PORTADA

A) HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	JUSTIFICACIÓN DE LA MODIFICACIÓN
1	21/06/2019	Lanzamiento procedimiento
2	23/07/2021	Se adicionaron y desarrollaron los títulos Controles Existentes y Formatos y Anexos.
3	30/09/2021	Se adiciona el título 4.4 de Cumplimiento de requisitos legales y contractuales, y los controles del mapa de riesgos relacionados con el procedimiento numeral 5.1
4	02/05/2023	❖ Redefine el numeral 2. alcance ❖ Redefine el numeral 6. FORMATOS Y ANEXOS Para el numeral 4.1 DESARROLLO DE ANEXO TÉCNICO PARA ESTUDIOS PREVIOS: ❖ Elimina el numeral 20. Seguridad ❖ Agrega el numeral 18. Condiciones mínimas técnicas y de seguridad digital: ❖ Redefine los numerales: 5, 6,7, 11,12,17

B) REVISIONES Y APROBACIONES DEL DOCUMENTO

ELABORÓ	REVISÓ	APROBÓ
Nombre: Jesús Goyes Alvarado	Nombre: German Armando Correa Amado	Nombre: Francisco Alvaro Ramirez Rivera
Cargo: Contratista Asesor TI - Oficina Asesora de Planeación y Sistemas	Cargo: Jefe Oficina Asesora de Planeación y Sistemas	Cargo: Director General.
Fecha: 24/05/2023	Fecha: 28/05/2023	Fecha: 02/05/2023

REVISÓ
Nombre: Oscar Herrera Isaza
Cargo: Contratista Asesor Sistemas de Gestión
Fecha: 25/05/2023

C) LISTA DE DISTRIBUCIÓN

N°	NOMBRE Y CARGO
1	Director General
2	Jefe Oficina Asesora de Planeación y Sistemas
3	Profesional Especializado Oficina Asesora de Planeación y Sistemas
4	Profesional Universitario Oficina Asesora de Planeación y Sistemas
5	Profesional Universitario Oficina Asesora de Planeación y Sistemas
6	Técnico Operativo Oficina Asesora de Planeación y Sistemas
7	Asesor Tecnologías de la Información

1. OBJETIVO

Establecer los lineamientos técnicos mínimos para la contratación de bienes y servicios de carácter tecnológico.

2. ALCANCE

Establecer el marco de los requisitos mínimos que deben contemplarse dentro de los estudios previos o similares, para la contratación de bienes y servicios de carácter tecnológico

3. RESPONSABLES

La responsabilidad de ejecutar este procedimiento está a cargo del equipo de trabajo de la Oficina Asesora de Planeación y Sistemas, de acuerdo con el alcance de sus funciones y experticia.

4. DESARROLLO DEL PROCEDIMIENTO

4.1. DESARROLLO DE ANEXO TÉCNICO PARA ESTUDIOS PREVIOS.

N°	ACTIVIDAD
1	*El proceso inicia con una necesidad manifiesta que involucre componentes tecnológicos, dentro de alguno de los planes y proyectos de los procesos de la Entidad.*
2	El líder del proceso debe establecer el objetivo y alcance del bien o servicio tecnológico, apoyándose para ello, en los ingenieros de Gestión Tecnológica, según se considere.
3	*Se avanza sobre bienes y servicios tecnológicos aprobados en el comité de adquisiciones*
4	Establecer los requisitos mínimos del bien o servicio, teniendo como referencia, las características y especificaciones técnicas publicadas por los fabricantes
5	***Características agregadas**, según aplique, como:* ❖ *Capacitación, Suministro, instalación, configuración y puesta en marcha en la sede donde opera FONPRECON.* ❖ *Suministro de cables de poder, red y demás accesorios necesarios para la operación del bien o servicio.* ❖ *Funcionalidad de administración remota* ❖ *Solicite marcas reconocidas en el mercado, con ciclo de vida vigente desde el fabricante y que este no se encuentre cercano a culminar* ❖ *Instalación de certificados*
6	**Soporte y asistencia técnica:** ❖ *Solicitar horario de soporte y asistencia técnica, teniendo en cuenta que algunos alcances como 7x24 pueden incrementar el costo del bien o servicio. Algunos acuerdos pueden ser:* ❖ *5x8, 8 horas por cinco días. 7x24x365, 24 horas todo el año*

