UNIVERSIDAD DE CUNDINAMARCA

MANUAL PARA EL TRATAMIENTO DE LOS RIESGOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

FUSAGASUGÁ
2019

UNIVERSIDAD DE CUNDINAMARCA

MANUAL PARA EL TRATAMIENTO DE LOS RIESGOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

Elaborado por: DIRECCIÓN DE SISTEMAS Y TECNOLOGÍA

FUSAGASUGÁ

2019

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVO GENERAL 4
3. OBJETIVOS ESPECÍFICOS 4
4. ALCANCE 5
5. DEFINICIONES 5
6. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO **¡Error! Marcador no definido.**
7. IDENTIFICACIÓN DE RIESGOS 6
   - 7.1 RIESGOS 6
   - 7.2 VULNERABILIDADES Y AMENAZAS 9
   - 7.2.1 AMENAZAS 9
   - 7.2.2 VULNERABILIDADES 10
8. ANÁLISIS Y EVALUACIÓN DEL RIESGO 15
   - 8.1 RIESGO ANTES Y DESPUES DE LOS CONTROLES 15
   - 8.2 TIPO DE IMPACTO 15
9. VALORACIÓN DEL RIESGO 16
   - 9.1 CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 16
   - 9.2 VALORACIÓN DE CONTROLES PARA TRATAMIENTO DE RIESGOS . 16
10. BIBLIOGRAFÍA Y WEBGRAFÍA 17

1. INTRODUCCIÓN

Este documento forma parte de las políticas y lineamientos establecidos dentro del Sistema de Gestión de Seguridad de la Información adoptado por la Universidad de Cundinamarca el 17 de mayo de 2017 en la Resolución 088 “Por la cual se adopta el Sistema de Gestión de la Seguridad de la Información – SGSI, y se establece la política, objetivos y alcance del Sistema de Seguridad de la Información de la Universidad de Cundinamarca”.

El presente manual busca establece una Política de Administración del Riesgo que determine los lineamientos a seguir en cuanto a riesgos, vulnerabilidades, amenazas y controles en Seguridad de la Información necesarios para cada Activo de la Información reportado y aprobado anualmente por la totalidad de funcionarios administrativos y docentes a tiempo completo y que además cuente con criticidad alta o media dentro de la institución.

2. OBJETIVO GENERAL

Implementar y divulgar una Política de Administración del Riesgo que, dentro del alcance del Sistema de Gestión de Seguridad de la Información, permita determinar riesgos, vulnerabilidades y amenazas de los Activos de la Información de la Universidad de Cundinamarca.

2.1 OBJETIVOS ESPECÍFICOS

- Identificar los riesgos asociados a cada tipo de Activo de la Información, así como sus respectivas causas y consecuencias dentro de los procesos que posee la institución.

- Identificar cada una de las vulnerabilidades y amenazas asociadas a las mismas presentes en cada proceso de la institución y que afecten

directamente la integridad, confidencialidad y disponibilidad de los activos de la información.

- Generar la matriz de riesgo para cada proceso (Estratégico, Misional, Apoyo y Seguimiento) donde se evidencie la identificación de activos de la información, así como al identificación, análisis y valoración de los riesgos asociados a los activos reportados por cada una de las áreas y oficinas.

3. ALCANCE

El alcance del presente manual y sus políticas, está destinado para todos los procesos Estratégicos, Misionales, de Apoyo y de Seguimiento en el que se, manipulen, resguarden, generen o almacenen Activos de la Información y que estén dentro de los parámetros establecidos por el Sistema de Gestión de Seguridad de la Información.

4. DEFINICIONES

Activo de la información: Todo aquel elemento o dispositivo que produce, almacena o ayuda a generar información de gran impacto para la organización y que por lo tanto de protegerse.
Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.[1]
Hardware (HW): Dispositivos de almacenamiento o equipos de cómputo que permitan generar, almacenan o contener información de la institución.
Información (IN): Conjunto de formatos y registros suministrados por el Sistema de Gestión de la Calidad, así como los diferentes formatos de autoría propia de cada área o proceso y los suministrados por entidades u organismos externos para el almacenamiento, gestión y reporte de información.
Otros (OT): Dispositivos electrónicos, documentos, llaves o tarjetas de acceso, o cualquier otro elemento que permita generar o almacenar información y que no se encuentre categorizada como hardware, software, talento humano o información.
Riesgo: El riesgo es el efecto de la incertidumbre sobre los objetivos.[2]
Software (SW): Conjunto de programas de cómputo utilitarios que permiten desempeñar funciones administrativas y de docencia.

