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

Tabla de Contenido

INTRODUCCIÓN

Las organizaciones de todo tipo y tamaño enfrentan factores e influencias, internas y externas, que crean incertidumbre sobre si, ellas lograran o no sus objetivos. El efecto que esta incertidumbre tiene en los objetivos de una organización es el “riesgo”.

Todas las actividades de una organización implican riesgo. Las organizaciones gestionan los riesgos mediante su identificación y análisis y luego evaluando si el riesgo se debería modificar por medio del tratamiento del riesgo con el fin de satisfacer los criterios del riesgo.

El MINENERGÍA, prácticamente desde antes y después de haber obtenido su certificación en el Sistema de Gestión de Calidad, ha establecido entre sus colaboradores, un ambiente de trabajos con enfoque a la cultura del riesgo en todas sus dependencias y grupos de trabajo.

Durante la ejecución del Contrato GGC N° 470 de 2017-2018, se dictaron talleres de riesgos a los Coordinadores y encargados de todos los procesos misionales, estratégicos, de apoyo y especiales.

Lo anterior como estrategia de adopción de una cultura de administración para la administración, seguimiento, gestión y control de riesgos en el MINENERGÍA, donde los mismos son registrados anualmente ante la Oficina de Planeación y Gestión Internacional (OPGI), con seguimiento y monitoreo trimestralmente.

1. CONTEXTUALIZACIÓN

El Ministerio de Minas y Energía, cuenta con una plataforma en el SIGME donde las diferentes dependencias publican sus riesgos, la actualización de estos riesgos se realiza cada año según las directrices de la Oficina de Planeación y Gestión Internacional. A excepción de algunos riesgos publicados por el Grupo de Infraestructura Tecnológica, sobre la gestión de la información.

No se catalogan los riesgos de información postulados por otras dependencias, pero si los consideran en sus valoraciones en el sentido que, sus productos involucren las plataformas tecnológicas, o afectaciones de sus resultados por pérdida de información impresa, escrita, o documental, de la cual no se cuente con respaldo electrónico o magnético.

Para todos los efectos, el MINENERGÍA hace acopio de las metodologías y normas vigentes para el análisis, gestión y tratamiento del riesgo, en especial la "*Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas-Riesgos de Gestión, Corrupción y Seguridad Digital-Versión 4.0"*

2. ANTECEDENTES

En los últimos años, hemos visto que los modelos de computación tradicionales han sido puestos “del revés”, en algunos casos, de forma literal. Además, al tiempo que ha cambiado el paisaje tecnológico, también lo ha hecho el entorno de amenazas, así como los diferentes métodos para defender contra esas amenazas. El trabajo con la seguridad de la información siempre será como jugar al gato y al ratón, ya que los proveedores de tecnología intentan seguir el ritmo al cambio permanente en los atacantes y el paisaje de amenazas. No obstante, existe una falta de correspondencia entre las amenazas actuales y las defensas adecuadas para proteger realmente los activos de una organización. Respecto al hecho de que el gasto en seguridad sigue aumentando cada año, podría argumentarse que, en el peor de los casos, gran parte de ese dinero se desperdicia o, en el mejor, se asigna de manera sub óptima.

Debido a este panorama si no se cuenta con una apropiada cultura de gestión de riesgos y oportuna gestión de incidentes por parte de los usuarios finales será complicado establecer enfoques proactivos ante un cambio tan dinámico de los entornos digitales.

Es importante que los usuarios manifiesten cualquier incidente relacionado con la confidencialidad, integridad y disponibilidad de la información y no convivan con los problemas, por otro lado, ante incidentes de este tipo y que sean catalogados como críticos se debe establecer un procedimiento de investigación de causa, para poder gestionar futuros incidentes relacionados o parecidos de una manera más efectiva.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Establecer una cultura de gestión de riesgos en el MINENERGÍA a partir de un Excel elaborado donde se realiza una declaración fundamentada de cada riesgo relacionado con la seguridad de la información.

3.2. OBJETIVOS ESPECÍFICOS

- Establecer mapas de calor basados en las identificaciones de riesgos que se realicen en las diferentes dependencias.

- Lograr altos niveles de madurez en la gestión del riesgo, de tal manera que los dueños de proceso ayuden a identificar controles apropiados para reducir, mitigar y/o administrar el riesgo.

- Establecer indicadores de gestión de riesgos en seguridad de la información a nivel institucional.

4. DESARROLLO

4.1. PARÁMETROS DE VALORACION PARA LA PROBABILIDAD

Categoría	Valor categoría	Descripción	Frecuencia
RARO	1	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
IMPROBABLE	2	El evento puede ocurrir en algún momento.	Al menos de una vez en los últimos 5 años.
POSIBLE	3	El evento podría ocurrir en algún momento.	Al menos de una vez en los últimos 2 años.
PROBABLE	4	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de una vez en el último año.
CASI SEGURO	5	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.

Tabla 1: Parámetros de valoración para la probabilidad

4.2. PARÁMETROS DE VALORACIÓN PARA LOS IMPACTOS

Categoría	Valor categoría	Impacto de confidencialidad	Impacto de credibilidad o imagen	Impacto legal	Impacto operativo
LEVE	1	Personal	Grupo de funcionarios	Multas	Ajustes a una actividad concreta.
MENOR	2	Grupo de trabajo	Todos los funcionarios	Demandas	Cambios en los procedimientos.
MODERADO	3	Relativa al proceso	Usuarios ciudad	Investigación Disciplinaria	Cambios en la interacción de los procesos.
ALTO	4	Institucional	Usuarios región	Investigación Fiscal	Intermitencia en el servicio.
CATASTROFICO	5	Estratégica	Usuarios país	Intervención - Sanción	Paro total del Proceso.

Tabla 2: Parámetros de valoración para los impactos

4.3. DECLARACIÓN FUNDAMENTADA DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN

Riesgo: R1

Perdida de Disponibilidad ante fallas en software debido a que no se renuevan algunos contratos de soporte críticos con fabricantes y/o fabricas de software.

Riesgo Inherente

(IC:	1	+	II:	5	+	IL:	5	+	IO:	4	)		X	PR:	5	=	RIESGO:	75

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABIL	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACIO N (0-2)	SOLIDEZ (Exi) (1-10)
01	Se registra Orden de Compra 36783 del 28-03-2019 -Mesa de Ayuda	###	5	2	10
02	El contrato de mesa de ayuda de servcios de TI, se encuentra vigente hasta el 31/12/2019	0,0%	5	2	10
03					0
04					0
05					0
		####		10,0	10,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACIO N (0-2)	SOLIDEZ (Exi) (1-10)
06		0,0%			0
07		0,0%			0
08					0
09					0
10					0
		0,0%		#¡DIV/0!	0,0

Nivel de Exposición

(IF:	1	+	IR:	5	+	IO:	5	+	IL:	4	)	15	X	PR:	1	=	RIESGO:	15

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABIL	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACIO N (0-2)	SOLIDEZ (Exi) (1-10)
01	Contrato de soporte con Red Hat	###	4	0	0
02	Contrato de soporte con Oracle	0,0%	4	0	0
03					0
04					0
05					0
		####		#¡DIV/0!	0,0
					10

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACIO N (0-2)	SOLIDEZ (Exi) (1-10)
06		###			0

Ilustración 1: Riesgos tecnologías de la información – R1

Riesgo: R2

No se tienen penalidades a contratistas correlacionadas con incumplimientos, deficiencia de servicios, fallas o errores en los sistemas en producción y caídas de las plataformas tecnológicas.