6	❖ *Evaluar y acordar una bolsa de horas según las necesidades del área funcional o el área de tecnología para mantenimiento evolutivo durante el tiempo de garantía de productos de desarrollo de software* ❖ *Especifique el tiempo de garantía requerido en partes, mano de obra especializada y soporte remoto y en sitio, mínimo un año*
7	**Compatibilidad:** ❖ Examinar y abordar la compatibilidad del equipo o servicio, con los equipos o servicios o componentes de la plataforma tecnológica en las versiones que operan en FONPRECON. ❖ Equipos o software certificados por el fabricante para soportar tecnología IP V6 ❖ Circuitos eléctricos regulados de 110 o 220 ❖ Entornos de dominio Microsoft ❖ Especifique de forma clara y verificada, seriales y modelo de equipos para los cuales adquiere componentes o servicios, así como versiones de software. ❖ Multiplataforma en casos de productos de software ❖ Acceso desde cualquier navegador de internet, computador o dispositivo móvil ❖ Capacidad de operar sobre entornos de virtualización. ❖ Desarrollo de software compatible con IPv6 ❖ Integración con servicios de la nube o servicios tecnológicos específicos de Fonprecon ❖ *Hardware o software certificados por el fabricante para soportar tecnología IPv6. Para los equipos, la información se corrobora en la ficha técnica del producto, para el software solicitar la certificación al proveedor acerca de que el desarrollo de software es compatible con IPv6* ❖ ***Evaluar y dimensionar las capacidades de almacenamiento, procesamiento y velocidad***
8	**Mecanismo de contratación:** Revise e identifique si el bien o servicio se ofrece desde alguno de los acuerdos marco de Colombia Compra Eficiente, de ser así, debe guiarse por las condiciones transversales y especificaciones ofrecidas, encontrando la mejor alternativa y basándose en los demás aspectos de este procedimiento
9	Especifique el cuadrante de Gartner donde se ubica el bien o servicio requerido. (Realizar esta actividad si aplica para la contratación en cuestión).
10	**Tamaño y forma de equipos:** Al tratarse de equipos, servidores, switch o cualquiera que se pueda disponer en un Rack del centro de datos, indique: ❖ Tamaño: en unidades de rack ❖ Factor de forma: Rack ❖ Fuentes de energía: redundantes ❖ Entrada de energía: 110 o 220 dependiendo del equipo en cuestión y disponibilidad de estos dos circuitos en el centro de datos ❖ Estaciones de trabajo tipo todo en uno o cpu y periféricos

	❖ Capacidad de la fuente de energía: Según especificaciones del equipo requerido ❖ Capacidad de almacenamiento: capacidad en teras o gigas ❖ Tipo de almacenamiento: características del almacenamiento en discos duros ❖ Características específicas y transversales según acuerdo marco
11	***Licenciamiento:*** ❖ *Verifique con el fabricante la forma de licenciamiento y especifique el que mejor se ajuste a la necesidad. (Actividad de Control)* ❖ *Sistemas operativos para servidores y estaciones de trabajo Microsoft Windows, la versión con ciclo de vida vigente y más extendido posible, que permita integración en un dominio Microsoft. Se puede optar por sistemas operativos Linux para servidores para casos específicos* ❖ *Licencia antivirus con los controles requeridos* ❖ *Licencia de paquete de ofimática, que incluya cliente de correo Outlook* ❖ *Registro y disponibilidad del licenciamiento en el portal de licencias de Microsoft para FONPRECON o el tenant respectivo* ❖ *Licenciamiento de usabilidad en favor de FONPRECON* ❖ *Licenciamiento de código fuente en favor de FONPRECON, en los casos de software a la medida.*
12	**Recepción de bienes o servicios:** ❖ *Revise y exija el cumplimiento de todas las características contempladas en el contrato* ❖ *Realice un acta de recepción, o en su defecto firme y toma copia del formato de entrega del proveedor.*
13	**Condiciones Técnicas de Obligatorio Cumplimiento:** Al anexo técnico debe agregar estas condiciones que aplican a cualquier bien o servicio: 1. Suscribir el acuerdo de confidencialidad, que se incluye como anexo en las políticas de seguridad y privacidad de la información de FONPRECON. *2.* Solicitar cronograma de suministro, instalación, configuración, pruebas, puesta en marcha, entrega, con identificación de responsables. 3. Entregar, instalar y poner en funcionamiento los bienes ofertados en el lugar indicado por el Fondo, instalaciones ubicadas en la carrera 10 24-55 pisos 2 y 3 de la ciudad de Bogotá D.C. dentro del plazo estipulado. FONPRECON efectuará la respectiva entrada de los bienes al almacén. 4. La gestión del servicio que incluye entrega, instalación y configuración de los equipos objeto de esta contratación se realizará en sitio en las instalaciones del Fondo, en horario hábil comprendido entre los días lunes a viernes de 8:00 a.m. a 5:00 p.m. 5. Entregar los equipos ofertados en su empaque original, totalmente sellado y con la documentación del caso, para ello la entidad verificará que el empaque original no haya sido violentado, o modificado, so pena de la no recepción o aceptación de los equipos que no observen tal condición 6. Brindar garantía en los equipos de mínimo cantidad en letras (cantidad en números) años contados a partir de la instalación y puesta en funcionamiento, por defecto de