[1] Ministerio de Tecnologías de la Información y las Comunicaciones
[2] Ministerio de Tecnologías de la Información y las Comunicaciones

Talento Humano (TH): Funcionarios administrativos de planta, termino fijo y OPS, docentes hora cátedra y tiempo completo que laboran en la institución.
Vulnerabilidades: Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.[3]

5. IDENTIFICACIÓN DE RIESGOS

A continuación, se dan a conocer los riesgos (causas y consecuencias), vulnerabilidades y amenazas con su respectivo indicador; los que serán utilizados en el desarrollo de las matrices de riesgo de cada proceso con que cuenta la institución.

5.1 RIESGOS

En la siguiente tabla se muestra el identificador y descripción asignado a cada riesgo evidenciado durante la elaboración de las matrices de riesgo, así como la identificación de las causas y consecuencias del mismo, las que se explicaran posteriormente.

IDENTIFICADOR	RIESGO	ID- CAUSA	ID-CONSECUENCIA
R1	Indisponibilidad del Hardware	C1 C2 C3 C4	Q1
R2	Mal funcionamiento del software	C5 C6 C7	Q2
R3	Que pierda su confidencialidad	C8 C9	Q3 Q4
R4	Que no sea integra	C10 C11 C12	Q5 Q6
R5	Que no esté disponible	C13 C14 C15 C16	Q7 Q8

[3] Ministerio de Tecnologías de la Información y las Comunicaciones

R6	Deficiencias en el desempeño laboral	C17 C18 C19 C20	C9 C10
R7	Deficiencias en la legalización de contratos	C21 C22 C23	C9 C11
R8	Incumplimiento en el programa de salud ocupacional	C24 C25 C26	Q11 Q12 Q13
R9	Deterioro del ambiente laboral	C27	Q14
R10	Capacitación inadecuada en el SGSI	C28	Q7 Q9 Q11 Q12

5.1.1 CAUSAS

IDENTIFICADOR	CAUSA
C1	Obsolescencia tecnológica
C2	Falta de espacio por alto consumo de recursos
C3	Puertos abiertos y servicios asociados que pueden causar la caída o falla de hardware
C4	Ausencia de Mantenimiento
C5	Saturación del sistema de información
C6	Copia fraudulenta del software
C7	Uso de software falso o copiado
C8	Acceso a usuarios no autorizados
C9	Que no esté almacenada debidamente
C10	Manipulación indebida
C11	Pérdida de información importante sin posibilidad de recuperarla
C12	Correo SPAM

C13	Fuga de información para fines diferentes al propósito inicial
C14	Ausencia de copias de respaldo
C15	Asignación errada de los derechos de acceso
C16	Ausencia de auditorías regulares
C17	Falta de socialización de las herramientas estratégicas y misionales de la institución
C18	Falta de mecanismos para evaluar el desempeños de los servidores de la institución.
C19	falta de compromiso en la aprobación de reglamentación a la evolución de desempeño
C20	Falta de incentivos por parte de los directivos para con los funcionarios de la universidad.
C21	Tardía presentación de la documentación para posesión o legalización.
C22	Omisión de documentos necesarios para legalización del contrato.
C23	Inadecuada disposición en los archivos de los contratos.
C24	Ausencia de un diagnostico real
C25	No aplicación de la normativa vigente
C26	Dificultades en la disponibilidad de recursos
C27	Inexistencia de un instrumento para medición del ambiente laboral.
C28	Deficiente evaluación del perfil de competencias y habilidades para el ejercicio del cargo asignado

5.1.2 CONSECUENCIAS

IDENTIFICADOR	CONSECUENCIAS
Q1	Pérdida de la continuidad del negocio, servicios afectados para los usuarios

	internos y externos. Afectación a toda la entidad
Q2	Corrupción de los datos
Q3	Toma de decisión sobre datos irreales
Q4	Desvío de información
Q5	Toma de decisión errada o parcial
Q6	Perdida de información
Q7	Retraso en procesos
Q8	Incumplimiento a la normatividad legal vigente
Q9	Deficiencia en los procesos
Q10	Baja calidad de los productos y servicios
Q11	Exposición a sanciones legales por parte de entes de control.
Q12	Deficiencia en la calidad de vida laboral
Q13	Aumento en índices de accidentes y enfermedades laborales y profesionales
Q14	Deficiencia en la calidad de vida laboral

