PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Oficina de Sistemas e Informática

Escuela Superior de Administración Pública

2020

TABLA DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

CONTROL DE CAMBIOS

NOMBRE	VERSIÓN	AUTOR	FECHA
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA ESCUELA DE ADMINISTRACIÓN PÚBLICA - ESAP	1.0	Oficina de Sistemas e Informática - OSI	JUNIO DE 2020

COMITÉ	ACTA DE APROBACIÓN	FECHA
Comité Institucional de Gestión y Desempeño	No.5	**1 de Julio de2020**

1 INTRODUCCION

Si en un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, las consecuencias derivadas de sucesos posteriores y relevantes como el terrorismo, la inestabilidad política, las pandemias y los códigos maliciosos, entre otros, han señalado la necesidad de incorporar nuevas amenazas presentes no solamente en el mundo físico sino también en el entorno digital, cuando se trate de comprender los riesgos más significativos a los activos de información. El análisis de riesgos de los activos de información nos permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis.

Gestionar eficazmente la seguridad de la información y riesgos de seguridad digital de los sistemas de información de la entidad, así como en los activos que participan en sus procesos y que se encuentran expuestos, permite garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de Seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del Sistema de Gestión de Seguridad de la Información y en concordancia a la normativa aplicable.

El plan de tratamiento de riesgos de seguridad, se encuentra alineado con el Plan Decenal de Desarrollo Institucional 2010-2020, dentro del escenario estratégico de Desarrollo Institucional, en la línea de acción Gestión de la Información, cuyo objetivo es disponer de la información apropiada para el desarrollo de las funciones de la ESAP, a través de la estrategia No.1 la cual busca gestionar información confiable, integra y oportuna para el desarrollo de las funciones y actividades de la ESAP.

Así mismo, este plan apoya la implementación de controles y acciones tendientes a la mitigación de los riesgos del proceso de gestión tecnológica, hallazgos de auditorias internas y apoya el cumplimiento del Modelo integrado de planeación y gestión del MINTIC, dentro de su política de gobierno Digital.

El seguimiento al plan de tratamiento de riesgos, se realizará de acuerdo con la GUIA PARA LA ADMINISTRACIÓN DE RIESGO DC-S-GC-06, ESAP, V2, diciembre 2019 y se integrará con los riesgos de seguridad digital y de la información.

2 OBJETIVOS

2.1 Objetivo general

Presentar el Plan de Tratamiento para los riesgos de seguridad de la información, identificados en los procesos incluidos en el alcance del SGSI de la Escuela Superior de Administración Pública, en adelante ESAP.

2.2 Objetivos Específicos

- Identificar los riesgos asociados a los procesos y los activos de información que hacen parte del alcance del SGSI
- Calcular el nivel de riesgo
- Establecer el plan de tratamiento de riesgos
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos

3 MARCO NORMATIVO

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales

NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices.
Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

4 DEFINICIONES

- **Activo**: cualquier elemento que tenga valor para la organización.
- **Análisis del riesgo**: Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- **Causa**: Elemento específico que origina el evento.
- **Contexto externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- **Contexto interno**[1]: Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- **Controles**: Procesos, políticas y/o actividades que pueden modificar el riesgo.
- **Criterios de riesgos**[2]: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- **Evaluación del Riesgo**: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
- **Evento**: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- **Fuente**: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.
- **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Identificación del riesgo**[3]: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.

[1] ISO 31000:2011
[2] Ibid.
[3] ISO 31000:2011

- **Riesgo aceptable**: Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.
- **Riesgo residual**: Nivel de riesgo que permanece luego de tomar medidas de tratamiento.
- **Riesgo**: Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de sus objetivos.
- **Riesgo de seguridad digital**: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

5 DESARROLLO DEL PLAN

5.1 IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto la ESAP. Es recomendable contar con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla. El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la Guía para la administración del riesgo y el diseño de controles en entidades públicas V4, emitida por el Departamento Administrativo de la Función Pública.