13	los materiales o en la fabricación de los mismos, consistente en la reparación o el reemplazo de las partes defectuosas. Durante los primeros cuatro (4) meses contados a partir de la instalación y puesta en funcionamiento de los equipos, deben cambiarse inmediatamente los bienes que resulten defectuosos, con fallas o de mala calidad, por otros en perfectas condiciones de igual o mejores características. 7. Durante el periodo de garantía, deberá prestarse el servicio de mantenimiento correctivo del equipo On-Site en modalidad 5x8, el contratista deberá tener disponibilidad inmediata dentro del horario laboral y extra laboral cuando el Fondo lo requiera, sin costo adicional para la Entidad. 8. Asumir los costos derivados de fletes, seguros, bodegaje y movimiento de técnicos (Soporte en Garantía). 9. En el evento en que la reparación en garantía de un equipo requiera el retiro del mismo de las Dependencias del Fondo el contratista deberá suministrar un equipo de similares o superiores características, por el tiempo que dure la reparación. 10. El proponente dentro de la oferta deberá abstenerse, so pena del rechazo de la misma, de ofertar equipos que sean considerados como remanufacturados o repotenciados o en similar estado de funcionamiento, toda vez que los equipos ofrecidos deberán ser nuevos, de marcas reconocidas que garanticen la calidad y la originalidad de los productos. El proponente deberá ser certificado por el fabricante como distribuidor autorizado de los equipos que oferte. Para validar este concepto, deberá anexarse carta del fabricante como distribuidor autorizado, con vigencia de expedición no mayor a 30 días. 11. El proveedor deberá sostener los valores de inversión ofertados en caso de la contratación bajo la modalidad de subasta inversa para cada uno de lotes en que participe, bajo la posibilidad de generar adiciones al contrato adjudicado, en búsqueda de obtención de mayor número de bienes/equipos 12. Toda la instalación, Garantías, registros y licenciamientos deberán ser documentados en forma consistente y completa. Garantizando la originalidad de los productos y componentes entregados. 13. Todo el personal que genere las configuraciones e instalaciones deberá estar correctamente uniformado e identificado (carnetizado) como miembros del contratista al interior del Fondo, y deberá cumplir con todas las normas de seguridad industrial para su personal. 14. Dentro del diseño y construcción de software, se debe garantizar la confiabilidad, integridad y disponibilidad de la información. 15. Durante la instalación configuración y puesta en marcha del bien o servicio, se debe garantizar la confiabilidad, integridad y disponibilidad de la información. 16. Manuales técnicos y de usuario, en la medida de lo posible que cumpla con atributos requeridos en lo relacionado con manuales técnicos en la NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001 - 4.2.2 Manual de la calidad: **Manual técnico**

Atributo	Descripción
Prerrequisitos	Prerrequisitos de instalación del sistema: Sistema operativo de los servidores de aplicaciones y base de datos, marca y versión de la base de datos, marca y versión de los servidores de aplicaciones, navegador, configuraciones de seguridad, etc.
Frameworks y estándares	Nombres y versiones de los frameworks y estándares bajo los cuales está construido el sistema.
Diagrama de casos de uso	Diagrama de casos de uso del sistema.
Diagrama ER	Modelo entidad relación del sistema
Diccionario de datos	Diccionario de datos del sistema.
Scripts de instalación	Scripts de instalación del sistema.
Diagrama de componentes	Diagrama de componentes del sistema.
Diagrama de servicios	Diagrama de servicios expuestos por el sistema.
Diagrama de despliegue	Diagrama de despliegue del sistema.
Diagrama de clases	Diagrama de las clases más relevantes del sistema

