PATRIMONIO AUTÓNOMO FONDO COLOMBIA EN PAZ – PA-FCP

CONVOCATORIA PÚBLICA No. 020 de 2018

ANÁLISIS PRELIMINAR DE LA CONTRATACIÓN

ANEXO 2
ESPECIFICACIONES TÉCNICAS

JULIO DE 2018

BOGOTÁ D.C.

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

ANEXO 2 ESPECIFICACIONES TÉCNICAS DEL SGSI

Siguiendo las recomendaciones de la ISO/IEC 27001:2013, este proyecto debe adelantarse contemplando en las etapas del ciclo PHVA:

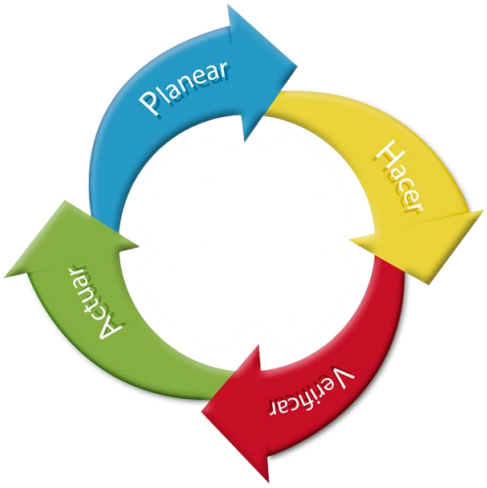

Ilustración 1. Ciclo PHVA.

En este sentido y con el fin de contar con la información necesaria, el proveedor deberá realizar un diagnóstico inicial que servirá de base para el desarrollo de las siguientes etapas.

De esta manera el proyecto debe contemplar las siguientes actividades dentro de cada etapa:

1. ETAPA 1 DIAGNÓSTICO

Hacer un estudio de la documentación existente relacionada con la JEP contemplada en el BMM[1] actual de la entidad, incluyendo entre otros: Misión, visión, cadena de valor, metas y objetivos estratégicos, definición de alto nivel de los procesos, organigrama, roles y funciones, arquitectura de sistemas de información. Este levantamiento de diagnóstico debe contemplar:

[1] Business Motivation Model por sus siglas en inglés.

1. Los procesos, sistemas de información, datos y plataforma de servicio que soporta la operación de EL INFORME gestionado por la Secretaría Ejecutiva a los magistrados, sistemas administrativos que se describen el **Anexo 1 antecedentes y contexto**
2. Los procesos misionales y de soporte definidos para la JEP, donde se consideren los roles, datos y plataformas tecnológicas que se encuentren disponibles o en proceso de estructuración.
3. Análisis de contexto identificando interesados internos y externos para la JEP, y estableciendo los requerimientos, necesidades y expectativas con respectos a la implementación del SGSI.
4. Análisis de la situación actual y un análisis de gap con respecto a la norma ISO 27001:2013 y a las recomendaciones de GEL. El objetivo es hacer una evaluación del nivel de madurez actual que sirva de referencia para medir la evolución de la JEP en el tiempo.
5. Ejecutar un análisis de vulnerabilidades a la infraestructura actual dispuesta en la JEP y relacionada en el anexo 1 – Antecedentes y Contexto JEP.
6. Realizar una identificación inicial de riesgos de seguridad de la información y su contexto en relación con la operación propia de la JEP.
7. Realizar y estructurar un instrumento para evaluar el grado de percepción y expectativas de los usuarios en la JEP con respecto a la seguridad de la información.

