PLAN GENERAL PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION

TRATAMIENTO DE RIESGOS PRIORIZADOS 2024

CÓDIGO: PL-GT-002

ESE Vidasinú

18/08/2022

E.S.E. vidasinú

Tabla de contenido

1. OBJETIVOS

Detallar el plan de tratamiento de riesgos de seguridad, para proteger la tecnología de información y comunicaciones de la E.S.E VIDA SINÚ, con mecanismos y controles que hagan frente a las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

2. ALCANCE

El plan de tratamiento de riesgos tiene como alcance proteger la información y la tecnología de información y comunicaciones de los procesos de la E.S.E VIDA SINÚ, utilizando como guía, las directrices del Ministerio Tecnologías de Información y Comunicaciones y el Departamento de la Función Pública.

3. SIGLAS Y ABREVIACIONES

ABREVIATURA	SIGNIFICADO
CCOC	Comando Conjunto Cibernético del Comando General de las Fuerzas Militares de Colombia
CCP	Centro Cibernético Policial de la Policía Nacional de Colombia
ColCERT	Grupo de Respuesta a Emergencias Cibernéticas de Colombia
CONPES	Consejo Nacional de Política Económica y Social de Colombia
CSIRT	Equipos de Respuestas ante Incidentes de Seguridad
MGRSD	Modelo Nacional de Gestión de Riesgos de Seguridad Digital
MINTIC	Ministerio de Tecnologías de la Información y las Comunicaciones
MIPG	Modelo Integrado de Planeación y Gestión
MSPI	Modelo de Seguridad y Privacidad de la Información
GRSD	Gestión de Riesgos de Seguridad Digital
ICC	Infraestructuras Críticas Cibernéticas
TI	Tecnologías de Información
TIC	Tecnologías de la Información y las Comunicaciones
TO	Tecnologías de Operación
DAF	Departamento administrativo de la Función Pública

Tabla 1: Siglas y Abreviaciones

Fuente: (DAF, 2019)

4. VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD DE LA INFORMACION

El Decreto 1078 de 2015 imparte los lineamientos del Gobierno Digital -GD, y entre estos está que las entidades públicas deben realizar la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI- con el objetivo de conformar un Sistema de Gestión de Seguridad de la Información, como tratar los riegos identificados al interior de la entidad y articularse con el Modelo Nacional de Gestión de Riesgos de Seguridad Digital – MGRSD.

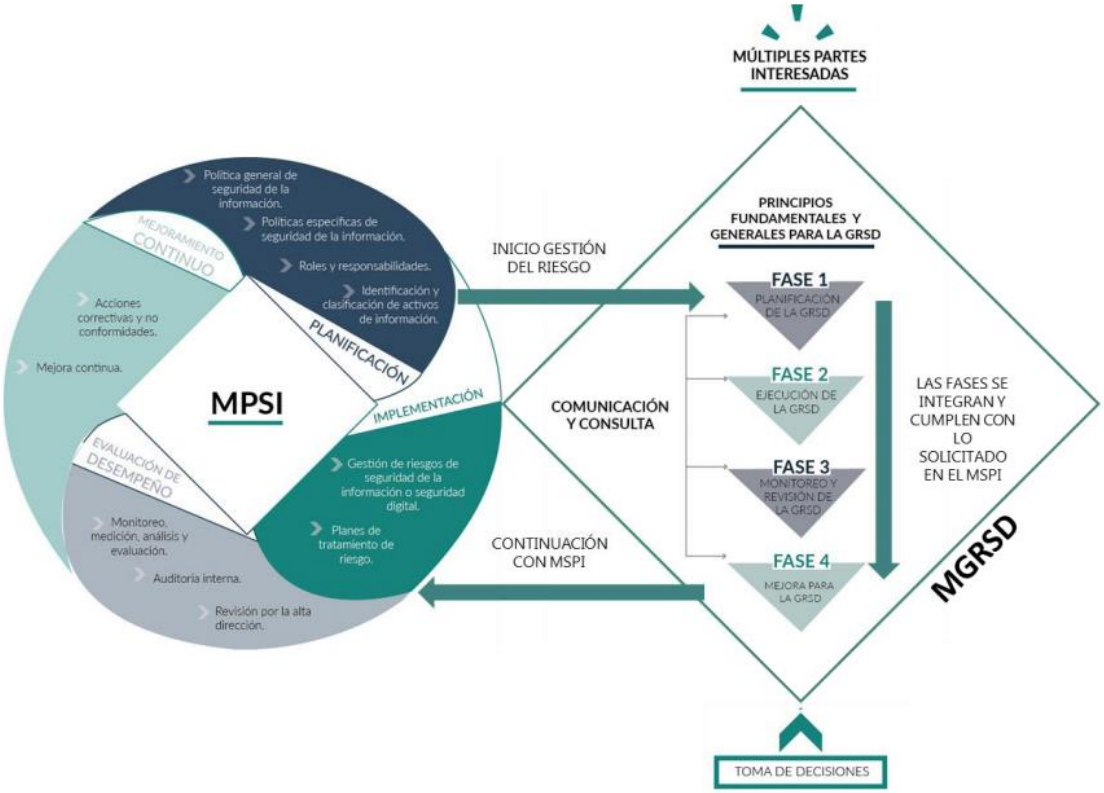

Ilustración 1: Interacción entre el MSPI y el MGRSD.