Manual de usuario:

Atributo	Descripción
fecha de la versión	Versión del documento y fecha de la versión.
Prerrequisitos de instalación	Prerrequisitos de instalación del sistema: Sistema operativo, navegador, configuraciones de seguridad, etc.
Manual de instalación del sistema	Paso a paso con las instrucciones de instalación y configuración del sistema en el computador del usuario
Manual de uso del sistema	Paso a paso de uso de las principales opciones del sistema. Incluya imágenes para cada paso.
Preguntas frecuentes	Preguntas frecuentes que pueden realizar los usuarios y su respectiva respuesta

14 14

Migración de datos: Para esta clase de servicios, solicite:

- Informe detallado de cantidad de registros en la fuente de los datos
- Informe detallado de cantidad de registros en el destino de la migración
- Cronograma de migración
- Acordar una fecha de corte para la migración, con el líder de proceso e informar al ejecutor de la migración
- Establecer si la fuente de datos se continúa manteniendo en operación para consulta o si se apaga.
- Tomar copia de seguridad o snapshot, de la fuente de datos, antes de la migración
- Controles de seguridad contemplados para la migración y entrada en operación
- *Control: Para las actividades que impliquen migración de datos verificar el cumplimiento de estos ítems solicitados*

Paso a producción de bienes o servicios:

15	❖ Debe contemplar el diligenciamiento del formato de paso a producción y el respectivo procedimiento ❖ Validación de todas las características contempladas en el contrato, anexo técnico, propuesta, estudios previos y demás documentos que hagan parte integral del contrato.
16	**Aspectos de cumplimiento:** Establecer los lineamientos, políticas, regulación y demás aspectos del Gobierno de Colombia, que deban cumplir los bienes o servicios adquiridos.
17	***Desarrollo de software:*** ❖ *El proveedor debe disponer de todos los componentes tecnológicos y de seguridad para su ambiente de pruebas durante las etapas previas a la puesta en operación, con acceso para supervisión del avance por parte de la Entidad.* ❖ *En todas las etapas, los avances, deben ser presentados a la Entidad para su aprobación.* ❖ *Hacer uso de estándares para el desarrollo y documentación.* ❖ *Catálogo de reportes requeridos, incluyendo aquellos que requieren publicación web*
18	***Condiciones mínimas técnicas y de seguridad digital:*** *implementar los siguientes controles en el desarrollo de aplicaciones web y aplicaciones de escritorio:* ❖ *Hardening del activo en relación a los roles activos* ❖ *Control de acceso con credenciales* ❖ *Modelo de interoperabilidad del MINTIC, como marco de referencia de lenguaje de intercambio de información, en la implementación de diccionarios de datos para formularios, desarrollo de aplicaciones, bases de datos, reportes y demás.* ❖ *Cifrado de contraseñas* ❖ *Caducidad de contraseñas* ❖ *Gestión de recuperación de contraseña* ❖ *Gestión de cambio de contraseñas para el usuario* ❖ *Implementar controles de seguridad durante todo el ciclo de vida del desarrollo de software* ❖ *Implementar controles de seguridad relacionados con el control de la autenticación, definición de roles y privilegios y separación de funciones* ❖ *Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).* ❖ *Aplicar mecanismos de hardening para eliminar configuraciones y credenciales por defecto, además de deshabilitar métodos HTTP peligrosos como put, delete, trace y restringir en lo posible la administración remota.* ❖ *Proteger la integridad del código, mediante: (i) la validación exhaustiva de: inputs, variables post y get (no enviar parámetros sensibles a través del método get), Cookies (habilitar atributos de seguridad como Secure y HttpOnly), y, cabeceras HTTP; (ii) la sanitización de los parámetros de entrada: es decir, que cuando se reciba la información de dichas variables se eliminen etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un script, además de la restricción de formatos y tamaños de subidas de archivos; (iii) la sanitización y*