2. ETAPA 2 PLANEACIÓN

1. Presentar la metodología para el desarrollo de la iniciativa de sistema de gestión de seguridad teniendo en consideración las definiciones y recomendaciones de la norma ISO27001:2013, el manual GEL y el Marco de Arquitectura de TI de MINTIC.
2. Seleccionar una metodología reconocida para identificación de activos de información según las definiciones de la ISO 27001:2013. Esta metodología debe estar basada en estándares y buenas prácticas. Debe estar plenamente documentada y contar con formatos o herramientas que permitan su aplicación repetida garantizando consistencia y comparabilidad entre diferentes aplicaciones de ella. Debe contemplar la valoración de activos de información bajo diferentes criterios financieros y legales entre otros.
3. Seleccionar una metodología reconocida para gestión de riesgos según las definiciones de la ISO 27005 y la ISO 31000. Esta metodología debe estar basada en estándares y buenas prácticas. Debe estar plenamente documentada y contar con formatos o herramientas que permitan su aplicación repetida garantizando consistencia y comparabilidad entre diferentes aplicaciones de ella.
4. Adelantar un BIA en alineación con la ISO 22301 a partir de la información disponible actualmente y la metodología para su actualización en función del desarrollo de la JEP. El BIA debe tener en cuenta los procesos actuales y los futuros previstos de

acuerdo al nivel de detalle de los procesos al momento de iniciar las actividades de esta consultoría.

5. Realizar la identificación, valoración y tratamiento relacionados con el Inventario de activos de la información actuales de la JEP siguiendo la metodología seleccionada. El análisis debe contemplar los activos actuales y los activos de información que se prevé manejará la JEP en función de su misión.
6. Definir y documentar los requerimientos de seguridad de los diferentes activos de información (actuales y los previstos) identificando igualmente niveles de clasificación de confidencialidad teniendo en cuenta los requerimientos legales, la valoración de los activos y otras implicaciones aplicables a la entidad.
7. Definir y diseñar los mecanismos, políticas y procedimientos para asegurar el intercambio seguro de información con terceros (Nacionales / Internacionales) aplicables para la JEP. Por ejemplo, con el intercambio de información con servicios en la nube.
8. Adelantar el análisis de riesgos de seguridad de la información (incluyendo los riesgos relacionados a continuidad) a los diferentes procesos actuales de la entidad usando para ello la metodología de gestión de riesgos seleccionada anteriormente.
9. Definir el plan de tratamiento de riesgos y la declaración de aplicabilidad, con los controles aplicables del anexo de la ISO 27002:2013, las definiciones de continuidad y otros controles aplicables. Igualmente verificando contra la norma ISO 27032. Se debe presentar un plan de ruta con proyectos específicos (recursos, alcance, tiempos y estrategia de cumplimiento sugerida) para la implementación de cada uno de los controles en la mitigación de los riesgos identificados.
10. Definir la estrategia de seguridad con base en el marco jurídico colombiano y las mejores prácticas aplicables a LA JEP incluidos estándares como GRC – CRISC, PMI – RPM, Norma ISO/IEC 27001:2005, Norma ISO/IEC 27002 y las definidas en Gobierno en línea MSPI, relacionadas con Seguridad y considerando las disposiciones establecidas en la Ley 594 de 2000, por medio de la cual se dicta la Ley General de Archivos en Colombia y se dictan otras disposiciones.
11. Definir y documentar las políticas, objetivos, procesos y procedimientos de seguridad de la información, privacidad y protección de datos personales, pertinentes para gestionar el riesgo hacia niveles óptimos de seguridad de la información para el caso específico de la JEP.
12. Elaborar el plan de continuidad de negocio y plan de recuperación de desastres que cumpla con los requisitos que a continuación se relacionan:
    a) Estar basados en la ISO 22301:2015 y otros estándares relacionados con buenas prácticas como gestión de crisis, documentación de BIA, BCM, etc.
    b) Estar integrada con los procesos de seguridad de la información, privacidad y protección de datos personales.
    c) Incluir lo ateniente a contexto de la organización, liderazgo, soporte y planeación según lo señalado al respecto en la ISO 22301:2015.

13. Identificar y establecer la política de protección y uso de datos aplicable a las actividades propias de la JEP, definiendo alcance, requisitos, responsabilidades de gestión de los datos y cumplimiento con respecto al manual de gobierno en línea y la Ley 1581 de 2012 y demás normatividad aplicable a la JEP.
14. Definir y documentar los indicadores de gestión que serán utilizados para el SGSI y para el modelo de privacidad, protección de datos personales y continuidad de negocio.
15. Establecer el modelo de auditoría interna a adelantar.
16. Identificar y definir para las estrategias las tecnologías aplicables para seguridad de la capa de aplicaciones, software de base o aplicativo, de acuerdo con cada proceso a ser automatizado en los sistemas definidos en la arquitectura de TI para la JEP.

