, plan de tratamiento, matriz de riesgos
V2: Número de activos críticos de información incluidos en el alcance de implementación del modelo; activos incluidos en la zona de riesgo inaceptable.		Inventario de Activos de información, nuevos

METAS

MINIMA	75-80 %	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

OBSERVACIONES

El indicador de cada proceso debe ser recolectado y promediado para construir un indicador que refleje el estado de la CDM. El terminó “incluir un activo” debe ser entendido como realizar la correcta

clasificación del activo, tratamiento, evaluación de riesgos y amenazas sobre el mismo y determinación de controles para minimizar el riesgo calculado. Para este indicador, solo se tienen en cuenta los controles que no implican adquisición de hardware o software.

Indicador 03: CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (Mide actividad 5 del cronograma del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información)

DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
V1. Controles de riesgos implementados	(V1 / V2) *100	Herramientas de Monitoreo/Usuarios Internos.
V2: Controles de riesgos implementados		

METAS

MINIMA	75-80 %	**SATISFACTORIA**	80 – 90 %	**SOBRESALIENTE**	100%

OBSERVACIONES

Busca identificar riesgos de seguridad y privacidad de la información y los controles implementados por la Entidad para su mitigación.

9. CONTROLES

- El profesional universitario con funciones de sistemas, elabora el plan de seguridad y privacidad de la información para mitigar los riesgos, junto con la política respectiva. Este plan tiene una periodicidad de ejecución anual.

- El Asesor de Planeación, Gestión de Calidad y Comunicaciones, realiza seguimiento de manera semestral al cumplimiento de las metas establecidas en el plan de seguridad y privacidad de la información, el cual se consolida en los informes del primer semestre de cada vigencia y en el de gestión anual de la entidad, presentados al (a) Contralor (a) Departamental.

- El Asesor (a) de Planeación, Gestión de Calidad y Comunicaciones realiza control al plan de acción de PETIC, mediante el diligenciamiento del formato 600.02.677 Seguimiento plan de acción PETIC, donde se establece la actividad de ejecutar al 100% el plan de seguridad y privacidad de la información.

10. FLUJOGRAMA

No aplica

11. DOCUMENTOS DE REFERENCIAS

- Normatividad relacionada con Seguridad y Privacidad de la Información.