18	*escape de variables en el código; (iv) verificación estándar de las Políticas de Origen de las cabeceras; y (v) la verificación y comprobación del token de CSRF (cuando aplique).* ❖ *Ejecutar monitoreos de seguridad sobre las páginas web que contemple, entre otras, las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques* ❖ *Exigir mecanismos de autenticación dentro de los sitios web a través de la creación de contraseñas fuertes y solicitar renovaciones periódicas de las mismas garantizando la accesibilidad de persona con discapacidad* ❖ *Mantener actualizado el software aun ciclo de vida vigente, frameworks, plugins y demás componentes de la solución.* ❖ *Restringir el uso de login contra ataques de fuerza bruta, implementando, entre otros: mecanismos de captcha accesibles o auto detectable, y/o limitar la tasa de intentos de login.* ❖ *Ocultar y restringir páginas de acceso administrativo.* ❖ *Restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.* ❖ *Crear copias de respaldo.* ❖ *Almacenar trazas o logs de auditoría de los eventos de seguridad, logins, entre otros.* ❖ *Garantizar conexiones seguras a través de uso de certificados, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales, para evitar la manipulación de parámetros en las peticiones. (adicional al cifrado SSL), También deben habilitar las cabeceras de seguridad, entre otras las siguientes: Content-Security-Policy (CSP), X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Strict-Transport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, Feature-Policy.* ❖ *Implementar mensajes genéricos de error, que no revelen información acerca de la tecnología usada, excepciones o parámetros que dispararon el error específico, los cuales deberán ser comprensibles por parte de las personas* ❖ *Proteger el binario de la aplicación, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing) para analizar la lógica de la aplicación.* ❖ *Sanitización de parámetros de entrada mediante la eliminación de etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un «script», además de la restricción de formatos y tamaños para subida de archivos.* ❖ *Sanitización de caracteres especiales (secuencia de Escape de variables en el código de Programación)* ❖ *Revisar las recomendaciones de seguridad en la guía de desarrollo seguro de aplicaciones y Servicios Web Seguros de la Open Web Application Security Project (OWASP).*

18	❖ *Implementar en los servidores los controles necesarios (hardware o software) de protección de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros.* ❖ *Incorporar validación de formularios tanto del lado del cliente como del lado del servidor.* ❖ *Implementar monitoreos de seguridad sobre la plataforma tecnológica que hace parte del sitio web (escaneo de vulnerabilidades, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios) y realizar las acciones de mitigación correspondientes.* ❖ *Establecer los planes de contingencia, DRP y BCP, que permita garantizar la continuidad de la sede electrónica o del sitio web 7/24 los 365 días del año.* ❖ *Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados.* ❖ *Implementar sistemas antivirus en el servidor web, para garantizar medidas contra infecciones de malware a los archivos del mismo.* ❖ *Controlar el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web* ❖ *Evitar el uso de procedimientos complementarios no controlados como scripts del tipo VB, JS, PS, entre otros.* ❖ *No usar direcciones IP explicitas en archivos de configuración, en cambio usar nombres FQDN con resolución DNS* ❖ *No quemar direcciones IP o nombres FQDN en el código fuente* ❖ *Realizar análisis estático del código con el objetivo de identificar vulnerabilidades que se encuentra en la programación de las aplicaciones.* ❖ *Cumplir con la estandarización de código fuente para portales web, siguiendo las buenas prácticas del W3C (World Web Wide Consortium), de forma que permita la correcta visualización de la información a los usuarios.* ❖ *Adoptar validadores HTML y CCS para la continua revisión del sitio web y su mejora continua, a través de las buenas prácticas del W3C (World Web Wide Consortium).* ❖ *Cumplir con los estándares definidos para la integración al Portal Único del Estado Colombiano GOV.CO, incluyendo la validación de la codificación, en caso de que les aplique.*
18	❖ *Incluir lenguaje común de intercambio para la generación y divulgación de la información y datos estructurados y no estructurados dispuestos en medios electrónicos, como los sitios web de los sujetos obligados y el Portal Único del Estado Colombiano GOV.CO, en caso de que les aplique.* ❖ *Implementar un sistema de control de versiones (Git), que permitan planear y controlar la vida de la aplicación, y en una fase a mediano plazo poder implementar un sistema de integración, cambio y despliegue continuo.*
	Alojamiento: ❖ Especifique si el producto o servicio se aloja en el centro de datos de FONPRECON o en un tercero

19	❖ Si el alojamiento es con un tercero, se debe solicitar aplicación y vigencia de políticas de tratamiento de datos personales, lineamientos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información *(Actividad de control)*
20	De manera permanente todos los servidores públicos que hacen parte del Grupo de Tecnología, deberán ejecutar los controles establecidos en el numeral 5 de este procedimiento incluido los controles del mapa de riesgos.