Riesgo Inherente

(IC:	5	+	IR:	5	+	IO:	4	+	IL:	3	)		X	PR:	5	=	RIESGO:	

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILID	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01	Para proveedores como INTERNEXA y UNE	###	4	2	8
02	Se tiene establecidas penalidades en la prestación del servicio como sucede por ejemplo en los acuerdo de servicio (ANS) de los canales de comunicación	0,0%			0
03					0
04					0
05					0
		100,0%		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
06		###			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#DIV/0!	0,0

Nivel de Exposición

(IF:	5	+	IR:	5	+	IO:	4	+	IL:	3	)	17	X	PR:	2	=	RIESGO:	

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILID	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01		###			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#DIV/0!	0,0

Ilustración 2: Riesgos tecnologías de la información – R2

Riesgo: **R3**

Falencias en Gobierno de TIC por no aplicar buenas practicas basadas en ITIL y una apropiada gestión de riesgos.

Riesgo Inherente

(IC:	4	+	IR:	2	+	IO:	3	+	IL:	3	)		X	PR:	5	=	RIESGO:	60

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	Se lleva registro del Catálogo de Servicios - ARANDA	###	5	2	10
02	Se lleva Registro de Incidentes - ARANDA	0,0%	5	2	10
03	Con contrato No. 750 de 2019, se realiza renovación del licenciamiento de Aranda y comra de más licencias.		4	2	8
04					0
05					0
		####		9,3	9,3

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		###			0
07		0,0%			0
08					0
09					0
10					0
		####		#¡DIV/0!	0,0

Nivel de Exposición

(IF:	4	+	IR:	2	+	IO:	3	+	IL:	3	)	12	X	PR:	1	=	RIESGO:	12

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		###			0
02		0,0%			0
03					0
04					0
05					0
		####		#¡DIV/0!	0,0
					9

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)

Ilustración 3: Riesgos tecnologías de la información - R3

Riesgo: R4

No se tiene absoluto control de la plataforma crítica del MINMINAS debido a que un alto porcentaje de servicios de la administración de la plataforma esta TERCERIZADO.

Riesgo Inherente

(IC:	5	+	IR:	5	+	IO:	2	+	IL:	3	)		X	PR:	5	=	RIESGO:	75

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	Se realizó Contrato Prestación de Servicios Admon Centro de Cómputo y Plataformas Claves	####	4	2	8
02	Se mantiene el contrato de Prestación de servicios profesionales del Administrador del Centro de Cómputo	0,0%	4	2	8
03	El contrato de Prestación de servcios se encuentra vigente hasta el 31/12/2019		4	2	8
04					0
05					0
		100,0%		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

												15						
(IF:	5	+	IR:	5	+	IO:	2	+	IL:	3	)	15	X	PR:	2	=	RIESGO:	30

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		####			0
02		0,0%			0
03					0
04					0
05					

Ilustración 4: Riesgos tecnologías de la información - R4

Riesgo: R5

Software - No existe una metodología de desarrollo seguro usada en la entidad.
Falta de metodología de desarrollo seguro.

Riesgo Inherente

(IC:	5	+	IR:	5	+	IO:	5	+	IL:	5	)		X	PR:	4	=	RIESGO:	80

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	Existe la Metodología: ARQUITECTURA DE REFERENCIA PARA EL DESARROLLO DE NUEVAS APLICACIONES DEL MINISTERIO DE MINAS Y	####	4	2	8
02	Se mantiene la metodologia	0,0%	5	2	10
03	El documento de Metódología de Pruebas no funcionales se encuentra actualizado con fecha de noviembre de 2019.		5	2	10
04					0
05					0
		100,0%		9,3	9,3

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición 20

(IF:	5	+	IR:	5	+	IO:	5	+	IL:	5	)	20	X	PR:	1	=	RIESGO:	20

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	Adquirir una herramienta de revisión de código.	####			0
02	Documentar una metodología de Desarrollo Seguro.	0,0%			0
03					0
04					0
05					

Ilustración 5: Riesgos tecnologías de la información - R5

Riesgo: R6

No se cuenta con los roles de Oficial de Seguridad de la Información y Oficial de Continuidad de Negocio, o quienes haga sus veces, que permitan ser preventivos en el tratamiento de riesgos de confidencialidad, integridad y disponibilidad.

Riesgo Inherente

(IC:	4	+	IR:	4	+	IO:	2	+	IL:	2	)		X	PR:	4	=	RIESGO:	48

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	En cuanto a esta actividad no se han definido el rol del Oficial seguridad de la Información.	####	1	0	0
02	En cuanto a esta actividad no se ha nombrado los roles de los Oficiales de seguridad de la Información y Continuidad del Negocio	0,0%	1	0	0
03					0
04					0
05					0
		#####		#¡DIV/0!	0,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		#####		#¡DIV/0!	0,0

Nivel de Exposición 12

(IF:	4	+	IR:	4	+	IO:	2	+	IL:	2	)	12	X	PR:	4	=	RIESGO:	48

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		####			0
02		0,0%			0
03					0
04					0

Ilustración 6: Riesgos tecnologías de la información - R6

Riesgo: R7

No existen apropiadas contramedidas para proteger las acciones de los empleados de contratistas y control sobre los equipos que estos utilizan dentro de las redes del MINENERGÍA

Riesgo Inherente

(IC:	3	+	IR:	3	+	IO:	3	+	IL:	3	)		X	PR:	3	=	RIESGO:	36

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	Todo el tráfico generado en los equipos del Ministerio de Minas y Energpia es auditado y controlado por Firewall de autenticación y ademas los contratistas cuentan con usuario y contraseña de autenticación con el dominio	###	4	2	8
02	Los permisos de acceso a la red del Minietrio de Minas y Energía se rigen por las fechas establecidas en el formato de ciclo de vida. Por lo tanto, los cantratistas al finalizar su periodo del contrato, se inhabilitan todos los provilegios de acceso.	0,0%	4	2	8
03					0
04					0
05					0
		100,0%		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		###			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición 12

(IF:	3	+	IR:	3	+	IO:	3	+	IL:	3	)	12	X	PR:	2	=	RIESGO:	24

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		###			0
02		0,0%			0
03					0

Ilustración 7: Riesgos tecnologías de la información - R7

Riesgo: R8

Software - Carencia de una metodología de pruebas al Software desarrollado.
Falta de pruebas de carga, stress, abuso, entre otras.