3. ETAPA 3 IMPLEMENTACIÓN Y OPERACIÓN

1. Definir el plan de mejoramiento el cual debe incluir las recomendaciones y propuestas de implementación para la superación de los aspectos deficientes en la gestión de la seguridad de la información y al cumplimiento de requisitos establecidos en GEL.
2. Definir la metodología y procedimientos de medición de eficacia de los controles definidos y especificar cómo se van a usar estas mediciones con el fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles.
3. Definir e implementar procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
4. Capacitar y realizar la transferencia de conocimiento a los funcionarios determinados por la JEP a fin de poder garantizar la gestión y operación del SGSI.
5. Desarrollar las actividades de las campañas de sensibilización en seguridad de la información dirigida a empleados y contratistas de la JEP.
6. Monitorear las condiciones de seguridad de la plataforma tecnológica actual de la JEP y definir las recomendaciones de remediación necesarias teniendo en cuenta criterios de beneficio/costo, así como los recursos de los cuales disponga la JEP. Estas recomendaciones deben estar orientadas a asegurar la plataforma, mientras comienza la operación del datacenter definitivo y la administración de la LAN. Este monitoreo debe contemplar las fases de diseño, montaje y operación del mismo e incluir la generación de informes periódicos según los acuerdos que se establezcan con la JEP al inicio del contrato.
7. Verificar las especificaciones de seguridad previstas para la contratación del datacenter definitivo para verificar que estén alineadas con las definiciones del SGSI.
8. Revisar y dar recomendaciones sobre el diseño de seguridad que se haga en el datacenter definitivo para verificar que estén alineadas con las definiciones del SGSI. Igualmente, sobre los términos de referencia de hasta 8 procesos de contratación previstos para la puesta en operación de la arquitectura tecnológica de la Entidad.

Esta revisión debe incluir la elaboración de cláusulas de seguridad de la información a incluir en las adquisiciones de tecnología para estos mismos 8 procesos de compra.

9. Implantar las políticas de seguridad definidas incluyendo las campañas de difusión y sensibilización requeridas.
10. Establecer estrategias y un plan de capacitación y sensibilización en seguridad informática y de la información, incluyendo aspectos relacionados con privacidad y protección de datos personales.

4. ETAPA 4 SEGUIMIENTO Y REVISIÓN DEL SGSI

1. Establecer e implementar una metodología y procedimientos de seguimiento y revisión del SGSI de acuerdo a las definiciones de la ISO 27001:2013 y con un énfasis especial para las consideraciones a tener en cuenta en la medida en que vayan entrando en operación los diferentes sistemas de apoyo de la JEP.

5. ENTREGABLES:

Se deben tener en consideración los requerimientos de documentación que establece la norma en función del alcance determinado en el presente anexo y en los demás documentos que hacen parte del Análisis Preliminar de la Contratación; incluyendo los aspectos relacionados con el control de registros establecido en la norma. La documentación que se genere debe entonces seguir estas recomendaciones y cubrir los diferentes aspectos señalados en la norma.

La documentación debe entonces contemplar por lo menos:

5.1. CONTEXTO DE LA JEP Y DIAGNÓSTICO

1. Documento de identificación y análisis de los procesos misionales y administrativos.
2. Documento con la definición de la estructura organizacional del SGSI.
3. Documento con la identificación actores de interés para la JEP con sus requerimientos y expectativas.
4. Documento con los resultados del análisis GAP y el nivel de madurez de la JEP.
5. Informe del análisis de brecha con respecto a los estándares NTC-ISO_IEC 27001:2013.
6. Plan de acción para cerrar las brechas identificadas en el análisis GAP.