4.2. ESTUDIO DE MERCADO.

N°	ACTIVIDAD
1	Con el anexo técnico de especificaciones, solicitar visita previa a proveedores, para validar condiciones de instalación y puesta en marcha, de forma que se identifiquen costos asociados que puedan ser incluidos en la propuesta. *(Actividad de control)* Solicitar cotizaciones del bien o servicio. *(Actividad de control)*
2	Ajustar los estudios previos y sus especificaciones técnicas en conformidad con las observaciones recibidas en la visita o reunión técnica. *(Actividad de control)*

4.3. SUPERVISIÓN TÉCNICA.

1 1	**Supervisión Técnica:** Para el seguimiento de la ejecución del contrato tenga en cuenta estas recomendaciones: *Realice un check list que resuma todos los requerimientos que debe cumplir el proveedor y que se encuentran en el contrato, estudios previos, propuesta y demás anexos. *(Actividad de control)* *Consulte con el área de contratación y tenga claridad de la fecha de aprobación de las pólizas *Consulte en el contrato la forma de inicio de la ejecución, puede ser según fecha de aprobación de pólizas de garantía o acta de inicio. *Si la ejecución del contrato inicia con acta de inicio, acuerde día y hora para el levantamiento de esta acta. *Consulte en el contrato el plazo de ejecución *Tenga claridad y datos de contacto del representante del proveedor o gerente del proyecto *Deje constancia de los faltantes que pueda encontrar, informando al jefe de la Oficina de Planeación y al proveedor, exigiendo completar la entrega del componente o característica

4.4. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES.

Se debe revisar el marco normativo aplicable al momento de contratar bienes y servicios de tecnología y de acuerdo a la temática que se desea cubrir se debe examinar el cumplimiento teniendo en cuenta lo consignado en el Catálogo de Marco Normativo (Políticas, normas y legislación).xlsx que se encuentra referenciado como un hipervínculo en el listado de Catálogos

dentro de la hoja principal del documento **Administración TI.xls** y que es administrado por la Oficina Asesora de Planeación y Sistemas.

5. CONTROLES EXISTENTES

5.1 CONTROLES MAPA DE RIESGOS RELACIONADOS CON EL PROCEDIMIENTO

Riesgo 1. CIBERSEGURIDAD

Como un conjunto de amenazas que ponen en riesgo la información digital que es procesada, almacenada y transportada por los equipos tecnológicos y sistemas de información de la Entidad que se encuentran interconectados entre si e interactúan con internet.

1. *El equipo de tecnología en algunas acciones específicas el profesional universitario y el profesional especializado del proceso de Gestión TI, realiza la administración y gestión diaria, de las soluciones de seguridad implementadas, tales como ANTIVIRUS, solución unificada de amenazas UTM, WSUS para aplicación de parches de seguridad, con el propósito de garantizar que la operación de estos componentes sea la esperada. Para ello debe basarse en las respectivas consolas de administración, así como en el software de inventario y logs denominado LANSWEPPER. Las evidencias son los logs de cada herramienta indicada así como los casos abiertos de soporte ante los proveedores de antivirus y solución UTM.*
1.1. *El ingeniero del equipo de trabajo de gestión tecnológica, en el momento que evidencia un incidente de ciberseguridad, realiza el reporte basándose en el procedimiento denominado PARA REPORTAR INCIDENTES DE CIBERSEGURIDAD, con el propósito de recibir asistencia técnica de organismos del Estado con mayor experticia en temáticas de ciberseguridad, dejando como evidencia el reporte mismo.*
1.2*. Los ingenieros que lideran el equipo de trabajo de gestión tecnológica, realizan el cambio semestral de las credenciales de administración de TI, con documentación y custodia centralizada, mediante utilidad de software KEEPASS, basándose en el procedimiento de CUSTODIA PARA CREDENCIALES DE ADMINISTRACIÓN DE TI, dejando como evidencia la documentación en el mismo sistema KEPASS y conservación de credenciales históricas que pueden ser requeridas para acceso a copias de seguridad.*
1.3*. El profesional universitario a cargo de la gestión de copias de seguridad, realiza copias de seguridad, de acuerdo con el procedimiento denominado GENERACIÓN Y RESTAURACIÓN DE COPIAS DE SEGURIDAD, POLÍTICAS DE TI, CIRCULAR 20192000000044 de 08-04-2019, bitácora de copias de bases de datos, servidores virtuales y copia de estaciones de trabajo, conservando la trazabilidad en el sistema Veeam Backup y documentación excel de cintas magnéticas. (Este control sirve para las causas 1, 3, 7 y 8 del riesgo #2)*
1.4. *Los ingenieros que componen el equipo de trabajo de gestión tecnológica, adoptan y aplican los planes, políticas y procedimientos, en cuanto a todo su contenido en procura de adoptar los lineamientos de seguridad y ciberseguridad en lo referente al uso del hardware y software . Estos documentos se encuentra disponibles en la unidad de red de CALIDAD y publicados en el sitio web de FONPRECON. Se debe dejar evidencia del reporte de incidentes de ciberseguridad, para los casos que se haya materializado el riesgo de ciberseguridad. (Este control sirve para la causa 2 del riesgo #1 y para las causas 1, 2 y 6 del riesgo #2)"*