Riesgo Inherente

(IC:	1	+	IR:	3	+	IO:	4	+	IL:	2	)		X	PR:	4	=	RIESGO:	40

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Ext) (1-10)
01	Con el fin de mitigar el control de este riesgo se está desarrollando una metodología para realizar pruebas no funcionales al software desarrollado	####	4	2	8
02	El documento de Metódología de Pruebas no funcionales se encuentra actualizado con fecha de noviembre de 2019.	0,0%	4	2	8
03					0
04					0
05					0
		#####		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Ext) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		#####		#¡DIV/0!	0,0

Nivel de Exposición 10

(IF:	1	+	IR:	3	+	IO:	4	+	IL:	2	)	10	X	PR:	2	=	RIESGO:	20

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Ext) (1-10)
01		####			0
02		0,0%			0
03					0

Ilustración 8: Riesgos tecnologías de la información - R8

Riesgo: R9

Software - Carencia de una Metodología de pruebas al Software desarrollado.

Riesgo Inherente

(IC:	5	+	IR:	5	+	IO:	5	+	IL:	5	)		X	PR:	3	=	RIESGO:	60

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	El Grupo TIC del Ministerio de Minas y Energía, ha eleborado un documento de Metódología de Pruebas no funcionales que se encuentra actaulizado con fecha a noviembre de 2019.	####	4	2	8
02		0,0%			0
03					0
04					0
05					0
		100,0%		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición 20

(IF:	5	+	IR:	5	+	IO:	5	+	IL:	5	)	20	X	PR:	2	=	RIESGO:	40

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		####			0
02		0,0%			0
03					0
04					0
05					

Ilustración 9: Riesgos tecnologías de la información - R9

Riesgo: **R10**

Falencias en el aseguramiento de redes. Ej. VLAN´s Inalámbricas y Asignación de VPN's

Riesgo Inherente

(IC:	3	+	IR:	3	+	IO:	3	+	IL:	3	)		X	PR:	3	=	RIESGO:	36

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (ExI) (1-10)
01	Se adelanta el proceso de reestructuración de la Red con la asignación correcta de la VLANS por dependencias o dispositivos finales como servidores, cámaras de seguridad, impresoras, entre otros. Para la Asignación de las VPNS se encuentra en proyecto un procedimiento que se anexa al formato de ciclo de vida de cómo y cuándo se hace la asignación de las VPNS para los usuarios finales	####	4	2	8
02	Se mantiene el control por medio del Formato de Ciclo de Vida solamente aplicando los privilegiós necesarios por el tiempo de vigencia del contrato.	0,0%	4	2	8
03					0
04					0
05					0
		#####		8,0	8,0
	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	**PESO**	**EFECTIVIDAD (1-5)**	**IMPLEMENTACION (0-2)**	**SOLIDEZ (ExI) (1-10)**
06		####			0
07		0,0%			0
08					0
09					0
10					0
		#####		#¡DIV/0!	0,0

Nivel de Exposición

										12								
(IF:	3	+	IR:	3	+	IO:	3	+	IL:	3	)	12	X	PR:	2	=	RIESGO:	24

Controles Recomendados

Ilustración 10: Riesgos tecnologías de la información - R10

Riesgo: **R11**

Falencias en la revisión, monitoreo, y registro a los Logs de seguridad y errores, eliminándolos sin control alguno.

Riesgo Inherente

(IC:	4	+	IR:	4	+	IO:	4	+	IL:	4	)		X	PR:	3	=	RIESGO:	48

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01	La plataforma de seguridad perimetral almacenada en cuanto a los logs de seguridad, cuenta con una plataforma de proposito especificifico desde la cual se exportan estos datos para tomar deciciones.	#####	4	2	8
02	Se hace un monitoreo con mayor frecuencia con el fin de mitigar posibles riesgos de seguridad (a nivel de infraestructura) y los log quedan almacenados en Disco Duro del equipo Fortianalyzer con el fin de realizar posteriores consultas	0,0%	4	2	8
03					0
04					0
05					0
		####		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
06		#####			0
07		0,0%			0
08					0
09					0
10					0
		####		#¡DIV/0!	0,0

Nivel de Exposición

												16						
(IF:	4	+	IR:	4	+	IO:	4	+	IL:	4	)	16	X	PR:	2	=	RIESGO:	32

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)

Ilustración 11: Riesgos tecnologías de la información - R11

Riesgo: **R12**

Personas - Los funcionarios del Ministerio no firman acuerdos de confidencialidad.
No se evidencian cláusulas de confidencialidad aplicadas a los funcionarios, contratistas y proveedores.

Riesgo Inherente

(IC:	5	+	IR:	4	+	IO:	3	+	IL:	5	)		X	PR:	5	=	RIESGO:	85

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	Se firman Acuerdos de Confidencialidad con los Proveedores Grupo TIC	####	5	2	10
02	Se continua con la firma de acuerdos de confidencialidad con los contratistas.	0,0%	4	2	8
03					0
04					0
05					0
		#####		9,0	9,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06	Se firmó Acuerdo de Confidecialidad con los Contratistas Grupo TIC 2019	####	4	2	8
07		0,0%			0
08					0
09					0
10					0
		#####		8,0	8,0

Nivel de Exposición 17

(IF:	5	+	IR:	4	+	IO:	3	+	IL:	5	)	10	X	PR:	1	=	RIESGO:	10

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	Realizar campaña de firma de acuerdos de confidencialidad.	####			0
02		0,0%			0
03					0
04					0

Ilustración 12: Riesgos tecnologías de la información - R12

Riesgo: R13

Indisponibilidad ante una falla prolongada de flujo de energía eléctrica y caída total de las UPS's de 30 KVA y 80 KVA que soportan en centro de computo.

Riesgo Inherente

(IC:	1	+	IR:	5	+	IO:	5	+	IL:	3	)		X	PR:	4	=	RIESGO:	56

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	Contratar la adquisición, instalación, configuración y puesta en funcionamiento de un Sistema de Alimentación Ininterrumpida (UPS) para el Ministerio de Minas y Energía y cuyas características técnicas se encuentran detalladas en los documentos de condiciones especiales (Formato de Características Técnicas)	####	4	2	8
02	Se encuentra en operación el Sistema de Alimentación Ininterrumpida (UPS) para el Ministerio de Minas y Energía, el cual presta los siguientes servicios alimentación electrica una vez haya interrupción de la energia comercial, regula los picos de voltaje cuando regresa la energia comercial, de esta gorma se garanatiza los disponibilidad de los servicios de TI por ausencia electrica	0,0%	4	2	8
03					0
04					0
05					0
		100,0%		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

(IF:	1	+	IR:	5	+	IO:	5	+	IL:	3	)	14	X	PR:	2	=	RIESGO:	28

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		####			0
02					0

Ilustración 13: Riesgos tecnologías de la información - R13

Riesgo: **R14**

No se tiene una política ni procedimiento establecido, para la eliminación permanente de información y remoción de licencias de software en medios y equipos dados de baja.
No se realiza eliminación segura en medios de almacenamiento.