Ilustración 1. Estructura general de la metodología de riesgos

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

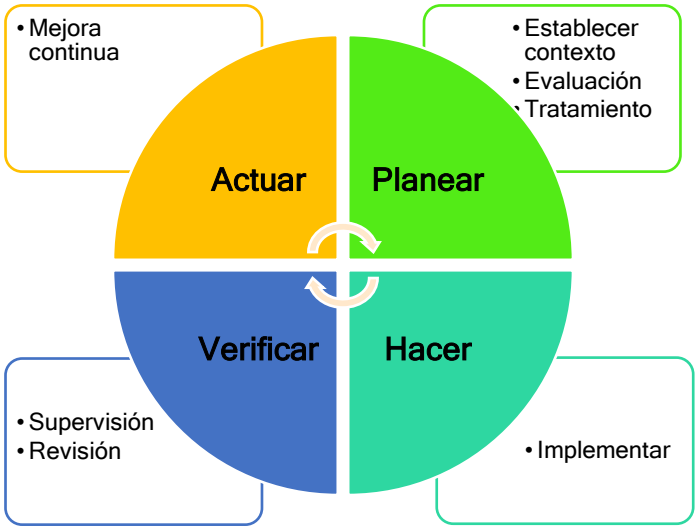

Ilustración 2. Ciclo PHVA y la gestión de riesgos

El proceso de identificación y evaluación de los riesgos de seguridad de la información está compuesto por los siguientes Hitos o actividades:

5.1.1 Programación y Agendamiento de Entrevistas

En esta fase se seleccionan los procesos incluidos en el alcance del SGSI de la ESAP y se procede a programar y a agendar a los líderes de las dependencias y grupos internos de trabajo que conforman los procesos, para la identificación de riesgos.

5.1.2 Entrevista con los Líderes

Se entrevista a cada líder de dependencia o grupo, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se consignan en la Matriz de Riesgos.

5.1.3 Identificación y Calificación de Riesgos

En esta fase, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.

5.1.4 Valoración del Riesgo Residual

En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

5.1.5 Mapas De Calor Donde Se Ubican Los Riesgos

Luego se procede a ubicar los riesgos en un mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

5.2 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Una vez ejecutadas las etapas de análisis y valoración de riesgos, y con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones aplicando el apetito de riesgos definido por la ESAP.

Si el riesgo se ubica en una zona no aceptable, cada líder responsable de los riesgos identificados con el apoyo de la Oficina de sistemas e informática, debe definir e implementar los controles necesarios para llevar el riesgo a un nivel aceptable a través del plan de tratamiento de riesgos.

A continuación, se definen las siguientes estrategias de tratamiento, asumir los riesgos bajos y moderados y gestionar el riesgo alto y extremo.

A continuación, se muestra la estrategia para abordar los riesgos y establecer su tratamiento:

PROCESO / DEPENDENCIA Y/O GRUPO INTERNO DE TRABAJO	ASUMIR EL RIESGO		REDUCIR EL RIESGO		TOTAL
	BAJO	MODERADO	ALTO	EXTREMO	
GESTION ADMINISTRATIVA / ALMACÉN E INVENTARIOS	1		4		5
CAPACITACION / ALTO GOBIERNO	7				7
ASESORÍA Y ASISTENCIA TÉCNICA	1		2		3
DOCENCIA / BIBLIOTECA Y CDIM	7		1		8
DOCENCIA	45	6			51
GESTION DOCUMENTAL/ GRUPO DE ARCHIVO Y CORRESPONDENCIA	2		3		5
PROCESO DE EVALUACIÓN Y AUTOEVALUA CIÓN/ CONTROL INTERNO DISCIPLINARIO	1				1
GESTIÓN ADMINISTRATIVA	1	7			8
GESTION FINANCIERA / GRUPO DE GESTIÓN CONTABLE	5		1		6
GESTIÓN DE LA COMUNICACIÓN	2		2		4
GESTIÓN FINANCIERA	1		3		4
SISTEMA GESTIÓN INTEGRAL	1				1
GESTIÓN JURÍDICA Y ASUNTOS LEGALES	9	3			12
GESTION ADMINISTRATIVA / GESTIÓN TALENTO HUMANO	9		4	1	14
GESTIÓN TECNOLÓGICA	4				4

PROCESO / DEPENDENCIA Y/O GRUPO INTERNO DE TRABAJO	ASUMIR EL RIESGO		REDUCIR EL RIESGO		TOTAL
	BAJO	MODERADO	ALTO	EXTREMO	
PLANEACIÓN ESTRATEGICA	8		4		12
GESTION FINANCIERA /PRESUPUESTO	6		1		7
GESTION FINANCIERO / RECAUDO Y CARTERA	10		2		12
CAPACITACION / SECRETARIA GENERAL			3		3
CAPACITACION / GRUPO DE SERVICIOS AL CIUDADANO	1		3		4
TOTAL	121	16	33	1	171
	137		34		

Controles recomendados

Frente a los 34 riesgos con estrategia de mitigación, para su gestión se proponen los siguientes controles de la norma ISO 27001 – Anexo A:

	ALMACÉN E INVENTARIOS	ASESORÍA Y ASISTENCIA TÉCNICA	BIBLIOTECA Y CDIM	DOCUMENTAL	GESTIÓN CONTABLE	GESTIÓN DE LA COMUNICACIÓN	GESTIÓN FINANCIERA	GESTIÓN TALENTO HUMANO	OFICINA ASESORA DE PLANEACION.	PRESUPUESTAL	RECAUDO Y CARTERA	SECRETARIA GENERAL	SERVICIO AL CIUDADANO	**Total general**
A.7.1.1. Selección.				1				1						2
A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información.				1					1	1			2	5
A.9.3. Responsabilidades de los usuarios.	3				1			1	2					7
A.10.1.1. Política sobre el uso de controles Criptográficos.		1												1
A.11.1.1. Perímetro de Seguridad Física.							2							2
A.11.1.3. Seguridad de oficinas, salones e instalaciones.				1									1	2
A.11.1.4. Protección contra amenazas externas y ambientales.								2				3		5
A.11.2.1. Ubicación y protección de los equipos.	1													1
A.11.2.2. Servicios Públicos de soporte.						1								1
A.11.2.4. Mantenimiento de equipos.							1				1			2
A.12.3.1. Copias de respaldo de la información.		1				1		2	1					5
A.15.2. Gestión de la prestación de servicios de proveedores.			1											1
Total general	4	2	1	3	1	2	3	5	4	1	2	3	3	34

En general, el control que más aplica es A.9.3. Responsabilidades de los usuarios, seguido de: A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información, A.11.1.4. Protección contra amenazas externas y ambientales, y A.15.2. Gestión de la prestación de servicios de proveedores.

5.3 SEGUIMIENTO Y CONTROL

El seguimiento y control se realiza de acuerdo a la **GUÍA PARA LA ADMINISTRACIÓN DE RIESGO v2 DC-S-GC-06.**

6 CRONOGRAMA

Para dar cumplimiento al ciclo de riesgo, el cronograma se establece anualmente, los riesgos de seguridad digital identificados se reflejarán en el Mapa de Riesgos Institucional, donde se establecerán las acciones de control y las fechas para implementar dichos controles, la oficina de sistemas e informática apoyará el proceso de definición de los controles con los líderes de cada uno de los grupos o dependencias.

La implementación se desarrolla en 2 fases, las cuales se definen a continuación:

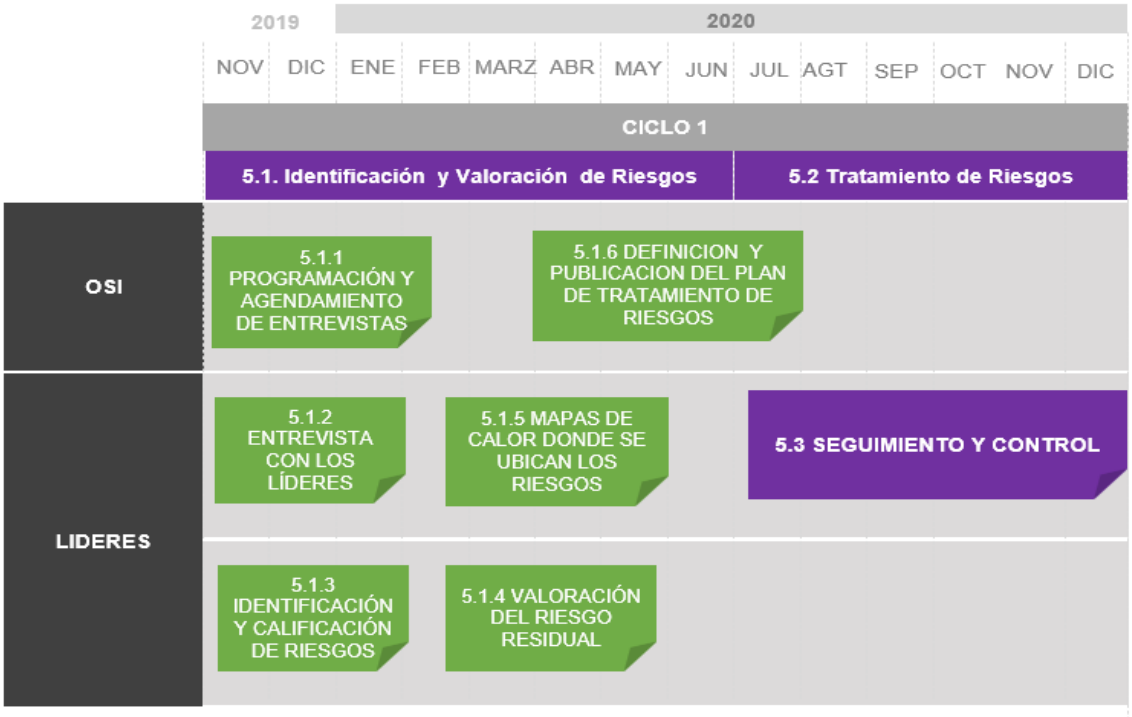

Ilustración 3. Cronograma

8. RECURSOS

La estimación y asignación de los recursos para el plan de tratamiento de riesgos de Seguridad de la información identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

Si el establecimiento de los controles implica la adquisición de herramientas tecnológicas bajo la responsabilidad de la Oficina de sistemas e informática, los recursos de inversión se tomarán del proyecto *"Fortalecimiento de las tecnologías de la información y la comunicación en la ESAP a nivel nacional."*

9. INDICADORES

La medición se realiza con un indicador de gestión que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y externo a través de la implementación y evaluación de controles.

El número de riesgos identificados como no aceptables no debe ser superior al 20% del total de riesgos identificados.

10. RESPONSABLES

La Oficina de sistemas e Informática asesora a las áreas en el proceso de identificación y valoración de los riesgos de seguridad de información y seguridad digital, los líderes de las áreas solicitarán a la Oficina asesora de planeación la inclusión de los mismos en el mapa de riesgos institucional, iinstrumento en donde se registran los riesgos identificados, su valoración y sus controles, para su seguimiento y control.

La oficina de sistemas e informática apoyará a los responsables de las áreas en la definición de los controles y hará seguimiento a su implementación, con el fin, de evidenciar en el siguiente ciclo la efectividad de los controles implementados y en consecuencia la disminución del riesgo No aceptable.

Así mismo, si se llegan a presentar incidentes de seguridad se validarán los riesgos identificados para determinar si obedece a un riesgo identificado y proceder a valorar, recalificar e implementar nuevos controles.

Los activos de información de la ESAP se encuentran disponibles para consulta en la página web https://www.esap.edu.co/portal/index.php/transparencia-2/ en la opción Instrumentos de gestión de Información de gestión pública.