2.1. *Los ingenieros de mesa de ayuda, atienden solicitudes recibidas por mesa de ayuda, correo electrónico o llamada telefónica, basándose tanto en el procedimiento denominado PARA LA SOLUCIÓN DE INCIDENTES Y REQUERIMIENTOS A TRAVES DE LA MESA DE AYUDA, como en las POLITICAS DE TI vigentes en lo relacionado con el uso de hardware, software y mesa de ayuda, dejando evidencia de la trazabilidad de cada caso en el sistema de mesa de ayuda. (Este control sirve para la causa 3 del riesgo #1 y para la causa 3 del riesgo #2)*
2.2. *La Dirección de Fonprecon, cada vez que haya una actualización emite circular informando la obligatoriedad de la lectura y aplicación del documento denominado Políticas de TI. (Este control sirve para las causas 4 y 6 del riesgo #1 y para la causa 6 del riesgo #2)"*

3.1*. La Oficina Asesora de planeación y sistemas debe mantener un catalogo de software autorizado, actualizado y revisado al menos una vez al año, para controlar lo que es permitido instalar en estaciones de trabajo y equipos del centro de datos.*
3.2*. Los ingenieros de mesa de ayuda, revisan mensualmente, el software instalado en las estaciones de trabajo, basándose para ello en la herramienta de inventario de software LANSWEPPER, contrastado con el catalogo de software autorizado de FONPRECON y proceden con lo pertinente para la desinstalación en coordinación con el jefe del proceso y el usuario del equipo en cuestión, dejando la evidencia mediante correo electrónico.*
Los ingenieros de mesa de ayuda, configuran los usuarios de red en las estaciones de trabajo, sin privilegios de administrador, para controlar instalación de software no autorizado. Ninguna estación de trabajo debe operar con privilegios administrativos. La evidencia es la configuración del usuario en cada estación de trabajo. (Este control sirve para la causa 1 del riesgo #1)"

4. *Los ingenieros que lideran tareas relacionadas con desarrollo y mantenimiento de software desarrollados en la entidad, mantienen siempre la custodia exclusiva para del código fuente, almacenado en la solución de control de versiones o en el servidor de archivos. La evidencia es la disponibilidad del sistema de control de versiones con acceso restringido para personal autorizado.*
4.1*. El jefe de la Oficina de Planeación y Sistemas junto con el líder del proceso, autorizan la intervención de código fuente por parte de un tercero, en los casos que considere necesario, mediante la autorización de entrega del código fuente y la suscripción del acuerdo de confidencialidad, que se encuentra dentro de las POLITICAS DE TI, como evidencia."*