Riesgo Inherente

(IC:	4	+	IR:	3	+	IO:	2	+	IL:	4	)		X	PR:	4	=	RIESGO:	52

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	No se cuenta con una política ni procedimiento para la eliminacón de información. No se han aplicado controles proventivos a este riesgo	###	1	1	0
02	En cuanto a la renovación de Licencias estas son notificada al Grupo de Servicios Administrativos para dar de baja.	0,0%	4	2	8
03					0
04					0
05					0
		100,0%		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		###			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición 13

(IF:	4	+	IR:	3	+	IO:	2	+	IL:	4	)	13	X	PR:	2	=	RIESGO:	26

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		###			0
02		0,0%			0
03					0
04					0
05					0

Ilustración 14: Riesgos tecnologías de la información - R14

Riesgo: **R15**

Probabilidad de ingresos no autorizados a sistemas del MINMINAS por personal no autorizado.
Carencia de una política de gestión de contraseñas.
No se establece un periodo de cambio de contraseña.

Riesgo Inherente

(IC:	4	+	IR:	4	+	IO:	2	+	IL:	2	)		X	PR:	4	=	RIESGO:	48

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	El administrador es el único que puede cambiar la contraseña si esta es olvidada.	####	4	2	8
02	El administrador del sistema de información es el autorizado para restablecer contraseñas de los usuarios en caso de ser necesario	0,0%	4	2	8
03					0
04					0
05					0
		#####		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		#####		#¡DIV/0!	0,0

Nivel de Exposición

											12							
(IF:	4	+	IR:	4	+	IO:	2	+	IL:	2	)	12	X	PR:	2	=	RIESGO:	24

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		####			0
02		0,0%			0

Ilustración 15: Riesgos tecnologías de la información - R15

Riesgo: **R16**

Falta de pruebas de contingencia.
No se tiene un procedimiento establecido para la recuperación de caídas en dispositivos activos de red.

Riesgo Inherente

(IC:	4	+	IR:	4	+	IO:	4	+	IL:	2	)		X	PR:	3	=	RIESGO:	42

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	Se cuenta con una herramieenta denominada Op Manager para hacer monitore de los dispositivos activos de la red.	####	4	2	8
02	El Ingeniero de Seguridad se encuentra documentando las guias o instructivos de las funciones de operación de recuperación de dispositivos.	0,0%	3	2	6
03					0
04					0
05					0
		#####		7,0	7,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		#####		#¡DIV/0!	0,0

Nivel de Exposición

(IF:	4	+	IR:	4	+	IO:	4	+	IL:	2	)	14	X	PR:	2	=	RIESGO:	28

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		####			0
02		0,0%			0
03					

Ilustración 16: Riesgos tecnologías de la información - R16

Riesgo: R17

Los usuarios que ingresan a la red inalámbrica no son autenticados contra el Directorio Activo.
Falta de control con el ingreso de usuarios y visitantes a la red inalámbrica.

Riesgo Inherente

(IC:	3	+	IR:	3	+	IO:	3	+	IL:	3	)		X	PR:	3	=	RIESGO:	36

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01	Se tiene VLAN independiente para visitantes.	###	4	2	8
02	Se mantine configurada una red para visitantes únicamente con acceso básico a internet, en cuanto autenticación se han configurado un portal	0,0%	4	2	8
03					0
04					0
05					0
		100,0%		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
06		###			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición 12

(IF:	3	+	IR:	3	+	IO:	3	+	IL:	3	)	12	X	PR:	2	=	RIESGO:	24

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01		###			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					8

Ilustración 17: Riesgos tecnologías de la información - R17

Riesgo: **R18**

No se tiene un estándar para el manejo de información confidencial.
El MINENERGÍA carece de un procedimiento que controle la Información confidencial.
No se utilizan herramientas tecnológicas para controles criptográficos.

Riesgo Inherente

(IC:	3	+	IR:	3	+	IO:	3	+	IL:	3	)		X	PR:	3	=	RIESGO:	36

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	El Grupo Información y Servicio al Ciudadano desarrolla actividades de ejecución del contrato GGC-530-2019 para definir los lineamientos necesarios y toma de decisiones de una herramienta que permita cumplir con la caracterización de documentos electrónicos de archivo producidos y gestionados por un Sistema de Información.	####	4	1	4
02	El Grupo Información y Servicio al Ciudadano definio 8 lineamientos con el fin de implementar una solución de Gestión Docuemental dentra de ellas se encuEntra el tema de manejo de información confidencial.	0,0%	4	2	8
03					0
04					0
05					0
		#####		6,0	6,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		#####		#¡DIV/0!	0,0

Nivel de Exposición 12

(IF:	3	+	IR:	3	+	IO:	3	+	IL:	3	)	12	X	PR:	3	=	RIESGO:	36

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01					

Ilustración 18: Riesgos tecnologías de la información - R18

Riesgo: R19

No se tiene una política establecida para la verificación de software creados dentro y fuera del MINENERGÍA.
No se cuenta con protección de inyección de código.

Riesgo Inherente

(IC:	3	+	IR:	3	+	IO:	3	+	IL:	3	)		X	PR:	3	=	RIESGO:	36

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Ext) (1-10)
01	Se cuenta con una metodología para el desarrollo de sistemas de información.	####	4	2	8
02	El administrador de la plataforma permanece realizando monitoreo a los servidores y el antivirus SE corre través de los PCs con el fin de minimizar que se cree softw are ´malicioso en las máquinas	0,0%	4	2	8
03	En el Fire wall se encuntra configuras varias reglas el cual cuenta con protección basada en firmas que detecta cualquier inyección en codigo y lo		4	2	8
04					0
05					0
		#####		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Ext) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		#####		#¡DIV/0!	0,0

Nivel de Exposición 12

(IF:	3	+	IR:	3	+	IO:	3	+	IL:	3	)	12	X	PR:	2	=	RIESGO:	24

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Ext) (1-10)
01		####			0
02					0

Ilustración 19: Riesgos tecnologías de la información - R19

Riesgo: R20

Falencias en el control de usuarios a áreas restringidas.
No se posee control de acceso a áreas restringidas.

Riesgo Inherente

(IC:	3	+	IR:	3	+	IO:	3	+	IL:	3	)		X	PR:	3	=	RIESGO:	36

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	En Centro de Datos se tiene acceso controlado	####	4	2	8
02	Se mantienen los permisos de acceso al Centro de Cómputo.	0,0%	4	2	8
03	Se implemento restricción de acceco a usuarios no autorizados al Grupo de TIC		4	2	8
04					0
05					0
		#####		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		#####		#¡DIV/0!	0,0

Nivel de Exposición 12

(IF:	3	+	IR:	3	+	IO:	3	+	IL:	3	)	12	X	PR:	2	=	RIESGO:	24

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		####			0
02		0,0%			0
03					0
04					0

Ilustración 20: Riesgos tecnologías de la información - R20

Riesgo: **R21**

Falencias en la clasificación de información.
Desconocimiento de lo que es información confidencial.