Fuente: (DAF, 2019)

La entidad encargada de establecer la metodología para la gestión de riesgo en las entidades pública es el DAF, el cual establece el siguiente proceso:

Ilustración 2: Proceso para la Administración del Riesgo

Fuente: (DAF, 2019)

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):

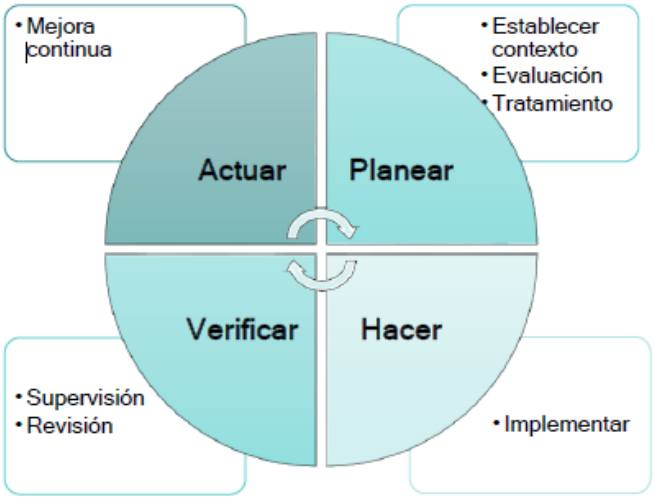

Ilustración 3: Ciclo PHVA

5. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En la evaluación o autodiagnósticos realizado con el instrumento de identificación de la línea base de seguridad del MSIP de MINTIC a la E.S.E VIDA SINÚ, se evidencio que se debe avanzar en la implementación de controles para mejorar los indicadores de riesgos de seguridad, por lo cual, se planteara un cronograma con las fases de gestión de riesgo del DAF enfocada a la seguridad digital.

Nro.	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	**GESTIONADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80	100	**GESTIONADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	**GESTIONADO**
A.8	GESTIÓN DE ACTIVOS	80	100	**GESTIONADO**
A.9	CONTROL DE ACCESO	80	100	**GESTIONADO**
A.10	CRIPTOGRAFÍA	40	100	**REPETIBLE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	80	100	**GESTIONADO**
A.12	SEGURIDAD DE LAS OPERACIONES	80	100	**GESTIONADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	80	100	**GESTIONADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	80	100	**GESTIONADO**
A.15	RELACIONES CON LOS PROVEEDORES	80	100	**GESTIONADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	100	**GESTIONADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	80	100	**GESTIONADO**
A.18	CUMPLIMIENTO	80	100	**GESTIONADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**77**	**100**	**DEFINIDO**

Tabla 2: Evaluación de Efectividad de controles

Fuente: Elaboración Propia

5.1. CRONOGRAMA DE PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Item	Hito	Fecha Inicio	Fecha Final
1	Contexto Estratégico	2/2/2020	31/12/2020
2	Identificación de Riesgos	2/2/2020	31/12/2020
3	Análisis de Riesgo	2/2/2020	31/12/2020
4	Valoración de los Riesgos	2/2/2020	31/12/2020
5	Identificar Controles	2/2/2020	31/12/2020
6	Implementar Controles	2/2/2020	31/12/2023
7	Mejora continua	2/2/2020	31/12/2024

Tabla 3: Cronograma del Plan de Tratamiento de Seguridad de la Información

5.2. TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN IDENTIFICADOS PARA EL 2023

Ver el documento de Excel Matriz_mapa_riesgos de TIC para el 2024

6. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El seguimiento y control se realiza de acuerdo a la GUÍA PARA LA ADMINISTRACIÓN DE RIESGO articles-5482_G8_Controles_Seguridad.

7. TERMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información,

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.
Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información

8. BIBLIOGRAFÍA

ISO/IEC 27001. ISO/IEC 27001:2013 Código para la práctica de la gestión de la seguridad de la información. Recuperado en noviembre de 2014 de https://www.iso.org/standard/66805.html

DAF. (7 de 11 de 2019). *www.funcionpublica.gov.co.* Obtenido de https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316352?_com_liferay_document_library_web_portlet_DLPortlet_INSTANCE_bGsp2IjUBdeu_redirect=https%3A%2F%2Fwww.funcionpublica.gov.co%2Fweb%2Feva%2Fbiblio

DAF. (7 de 11 de 2019). *www.funcionpublica.gov.co.* Obtenido de https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

MINTIC. (7 de 11 de 2019). *www.mintic.gov.co.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf