PLAN PARA LA GESTIÓN SISTEMÁTICA Y CÍCLICA DE RIESGOS DE SEGURIDAD DIGITAL

2024

CONTENIDO

1. OBJETIVO

Analizar la práctica y gestión de riesgos de seguridad digital en el cual se logren identificar las amenazas y vulnerabilidades a las que la Institución pueda estar expuesta desde el un entorno cibernético, con el fin de fortalecer el ambiente de control y metodología de gestión de riesgos basados en Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD) del MINTIC.

2. ALCANCE

El alcance del plan para la gestión sistemática y cíclica de riesgos de seguridad digital inicia con la fase de análisis, identificación, planificación de acciones; y concluye con la fase de mejoramiento continuo de la gestión de riesgos de seguridad digital y el plan de acción mediante el cual se realizará el identificación y tratamiento de los riesgos de seguridad digital identificados en la ESE Instituto de Saludo de Bucaramanga.

3. RESPONSABLE

Coordinador de TI, Ingeniero oficial de seguridad informática y protección de datos, Líder de infraestructura de TI y Líder de sistemas de información.

4. DEFINICIONES

Activo: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (3854 C. , 2016, Pág. 24)

Activo cibernético: En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. (3854 C. , 2016, Pág. 24)

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (27000:2016, 2016)

Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (3854 C. , 2016, Pág. 24)

Análisis del riesgo: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).

Csirt: Por su sigla en inglés: *Computer Security Incident Response Team* (Equipo de respuesta a incidentes de seguridad cibernética). (http:// www.first.org).

Gestión de riesgos de seguridad digital: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854, pág. 24). (3854, 2016)

Riesgo: es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente 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. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

Seguridad digital: es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Definiciones establecidas por la OCDE, y otras tomadas del documento CONPES 3854 de 2016

5. DESARROLLO

5.1. AUTODIAGNÓSTICO

Para el periodo 2023, se ha llevó a cabo el 100% de las actividades planificadas en el marco de la gestión sistemática y cíclica de riesgos de seguridad digital. Este logro ha sido posible gracias a la colaboración efectiva entre los diversos procesos dentro del área de Gestión de las TICS.

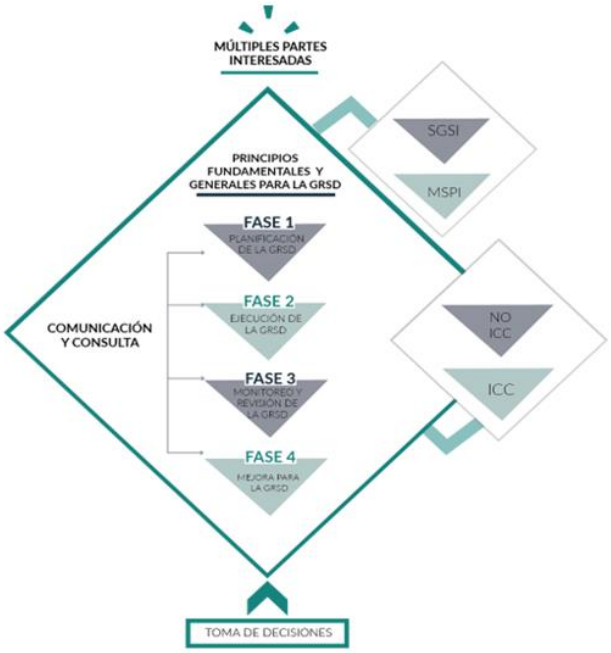
En particular, se ha ejecutado un exhaustivo análisis de riesgos que ha permitido identificar posibles amenazas y evaluar la probabilidad de su ocurrencia. Además, se ha implementado con éxito un campus virtual, sentando las bases para el despliegue de un curso virtual sobre seguridad de la información durante el año 2024.

Durante el último periodo, se ha llevado a cabo un monitoreo riguroso en seguridad de la información, lo que ha posibilitado identificar aspectos específicos que requieren fortalecimiento en los procesos. Asimismo, se ha procedido a la actualización de las políticas de seguridad de la información, asegurando así que estén alineadas con las mejores prácticas y normativas vigentes.

5.2. PLAN PARA LA GESTIÓN SISTEMÁTICA Y CÍCLICA DE RIESGOS DE SEGURIDAD DIGITAL

El plan para la gestión sistemática y cíclica de riesgos de seguridad digital propone la implementación y mejora continua a nivel institucional en las actividades para aplicar del modelo de gestión de riesgos de seguridad digital (MGRSD) y de incidentes propuesto por el MinTic. Facilitando la identificación y manejo de eventos de seguridad informática; dicha mejora busca lograr una gestión proactiva para el tratamiento de riesgos, mediante los lineamientos de seguridad y privacidad de la información con el fin de establecer acciones para proteger los activos de información preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Ilustración 1Marco conceptual del MGRSD



Fuente: Modelo Nacional de Gestión de Riesgos de Seguridad Digital

5.3. SITUACIÓN ACTUAL

El Instituto de Salud de Bucaramanga – ISABU E.S.E. entendiendo la Gestión de riesgos de seguridad digital, como una estrategia y siguiendo los lineamientos trazados por el Gobierno Nacional con lo expuesto en la Ley de transparencia 1712 de 2014, la Estrategia Gobierno en Línea y la Política de Gobierno Digital. Establece el plan para la gestión sistemática y cíclica de riesgos de seguridad digital en el cual se identifiquen los posibles riesgos, vulnerabilidades de seguridad digital.

En la gestión de riesgos de seguridad digital resulta importante realizar un análisis de identificación de posibles riesgos con el fin de poder establecer un plan de acción adecuado que logre mitigar las vulnerabilidades existentes en la

institución, por consiguiente, resulta indispensable definir actividades que de manera articulada permitan implementar medidas de control para la prevención, contención y mitigación de amenazas a las que se encuentran expuestos los activos de información de la entidad.

La ESE Instituto de salud de Bucaramanga, posee una estructura organizacional con procesos estratégicos, misionales, de Soporte, de verificación y mejora caracterizados en el Sistema Integrado de Gestión que permiten realizar la identificación, tratamiento, monitoreo y revisión de los riesgos de seguridad digital más críticos de la entidad que pueden impactar de manera considerable el desarrollo de funciones y logro de objetivos propuestos. Adicionalmente, se cuenta con distintos sistemas de información y servicios tecnológicos que soportan los procesos y por lo cual es necesario velar por la protección y seguridad de estos activos de información.

Para lograr lograr el objetivo del Plan en la gestión de riesgos de seguridad digital se deben involucrar los siguientes procesos de manera sistemática y cíclica:

5.3.1. Planificación y preparación para la gestión de riesgos: la institución debe preparase antes de la materialización de una amenaza para ello se debe realizar una detección y análisis de los posibles riesgos de seguridad de la información, ciberseguridad y protección de la privacidad.

5.3.2. Detección y análisis: En esta fase se realiza análisis de posibles vulnerabilidades y se determina si ha ocurrido algún incidente, para el cual se validan los reportes en los equipos de seguridad, y se indaga sobre información relacionada con los posibles incidente, se documenta la investigación, se recopila la evidencia, se prioriza la gestión del incidente según su impacto y en caso de efectuarse algún incidente se reporta al interior de la institución y al CSIRT Gobierno.

5.3.3. Mitigación y Actualización de Plan de acción: Para poder mitigar los posibles riesgos se deben de crear acciones y mantener actualizado el sistema de seguridad digital, identificando el vector de posibles ataques. Una vez se identifican las brechas de seguridad y vulnerabilidades en el entorno tecnológico; también se realiza un seguimiento periódico establecido en las políticas de la entidad para observar los factores que aún se deben mejorar.

5.4. ACTIVIDADES PLAN PARA LA GESTIÓN SISTEMÁTICA Y CÍCLICA DE RIESGOS DE SEGURIDAD DIGITAL

Con el fin de Identificar, clasificar riesgos y vulnerabilidades de seguridad digital en la Institución se programa las siguientes actividades para la vigencia del 2024.

No.	Actividad	Descripción de la actividad	Responsable	Formato
1	Documentar de SGSI (Sistema de Gestión de Seguridad de la Información ISO 27001:2022) para la ESE ISABU a través de la Política de seguridad de la información, ciberseguridad y protección de la privacidad.	Documentación de SGSI (sistema de gestión de seguridad de la información ISO 27001:2022), con el objetivo de tener un marco de trabajo que permita gestionar la seguridad de la información de manera integral dentro de la entidad	Ingeniero oficial de seguridad informática y protección de datos	Política de seguridad de la información, ciberseguridad y protección de la privacidad.
2	Realizar análisis de riesgos de TI con su respectiva valoración, en el cual se identifiquen los controles actuales y los controles a implementar para mitigar la probabilidad de ocurrencia.	Realización de análisis de riesgos de TI con su respectiva valoración, en el cual se identifiquen los controles actuales y los controles a implementar para mitigar la probabilidad de ocurrencia.	Ingeniero oficial de seguridad informática y protección de datos	Entregable Análisis de riesgos
3	Diseñar y realizar curso virtual para fortalecer la sensibilización de seguridad de la información, ciberseguridad y protección de la privacidad	Fortalecer conocimientos de seguridad de la información, ciberseguridad y protección de la privacidad por medio de la implementación de un curso que permita dar a conocer a todos los colaboradores las políticas, riesgos y buenas prácticas de la seguridad de la información, ciberseguridad y privacidad, inicialmente registrado a los colaboradores de planta.	Ingeniero oficial de seguridad informática y protección de datos	Entregable campus y curso virtuales

5.5. ANEXO

Formato Plan Estratégico e Institucional Código: PLA-F-012

6. DOCUMENTOS REFERENCIADOS

- 27000:2016, I. (2016). *ISO/IEC 27000:2016*. Obtenido de https://www.iso.org/standard/66435.html
- 3854. (2016). *CONPES 3854*. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes
- 3854, C. (2016, Pág. 24). *CONPES*. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf
- MinTic. (s.f.). *Modelo de Gestión de Riesgos de Seguridad Digital* . Obtenido de https://www.mintic.gov.co/portal/715/articles-61854_documento.docx
- mintic.gov. (s.f.). *Guis para la administracion de riesgos y diseño de controles en entidades públicas - Seguridad de la información* . Obtenido de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MGRSD/
- Publica, F. (s.f.). *Politica de seguridad Digital - Función Publica*. Obtenido de https://www.funcionpublica.gov.co/documents/28587410/34299507/Politica+de+Seguridad+Digital.pdf/ac8b063d-59ed-1c03-d23b-3e9d5fa5a36c?t=1631298504631

7. CONTROL DE MODIFICACIONES

CONTROL DE MODIFICACIONES			
Versión	**Fecha**	**Descripción de la Modificación**	**Realizada por**
1	25/01/2023	Documento Nuevo	Elaboró: Apoyo profesional de gestión de las Tics. Revisó: Lideres de Proceso Gestión de las Tics.
2	30/01/2024	Modificación del numeral 3, en el cual se incluyeron los responsables de acuerdo a los roles actuales del área Inclusión de componente autodiagnóstico Actualización del numeral 5.1.1 en el cual se ajustó el párrafo a la nueva NTC ISO 27001 denominada seguridad de la información, ciberseguridad y protección de la privacidad. Actualización del numeral 5.4 actividades plan para la gestión sistemática y cíclica de riesgos de seguridad digital	Elaboró: Ingeniero Oficial de Seguridad Informática y protección de datos. Revisó: Coordinador TI