Riesgo Inherente

(IC:	3	+	IR:	3	+	IO:	3	+	IL:	3	)		X	PR:	3	=	RIESGO:	36

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	El Grupo Información y Servicio al Ciudadano desarrolla actividades de ejecución del contrato GGC-530-2019 para definir los lineamientos necesarios y toma de decisiones de una herramienta que permita cumplir con la caracterización de documentos electrónicos de archivo producidos y gestionados por un Sistema de Información.	####	4	2	8
02	El Grupo Información y Servicio al Ciudadano definio 8 lineamientos con el fin de implementar un asolución de Gestión Docuemental dentra de ellas se encuntra el tema de manejo de información confidencial.	0,0%	4	2	8
03					0
04					0
05					0
		#####		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		#####		#¡DIV/0!	0,0

Nivel de Exposición 12

(IF:	3	+	IR:	3	+	IO:	3	+	IL:	3	)	12	X	PR:	2	=	RIESGO:	24

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		####			0

Ilustración 21: Riesgos tecnologías de la información - R21

Riesgo: R22

No se renuevan contratos oportunamente con proveedores críticos.

Riesgo Inherente

(IC:	1	+	IR:	1	+	IO:	5	+	IL:	5	)		X	PR:	5	=	RIESGO:	60

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01	Se registra Orden de Compra 36783 del 28-03-2019 -Mesa de Ayuda	####	5	2	10
02	Se cuenta con contratro de soporte - Mesa de ayuda - hasta el 28 de febrero de 2020	0,0%	4	2	8
03					0
04					0
05					0
		100,0%		9,0	9,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

(IF:	1	+	IR:	1	+	IO:	5	+	IL:	5	)	12	X	PR:	1	=	RIESGO:	12

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		####			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					9

Ilustración 22: Riesgos tecnologías de la información - R22

Riesgo: **R23**

Procedimiento Gestión de Continuidad y Recuperación de los Servicios de Informática y Comunicaciones. Revisión continua de los protocolos DRP existentes.

Riesgo Inherente

(IC:	1	+	IR:	5	+	IO:	5	+	IL:	5	)		X	PR:	5	=	RIESGO:	80

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		####			0
02	No se cuenta con disponibilidad de servicios DRP para la plataforma del Ministerio de Minas y Energía.	0,0%			0
03	En el 2019 no se realizaron pruebas de continuidad por no disposición de servicios de DRP.				0
04					0
05					0
		#####		#¡DIV/0!	0,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		####			0
07		0,0%			0
08					0
09					0
10					0
		#####		#¡DIV/0!	0,0

Nivel de Exposición

(IF:	1	+	IR:	5	+	IO:	5	+	IL:	5	)	16	X	PR:	5	=	RIESGO:	80

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		####			0
02		0,0%			0
03					0
04					0
05					0

Ilustración 23: Riesgos tecnologías de la información - R23

4.4. TABLA DE RESUMEN DE RIESGOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN

N° Riesgo	Nombre del Riesgo
R1	Pérdida de Disponibilidad ante fallas en software debido a que no se renuevan algunos contratos de soporte críticos con fabricantes y/o fábricas de software.
R2	No se tienen penalidades a contratistas correlacionadas con incumplimientos, deficiencia de servicios, fallas o errores en los sistemas en producción y caídas de las plataformas tecnológicas.
R3	Falencias en Gobierno de TIC por no aplicar buenas practicas basadas en ITIL y una apropiada gestión de riesgos.
R4	No se tiene absoluto control de la plataforma crítica del MINENERGÍA debido a que un alto porcentaje de servicios de la administración de la plataforma esta TERCERIZADO.
R5	Software - No existe una metodología de desarrollo seguro usada en la entidad. Falta de metodología de desarrollo seguro.
R6	No se cuenta con los roles de Oficial de Seguridad de la Información y Oficial de Continuidad de Negocio que permitan ser preventivos en el tratamiento de riesgos de confidencialidad, integridad y disponibilidad.
R7	No existen apropiadas contramedidas para proteger las acciones de los empleados de contratistas y control sobre los equipos que estos utilizan dentro de las redes del MINENERGÍA.
R8	Software - Carencia de una metodología de pruebas al Software desarrollado. Falta de pruebas de carga, stress, abuso, entre otras.
R9	Software - Carencia de una metodología de pruebas al Software desarrollado. Fallas en el proceso de contratación. No se evidencia estructuración de niveles de acuerdo de servicio para asociarlos a penalizaciones.
R10	Falencias en el aseguramiento de redes. Ej. VLAN´s Inalámbricas y Asignación de VPN's
R11	Falencias en la revisión, monitoreo y registro a los Logs de seguridad y errores, eliminándolos sin control alguno.
R12	Personas - Los funcionarios del Ministerio no firman acuerdos de confidencialidad. No se evidencian cláusulas de confidencialidad aplicadas a los funcionarios, contratistas y proveedores.
R13	Indisponibilidad ante una falla prolongada de flujo de energía eléctrica y caída total de las UPS's que soportan en centro de cómputo.
R14	No se tiene una política ni procedimiento establecido, para la eliminación permanente de información y remoción de licencias de software en medios y equipos dados de baja. No se realiza eliminación segura en medios de almacenamiento.

N° Riesgo	Nombre del Riesgo
R15	Probabilidad de ingresos no autorizados a sistemas del MINENERGÍA por personal no autorizado. Carencia de una política de gestión de contraseñas. No se establece un periodo de cambio de contraseña.
R16	Falta de pruebas de contingencia. No se tiene un procedimiento establecido para la recuperación de caídas en dispositivos activos de red.
R17	Los usuarios que ingresan a la red inalámbrica no son autenticados contra el Directorio Activo. Falta de control con el ingreso de usuarios y visitantes a la red inalámbrica.
R18	No se tiene un estándar para el manejo de información confidencial. El MINENERGÍA carece de un procedimiento que controle la Información confidencial. No se utilizan herramientas tecnológicas para controles criptográficos.
R19	No se tiene una política establecida para la verificación de software creados dentro y fuera del MINENERGÍA. No se cuenta con protección de inyección de código.
R20	Falencias en el control de usuarios a áreas restringidas. No se posee control de acceso a áreas restringidas.
R21	Falencias en la clasificación de información. Desconocimiento de lo que es información confidencial.
R22	No se renuevan contratos oportunamente con proveedores críticos.
R23	Procedimiento Gestión de Continuidad y Recuperación de los Servicios de Informática y Comunicaciones. Revisión continua de los protocolos del Plan de Recuperación ante Desastres existentes.

Tabla 3: Tabla resumen de riesgos

4.5. MAPA DE CALOR DE RIESGOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN

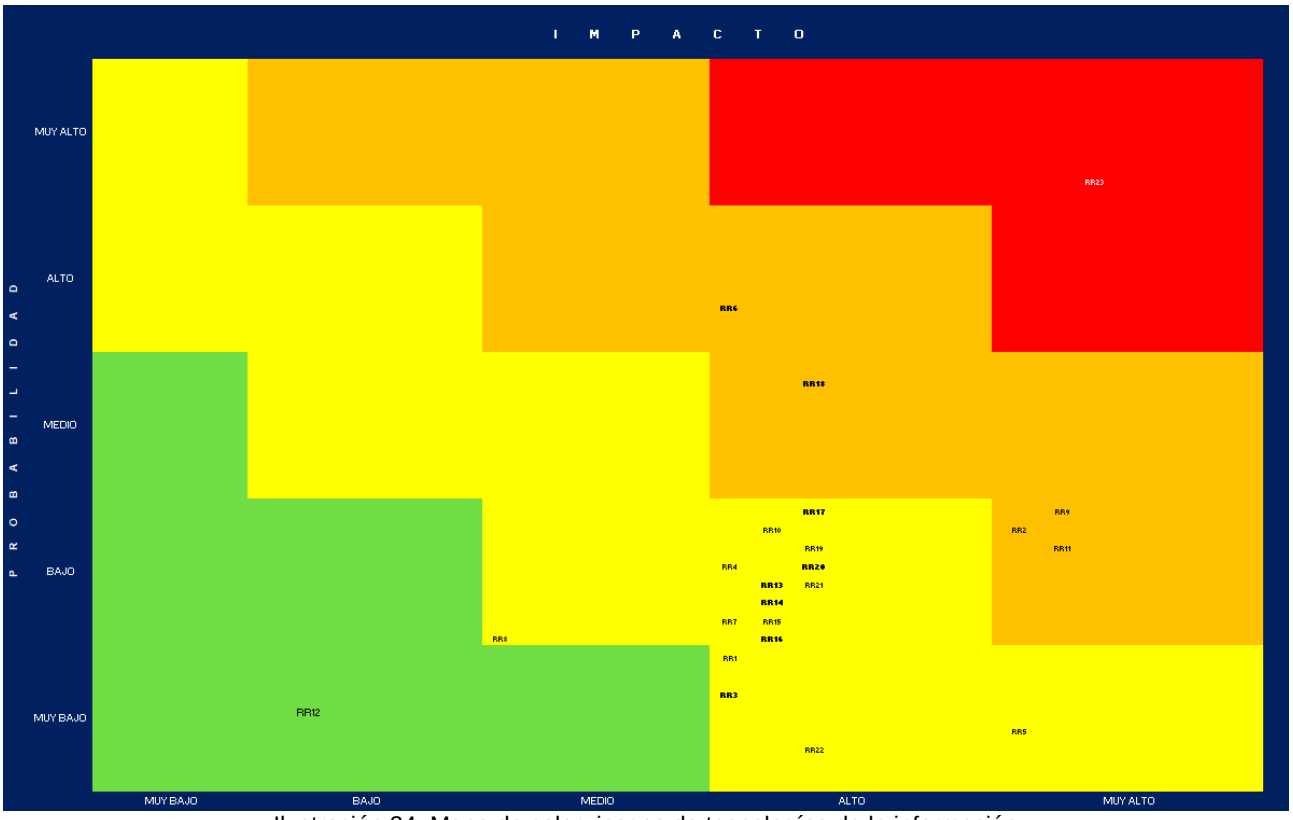

Ilustración 24: Mapa de calor riesgos de tecnologías de la información

Según mapa de calor en la zona roja o zona y con el esfuerzo hecho por el Grupo TIC (hoy Grupo de Infraestructura Tecnológica), solamente quedó el siguiente riesgo:

No. Riesgo	Nombre del riesgo
R23	Procedimiento Gestión de Continuidad y Recuperación de los Servicios de Informática y Comunicaciones. Revisión continua de los protocolos existentes del Plan de Recuperación ante Desastres.

Tabla 4: Zona roja o zona de riesgos inaceptables

4.6. DECLARACIÓN FUNDAMENTADA DE LOS RIESGOS RELACIONADOS CON PROCESOS MISIONALES Y DE APOYO

MAPA DE RIESGOS

Riesgo: **R1**

Riesgos de manipulacion de informacion por usuarios activos posterior a la finalizacion del contrato.

Causa: Talento Humano no es notificada oportunamente de las bajas de personal del MINMINAS o del personal de los contratistas.

Riesgo Inherente

(IC:	5	+	II:	1	+	IL:	3	+	IO:	2	)		X	PR:	3	=	RIESGO:	33

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exl) (1 10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exl) (1 10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0
		11			

Nivel de Exposición

(IF:	5	+	IR:	1	+	IO:	3	+	IL:	2	)	11	X	PR:	3	=	RIESGO:	33

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exl) (1 10)
01	Establecer Ciclo de Vida de Usuarios automatizado que involucre tanto personal del MINMINAS como personal de contratistas.	100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					0
	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exl) (1 10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0

Riesgo Residual

												100,0%		#¡DIV/0!	0,0	0		
												11			0			
(IF:	5	+	IR:	1	+	IO:	3	+	IL:	2	)	11	X	PR:	3	=	RIESGO:	33

Ilustración 25: Riesgos procesos misionales - R1

MAPA DE RIESGOS

Riesgo: **R2**

Ausencia de documento de autorizacion al personal interno y externo del Ministerio en el tratamiento de sus datos personales.

Riesgo Inherente

(IC:	5	+	IR:	2	+	IO:	1	+	IL:	5	)		X	PR:	4	=	RIESGO:	52

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

(IF:	5	+	IR:	2	+	IO:	1	+	IL:	5	)	13	X	PR:	4	=	RIESGO:	52

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01	Establecer campaña de firma de documento de autorizacion de tratamiento de datos personales a nivel interno y externo del MINMINAS.	100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					0
	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0

Riesgo Residual

												100,0%		#¡DIV/0!	0,0			
												13			0			
(IF:	5	+	IR:	2	+	IO:	1	+	IL:	5	)	13	X	PR:	4	=	RIESGO:	52

Ilustración 26: Riesgos procesos misionales - R2

MAPA DE RIESGOS

Riesgo: **R3**

Perdida de Informacion o modificacion de archivos contenidos en las carpetas compartidas de las unidades institucionales O y X.

Riesgo Inherente

(IC:	2	+	IR:	2	+	IO:	5	+	IL:	4	)		X	PR:	5	=	RIESGO:	65

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

											13							
(IF:	2	+	IR:	2	+	IO:	5	+	IL:	4	)	13	X	PR:	5	=	RIESGO:	65

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01	Establecer campañas de clasificacion de informacion y definir propietarios sobre las carpetas compartidas.	100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0
					0

Riesgo Residual

											13							
(IF:	2	+	IR:	2	+	IO:	5	+	IL:	4	)	13	X	PR:	5	=	RIESGO:	65

Ilustración 27: Riesgos procesos misionales - R3

MAPA DE RIESGOS

Riesgo: **R4**

Indisponibilidad de las carpetas compartidas institucionales.

Riesgo Inherente

(IC:	2	+	IR:	1	+	IO:	4	+	IL:	1	)		X	PR:	4	=	RIESGO:	32

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

(IF:	2	+	IR:	1	+	IO:	4	+	IL:	1	)	8	X	PR:	4	=	RIESGO:	32

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0

Riesgo Residual

												100,0%		#¡DIV/0!	0,0		
												8			0		
(IF:	2	+	IR:	1	+	IO:	4	+	IL:	1	)	8	X	PR:	4	=	RIESGO:	32

Ilustración 28: Riesgos procesos misionales - R4

MAPA DE RIESGOS

Riesgo: **R5**

Perdida de oportunidad, credibilidad y seguridad de la informacion por expedientes no correlacionados en P8, imágenes no legibles y/o perdida de expedientes en P8.