5.2. DEFINICIÓN DEL SGSI Y DE LAS POLÍTICAS

1. Documento con la definición del dominio y el alcance del SGSI.
2. Documento con el plan Estratégico de Seguridad de la Información.
3. Documento que contenga la arquitectura detallada del SGSI para la JEP. Debe cumplir con los requisitos fijados por MINTIC para el Modelo de Seguridad y Privacidad de la Información.
4. Plan de Implementación del SGSI.
5. Documento con la definición de responsabilidades tanto de la JEP como del contratista con el SGSI y la definición de los modelos de seguridad.
6. Definición de estrategias de aseguramiento de acuerdo con la ley colombiana y al contexto organizacional de la JEP.
7. Documento con la definición de los objetivos de seguridad de la información.
8. Documento con las políticas, procedimientos, guías, plantillas, objetivos, procesos y procedimientos de seguridad de la información, privacidad y protección de datos.
9. Documento con la definición y la política de alto nivel en conjunto con las áreas competentes que contenga las sanciones por incumplimiento de las políticas.
10. Declaración de aplicabilidad de conformidad con la ISO 27001 y el marco de arquitectura de TI del Estado colombiano.

5.3. LEVANTAMIENTO DE ACTIVOS DE INFORMACIÓN Y GESTIÓN DE RIESGOS

1. Documento con la estrategia y el plan para el levantamiento, clasificación y gestión de activos de información actuales y futuros.
2. Crear la matriz con la identificación, valoración y clasificación de los activos de información.
3. Documento con los requerimientos de seguridad de los activos de información.
4. Documento con la estrategia y el plan de definición y gestión de riesgos.
5. Definición de métricas y controles para la posterior evaluación de los riesgos.
6. Guías, instructivos, plantillas o demás formatos necesarios para facilitar la gestión y uso de activos.

5.4. DEFINICIÓN Y GESTIÓN DE VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA JEP.

1. Documento con los resultados del análisis de vulnerabilidades y su matriz asociada.
2. Plan de tratamiento de vulnerabilidades de la infraestructura actual.
3. Definición de estrategias de aseguramiento de cada capa de la infraestructura.

4. Definición de políticas y de estrategias de ejecución de pruebas de penetración y pruebas de ethical hacking en la infraestructura.
5. Definición de métricas y controles para la posterior evaluación de vulnerabilidad y así definir estrategias de mejoramiento continuo.
6. Reportes de conclusiones sobre ejecución de las pruebas de vulnerabilidades, pruebas de penetración y ethical hacking. En este reporte se debe incluir una descripción de las pruebas, recomendaciones y conclusiones del caso.

5.5. PLAN DE CONTINUIDAD DE NEGOCIO

1. Documento con los resultados del análisis de impacto del negocio (BIA - Business Impact Analisys).
2. Documento con el plan de implementación de las estrategias para la continuidad de negocio.
3. Documento con el plan de recuperación ante fallos, incidentes y desastres.
4. Documento con los procedimientos de detección, tratamiento y documentación de incidentes.

5.6. CAPACITACIÓN Y SENSIBILIZACIÓN

1. Documento con la definición y el plan de capacitación del personal o contratistas.
2. Documento con la definición y el plan de sensibilización a los empleados de la JEP.
3. Informe y actas de actividades realizadas de capacitación y sensibilización.
4. Capacitación en SGSI, alineado con la norma ISO27001, Lineamientos de Seguridad de la información según GEL y en gestión de riesgos de ISO 31000 con una duración mínima de 20 horas en las instalaciones de la JEP impartida u para un máximo de (20) funcionarios de la JEP.
5. Realización de tres (3) campañas de sensibilización que incluyan el suministro de folletos, pendones, tableros, piezas gráficas para la intranet, piezas gráficas para los fondos de escritorio, stickers (anuncios informativos y de expectativa en puertas de ascensores y en áreas comunes o de alto tráfico), y un informe de cada campaña que incluya los resultados de una encuesta de medición de impacto.

5.7. MONITOREO DE LA INFRAESTRUCTURA TECNOLÓGICA Y ACOMPAÑAMIENTO.

1. Plan de monitoreo de la Infraestructura Tecnológica actual y futura de la JEP.
2. Informe de despliegue de la solución de monitoreo de la Infraestructura Tecnológica.
3. Reporte de evaluación y del Monitoreo con fines de ajuste de diseño para la Infraestructura Futura.

4. Documento con los requerimientos técnicos para la contratación de elementos necesarios para la implementación de la arquitectura de seguridad y de los planes de prevención y mejoramiento de hardware y software.
5. Recomendaciones de seguridad de la información para incluir en proyectos de TI que estén en curso en la JEP.