5.2 VULNERABILIDADES Y AMENAZAS

5.2.1 AMENAZAS

IDENTIFICADOR	AMENAZA
A1	Incumplimiento en el mantenimiento correctivo y/o preventivo
A2	Hurto a medios o documentos
A3	Incumplimiento de la ley 1672 de 2013
A4	Daños físicos que puede causar pérdida de información
A5	Pérdida del suministro de energía
A6	Abuso de los derechos
A7	Corrupción de datos
A8	Error de uso
A9	Falsificación de derechos

A10	Procesamiento ilegal de datos
A11	Mal funcionamiento del software
A12	Manipulación con software
A13	Uso no autorizado del equipo
A14	Espionaje remoto
A15	Uso de software falsificado o copiado
A16	Incumplimiento en la disponibilidad del personal
A17	Destrucción de equipos y medios
A18	Negación de acciones.
A19	Hurto de equipos

5.2.2 VULNERABILIDADES

TIPO DE ACTIVO	IDENTIFICADOR	VULNERABILIDAD	AMENAZAS
HW	V1	Mantenimiento insuficiente y/o fuera de la planeación	A1
	V2	Falta de programa para disposición final de RAEE's	A2 A3
	V3	Daños ocasionados por humedad, polvo o suciedad	A4
	V4	Susceptibilidad a las variaciones de voltaje	A5
	V5	Almacenamiento sin protección	A2
	V6	Falta de cuidado en la disposición final	A2
	V7	Copia no controlada	A2
	V8	Ausencia o insuficiencia de pruebas de software	A6

SW	V9	Defectos bien conocidos en el software	A6
	V10	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	A6
	V11	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	A6
	V12	Ausencias de pistas de auditoria	A6
	V13	Asignación errada de los derechos de acceso	A6
	V14	En términos de tiempo utilización de los datos errados en los programas de aplicación	A7
	V15	Interfaz de usuario compleja	A7
	V16	Ausencia de documentación	A8
	V17	Configuración incorrecta de parámetros	A8
	V18	Fechas incorrectas	A8
	V19	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario	A9

	V20	Tablas de contraseñas sin protección	A9
	V21	Gestión deficiente de las contraseñas	A9
	V22	Habilitación de servicios innecesarios	A10
	V23	Software nuevo o inmaduro	A11
	V24	Especificaciones incompletas o no claras para los desarrolladores	A11
	V25	Ausencia de control de cambios eficaz	A11
	V26	Descarga y uso no controlado de software	A12
	V27	Ausencia de copias de respaldo	A12
	V28	Ausencia de protección física de la edificación, puertas y ventanas	A2
	V29	Fallas en la producción de informes de gestión	A13
SE	V30	Ausencia en un eficiente control de cambio en la accesibilidad de los servicios	A8
	V31	Asignación errada al acceso de servicios.	A6
	V32	Líneas de comunicación y navegación sin protección	A14
	V33	Arquitectura insegura de red.	A14

	V34	Acceso a servicios en conexión de red pública sin protección	A13
	V35	Ausencia de políticas sobre el uso del correo electrónico	A8
IN	V36	Ausencia de procedimientos para el manejo de información clasificada	A8
	V37	Ausencia de autorización de los recursos de procesamiento de información	A2
	V38	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	A15
	V39	Ausencia del personal	A16
	V40	Procedimientos inadecuados de contratación	A17
	V41	Entrenamiento insuficiente en seguridad	A8
	V42	Uso incorrecto de software y hardware	A8
	V43	Falta de conciencia acerca de la seguridad	A8
	V44	Ausencia de mecanismos de monitoreo	A10
	V45	Trabajo no supervisado del	A2

TH		personal externo o de limpieza	
	V46	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	A13
	V47	Ausencia de procedimiento formal para el registro y retiro de usuarios	A6
	V48	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	A18
	V49	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	A8
	V50	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	A19
	V51	Ausencia de revisiones regulares por parte de la gerencia	A13
	V52	Ausencia de procedimientos para la presentación de informes sobre las	A13

		debilidades en la seguridad	
OT	V53	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	A2 A7 A19

6. ANÁLISIS Y EVALUACIÓN DEL RIESGO

6.1 RIESGO ANTES Y DESPUÉS DE LOS CONTROLES

La guía de Riesgos del DAFP, presenta mediante la Matriz de Calificación, Evaluación y Respuesta a los riegos, la manera de generar una comparación cualitativa de la probabilidad de ocurrencia de un riesgo asociado a un activo, versus el impacto que puede llegar a tener el incidente, además de identificar zonas de riesgo y el posible tratamiento que pueden tener. En la siguiente tabla se muestran los diferentes resultados al generar la comparación mencionada anteriormente.