Riesgo Inherente

(IC:	4	+	IR:	4	+	IO:	4	+	IL:	4	)		X	PR:	5	=	RIESGO:	80

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exl) (1 10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exl) (1 10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

											16							
(IF:	4	+	IR:	4	+	IO:	4	+	IL:	4	)	16	X	PR:	5	=	RIESGO:	80

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exl) (1 10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					0
	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exl) (1 10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0

Riesgo Residual

											100,0%			#¡DIV/0!	0,0			
											16				0			
(IF:	4	+	IR:	4	+	IO:	4	+	IL:	4	)	16	X	PR:	5	=	RIESGO:	80

Ilustración 29: Riesgos procesos misionales - R5

MAPA DE RIESGOS

Riesgo: **R6**

Indisponibilidad del sistema de informacion P8.

Riesgo Inherente

(IC:	3	+	IR:	4	+	IO:	4	+	IL:	3	)		X	PR:	4	=	RIESGO:	56

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

(IF:	3	+	IR:	4	+	IO:	4	+	IL:	3	)	14	X	PR:	4	=	RIESGO:	56

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0

Riesgo Residual

											100,0%			#¡DIV/0!	0,0	0		
											14				0			
(IF:	3	+	IR:	4	+	IO:	4	+	IL:	3	)	14	X	PR:	4	=	RIESGO:	56

Ilustración 30: Riesgos procesos misionales - R6

MAPA DE RIESGOS

Riesgo: **R7**

Vulneracion de la reserva legal de la informacion de los expedientes disciplinarios (expediente fisico, sistemas P8, correos electronicos).

Riesgo Inherente

(IC:	4	+	IR:	4	+	IO:	3	+	IL:	3	)		X	PR:	4	=	RIESGO:	56

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
01	Se cuenta con oficina cerrada y con acceso controlado.	100,0%	3	2	6
02	El sistema P8 maneja control de acceso a la informacion.	0,0%	3	2	6
03					0
04					0
05					0
		100,0%		#¡DIV/0!	6,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

(IF:	4	+	IR:	4	+	IO:	3	+	IL:	3	)	14	X	PR:	3	=	RIESGO:	42

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Riesgo Residual

(IF:	4	+	IR:	4	+	IO:	3	+	IL:	3	)	14	X	PR:	3	=	RIESGO:	42

Ilustración 31: Riesgos procesos misionales - R7

MAPA DE RIESGOS

Riesgo: **R8**

Perdida de informacion por fallas de flujo electrico.

Riesgo Inherente

(IC:	1	+	IR:	5	+	IO:	5	+	IL:	1	)		X	PR:	4	=	RIESGO:	48

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
01	Se cuenta con UPS que soporta los computadores de todo el edificio del MINMINAS.	100,0%	4	2	8
02		0,0%			0
03					0
04					0
05					0
		100,0%		8,0	8,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

	12																	
(IF:	1	+	IR:	5	+	IO:	5	+	IL:	1	)	12	X	PR:	2	=	RIESGO:	24

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					8

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0

Riesgo Residual

												100,0%		#¡DIV/0!	0,0			
												12			0			
(IF:	1	+	IR:	5	+	IO:	5	+	IL:	1	)	12	X	PR:	2	=	RIESGO:	24

Ilustración 32: Riesgos procesos misionales - R8

MAPA DE RIESGOS

Riesgo: **R9**

Indisponibilidad de informacion por desconexion de la carpeta institucional.

Riesgo Inherente

(IC:	2	+	IR:	2	+	IO:	4	+	IL:	4	)		X	PR:	4	=	RIESGO:	48

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

(IF:	2	+	IR:	2	+	IO:	4	+	IL:	4	)	12	X	PR:	4	=	RIESGO:	48

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exi) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0

Riesgo Residual

										100,0%			#¡DIV/0!	0,0			
										12				0				
(IF:	2	+	IR:	2	+	IO:	4	+	IL:	4	)	12	X	PR:	4	=	RIESGO:	48

Ilustración 33: Riesgos procesos misionales - R9

MAPA DE RIESGOS

Riesgo: **R10**

Perdida de informacion debido a que cada año se cancelan los perfiles de los usuarios contratistas. Quedando inaccesible la informacion de la unidad C, entre estos los archivos o carpetas que se tengan en el escritorio del usuario.

Riesgo Inherente

(IF:	4	+	IR:	4	+	IO:	4	+	IL:	2	)		X	PR:	4	=	RIESGO:	56

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

												14						
(IF:	4	+	IR:	4	+	IO:	4	+	IL:	2	)	14	X	PR:	4	=	RIESGO:	56

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					0
	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1 5)	IMPLEMENTACION (0 2)	SOLIDEZ (Exi) (1 10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0

Riesgo Residual

												100,0%		#¡DIV/0!	0,0	0		
												14			0			
(IF:	4	+	IR:	4	+	IO:	4	+	IL:	2	)	14	X	PR:	4	=	RIESGO:	56

Ilustración 34: Riesgos procesos misionales - R10

MAPA DE RIESGOS

Riesgo: **R11**

Perdida de informacion por almacenamiento local en discos duros de equipo por insuficiente espacio para almacenar en la carpeta compartida X. Existen proyectos como PENUD (PROGRAMA ESPECIAL DE NACIONES UNIDAS PARA EL DESARROLLO), el cual ocupa mas de la cuota asignada que son 70GB. Ante esto los usuarios guardan sus proyecto en la particion D del disco duro local, pero esta no es respaldada o no se hacen backups. El tamaño de esta informacion se da por archivos cartograficos de Argis.

Riesgo Inherente

(IC:	4	+	IR:	4	+	IO:	4	+	IL:	2	)		X	PR:	5	=	RIESGO:	70

Controles Existentes

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0
		100,0%		#¡DIV/0!	0,0

Nivel de Exposición

												14						
(IF:	4	+	IR:	4	+	IO:	4	+	IL:	2	)	14	X	PR:	5	=	RIESGO:	70

Controles Recomendados

	CONTROLES PREVENTIVOS (REDUCEN PROBABILIDAD)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
01		100,0%			0
02		0,0%			0
03					0
04					0
05					0
		100,0%		#¡DIV/0!	0,0
					0

	CONTROLES CORRECTIVOS (REDUCEN IMPACTOS)	PESO	EFECTIVIDAD (1-5)	IMPLEMENTACION (0-2)	SOLIDEZ (Exl) (1-10)
06		100,0%			0
07		0,0%			0
08					0
09					0
10					0

Riesgo Residual

												100,0%		#¡DIV/0!	0,0			
												14			0			
(IF:	4	+	IR:	4	+	IO:	4	+	IL:	2	)	14	X	PR:	5	=	RIESGO:	70

Ilustración 35: Riesgos procesos misionales - R11

4.7. TABLA DE RESUMEN DE RIESGOS RELACIONADOS CON PROCESOS MISIONALES Y DE APOYO

No. Riesgo	Nombre del riesgo
R1	Riesgos de manipulación de información por usuarios activos posterior a la finalización del contrato.
R2	Ausencia de documento de autorización al personal interno y externo del Ministerio en el tratamiento de sus datos personales.
R3	Pérdida de Información o modificación de archivos contenidos en las carpetas compartidas de las unidades institucionales O y X.
R4	Indisponibilidad de las carpetas compartidas institucionales.
R5	Pérdida de oportunidad, credibilidad y seguridad de la información por expedientes no correlacionados en P8, imágenes no legibles y/o perdida de expedientes en P8.
R6	Indisponibilidad del sistema de información P8.
R7	Vulneración de la reserva legal de la información de los expedientes disciplinarios (expediente físico, sistemas P8, correos electrónicos).
R8	Pérdida de información por fallas de flujo eléctrico.
R9	Indisponibilidad de información por desconexión de la carpeta institucional.
R10	Pérdida de información debido a que cada año se cancelan los perfiles de los usuarios contratistas. Quedando inaccesible la información de la unidad C:\, entre estos los archivos o carpetas que se tengan en el escritorio del usuario.
R11	Pérdida de información por almacenamiento local en discos duros de equipo por insuficiente espacio para almacenar en la carpeta compartida X.

Tabla 5: Resumen riesgos procesos misionales

4.8. MAPA DE CALOR DE RIESGOS DE PROCESOS MISIONALES Y DE APOYO

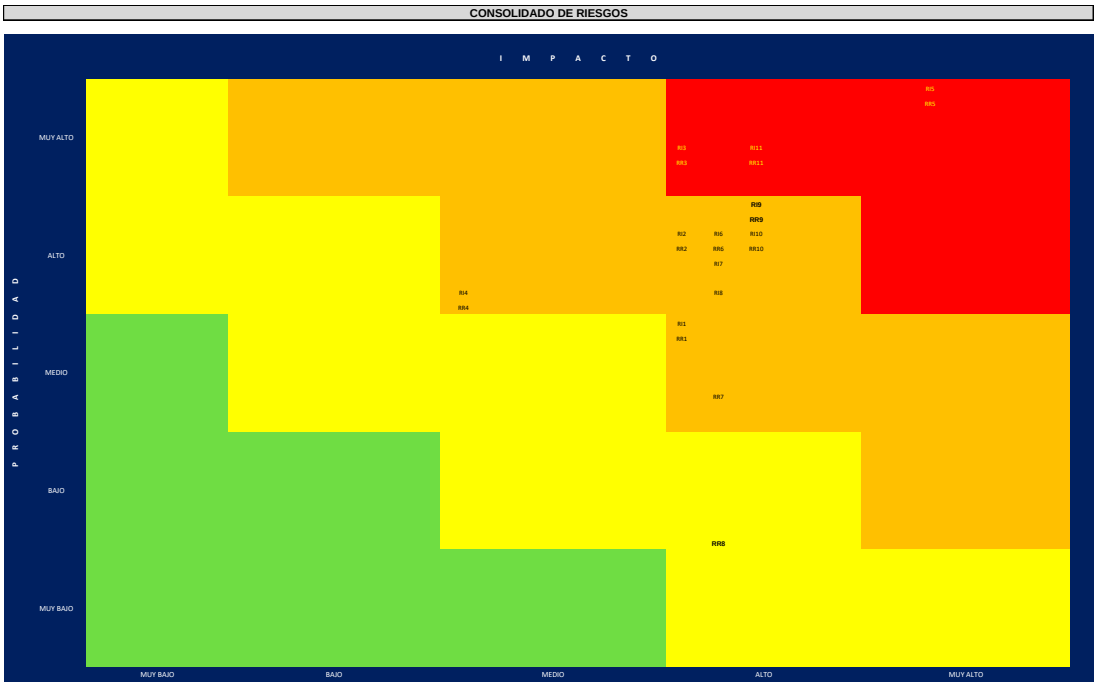

Ilustración 36: Mapa de calor riesgos procesos misionales

Según mapa de calor en la zona roja o zona de riesgos inaceptables quedan los siguientes riesgos que se recomienda tratar a corto plazo.

No. Riesgo	Nombre del riesgo
R3	Pérdida de Información o modificación de archivos contenidos en las carpetas compartidas de las unidades institucionales O:\ y X:\
R5	Pérdida de oportunidad, credibilidad y seguridad de la información por expedientes no correlacionados en P8, imágenes no legibles y/o perdida de expedientes en P8.
R11	Pérdida de información por almacenamiento local en discos duros de equipo por insuficiente espacio para almacenar en la carpeta compartida X.

Tabla 6: zona roja o zona de riesgos inaceptables

5. CONCLUSIONES

5.1. Es esencial que en el Ministerio se implementen soluciones de TI que puedan responder de manera preventiva y proactiva a las amenazas cibernéticas reales y percibidas a través de una eficiente estrategia de gestión de riesgos.

5.2. Para los procesos misionales se debe establecer una cultura de gestión de riesgos en donde se analicen las actividades críticas y responsables, con el objeto de entregar los resultados esperados.

5.3. Durante las valoraciones trimestrales realizadas en el año 2019, se puede percibir que el Grupo de Infraestructura Tecnológica (antes Grupo TIC), llevó a cabo tareas de mitigación, aplicando los controles que permitieron que los riesgos de la zona crítica, bajaran a zonas moderadas o leves, mejorando el mapa de calor de los mismos y contrarrestando de la mejor manera su posible materialización.

5.4. Otros riesgos no se pudieron gestionar de la misma forma, debido a que no se contó con los recursos, la disposición, y/o simplemente no estuvieron contemplados dentro de la lista de prioridades de la gestión autorizadas y permitida en el Grupo de Infraestructura Tecnológica (antes Grupo TIC).

5.5. El Grupo de Infraestructura Tecnológica (antes Grupo TIC), realiza la administración, seguimiento, control, con el objeto de mitigarlos de la mejor manera y evitar su posible materialización.

6. RECOMENDACIONES

6.1. Se recomienda la mejora continua en la gestión del riesgo a través del análisis de procesos y estructura organizacional de la entidad.

6.2. La gestión mejorada del riesgo incluye el análisis, actualización y/o identificación de nuevos riesgos, el establecimiento de los controles y las tareas para el tratamiento del riesgo, el monitoreo y la comunicación efectiva frente a todo lo anterior.

7. MEJORES PRÁCTICAS

La gestión del riesgo se considera parte central de los procesos de gestión en el MINENERGÍA. La estructura y los procesos de gobierno se basan en la gestión del riesgo. La gestión eficaz del riesgo es considerada por la Alta Dirección, como un factor esencial para el logro de los objetivos misionales, funcionales y de operación.

La gestión, administración, seguimiento y empoderamiento del riesgo, se ha convertido en una premisa dentro de las labores normales de los funcionarios, servidores públicos, contratistas, terceros asociados, colaboradores y en general cualquier tipo de usuario final que interactúe, trabaje, comparta, distribuya información institucional en el MINENERGÍA, haciendo parte de la cultura organizacional.