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

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía No. 7 de Gestión del Riesgo. MinTIC.

6.2 TIPO DE IMPACTO

Para determinar el tipo de impacto que ocasionaría cada uno de los riesgos identificados para cada Activo de la Información (Hardware, Software, Información, Talento Humano y Otros), se utilizaron los criterios de impacto propuestos por el MinTIC en su Guía de Gestión del Riesgo (Guía No. 7), especificando el grado de daño y las pérdidas financieras que puede ocasionar la ocurrencia de un evento de Seguridad de la Información. Los siguientes son los tipos de impactos utilizados en el desarrollo de las respectivas matrices de riesgo.

- Brechas en la seguridad de la información (Perdida de confidencialidad, integridad y disponibilidad de la información).
- Operaciones deterioradas.
- Pérdida del negocio y del valor financiero.
- Alteración de planes y fechas límites.
- Daños para la reputación.
- Incumplimiento de los requisitos legales.

7. VALORACIÓN DEL RIESGO

7.1 CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La información es un recurso que, como el resto de los activos, tiene valor para el organismo y por consiguiente debe ser debidamente protegida. Las políticas de seguridad y privacidad de la información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de las entidades del Estado.[4]

A continuación, se dan a conocer los Controles propuestos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en la Guía 8 del Modelo de Seguridad y Privacidad de la Información, para ser utilizado en el desarrollo de las actividades concernientes a la fase de Planificación y la fase de Implementación.

7.2 VALORACIÓN DE CONTROLES PARA TRATAMIENTO DE RIESGOS

[4] Guía No. 8. Controles de Seguridad y Privacidad de la Información. MinTIC.

En ésta etapa del proceso se evalúan los controles existentes en la institución, estableciendo parámetros, criterios y puntajes utilizando las herramientas propuestas por la Guía de Riesgos del DAFP y que a su vez hacen parte de la Guía de Gestión del Riesgo (No.7) a fin de hacer una cuantificación del análisis de los controles elegidos.

PARÁMETROS	CRITERIOS	TIPO DE CONTROL		PUNTAJES
		Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer el control.			15
	Existen manuales, instructivos o procedimientos para el manejo de la herramienta			15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.			30
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.			15
	La frecuencia de ejecución del control y seguimiento es adecuada.			25
	TOTAL			100

RANGOS DE CALIFICACIÓN DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO DESPLAZA EN LA MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS	
	CUADRANTES A DISMINUIR EN LA PROBABILIDAD	CUADRANTES A DISMINUIR EN EL IMPACTO
Entre 0-50	0	0
Entre 51-75	1	1
Entre 76-100	2	2

Fuente: Guía No. 7 de Gestión del Riesgo. MinTIC

8. BIBLIOGRAFÍA Y WEBGRAFÍA

Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 4. Dirección de Gestión y Desempeño Institucional. Departamento Administrativo de la Función Pública.

Ministerio de Tecnologías de la Información y las Comunicaciones www.mintic.gov.co

Guía de Gestión de Riesgos. Guía No.7 Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA DE APROBACIÓN**			**DESCRIPCIÓN DEL CAMBIO**
	AAAA	**MM**	**DD**	
1	2018	12	13	Elaboración del documento
2	2019	03	04	Ajuste en la nomenclatura de la tabla denominada “Vulnerabilidades”

ELABORÓ	
NOMBRES Y APELLIDOS	**CARGO**
Angélica María Molina Olaya	Técnico

REVISÓ	
NOMBRES Y APELLIDOS	**CARGO**
María del Pilar Delgado Rodríguez	Profesional Universitario I
Jorge Alfredo Mayorga Cárdenas	Profesional Director de Área
Paola Andrea Ramírez Suaza	Profesional Director de Área

APROBÓ (GESTOR RESPONSABLE DEL PROCESO)				
NOMBRES Y APELLIDOS	**CARGO**	**FECHA**		
		AAAA	**MM**	**DD**
Edilson Martínez Clavijo	Director Sistemas y Tecnología	2019	03	04