5. *El ingeniero a cargo, administra diariamente el sistema WSUS, de actualizaciones productos de software Microsoft, verificando que su operación sea la esperada, basándose para ello en el procedimiento denominado PARA APLICACIÓN DE PARCHES DE SEGURIDAD y la consola de administración de WSUS, conservando la trazabilidad en dicho sistema del estado de cada equipo y actualización. (Este control sirve para la causa 1 del riesgo #2)*
5.1. *El ingeniero a cargo, administra los equipos del centro de datos, y gestiona la aplicación de parches de seguridad del fabricante, al menos una vez al año, dejando como evidencia la documentación realizada al respecto en control de cambios de la matriz excel Admin TI. Para esta actividad puede apoyarse en la documentación y soporte técnico del fabricante.*
5.2. *El ingeniero a cargo, realiza análisis de vulnerabilidades en los equipos del centro de datos y estaciones de trabajo, mediante la utilidad open source GSM (Greenbone Security Manager) versión community, con el fin de generar informe con oportunidades de mejora. Se realiza una vez al año con la consecuente implementación de mejoras. Se evidencia en la consola de gestión de vulnerabilidades de GSM. (Este control sirve para la causa 5 del riesgo #1)"*

6. *La Oficina Asesora de Planeación y Sistemas, identifica temáticas sobre ciberseguridad y coordina su socialización mediante estrategias de socialización o sesiones de sensibilización con ayudas multimedia, capacitaciones, boletines, entre otros, dejando como evidencia el registro de asistencia a estas últimas y el boletín socializado por correo electrónico. (Este control sirve para la causa 1 del riesgo #1)*

7. *Los ingenieros a cargo de administración de tecnología, mantienen actualizado el libro excel 'Admin TI' con relación al inventario de hardware y sus garantias vigentes, para mantener un control del ciclo de vida de cada componente de hardware, incluyendo lo relacionado a fechas de corte de licencias y garantías para los equipos del centro de datos.. La evidencia es la actualización continua de este documento. (Este control sirve para las causas 5 y 9 del riesgo #2)*

Riesgos 2. INDISPONIBILIDAD DE LA PLATAFORMA TECNOLÓGICA

Perder total o parcialmente la capacidad de operación tecnológica impidiendo la entrega y acceso a los servicios de TI.

1. *Los ingenieros administradores del centro de datos, o proveedor de infraestructura y plataforma tecnológica configuran y activan el sistema de alertas de fallas de hardware y software con reporte en tiempo real, desde las funcionalidades de cada fabricante (DELL, Hewlett Packard, WatchGuard, etc), así como desde la plataforma online https://uptimerobot.com/ , con el propósito de atender de forma inmediata el incidente empezando con acciones correctivas del equipo de trabajo de tecnología y posterior escalado mediante la apertura de casos de soporte con el respectivo proveedor del servicio o activo en función de los acuerdos de niveles de servicio. Se restablece conectividad de canal Backup con remplazo del equipo router que presente falla técnica.*
1.1. *Los ingenieros administradores del centro de datos, diariamente realizan la gestión de logs tanto de la solución unificada de amenazas UTM, basándose en el sistema de logs Watchguard Dimensión, como de la herramienta LanSwepper. con el propósito de aplicar los correctivos del caso de forma inmediata. Para los casos que amerite, se deba hacer uso de la garantía y soporte del proveedor de la solución.*
1.2. *Los ingenieros administradores del centro de datos, mantienen actualizado y vigente el Plan de Contingencia, con el propósito de implementar acciones en el menor tiempo posible, en caso fallas de hardware y software. Esos casos deben documentarse en la matriz excel Admin TI, control de cambios.*
1.3. *La Oficina Asesora de Planeación y Sistemas, mantiene vigente la garantía de los equipos servidores del centro de datos, Hewlett Packard y DELL, con renovación al vencimiento de la misma, con alcance de suministro de partes, soporte en sitio para análisis y configuración e instalación, asistencia telefónica. La existencia de este contrato vigente se considera la evidencia como tal.*
1.7. *La Oficina Asesora de Planeación y Sistemas, incluye en el plan anual de mantenimiento, actividades de mantenimiento preventivo y correctivo a la red eléctrica y a los equipos de aire acondicionado y UPS del centro de datos, La evidencia es la ejecución del plan de mantenimiento."*

2. *La Oficina Asesora de Planeación y Sistemas, fortalece el proceso de Gestión Tecnológica, con asesoría especializada en la gestión del hardware, software, seguridad y ciberseguridad, cuya contratación se hace al inicio de cada año y su evidencia es el contrato de prestación de servicios. (Este control sirve para las causas 1 de los riesgos #1 y #2)*
2.1. *El jefe de la Oficina de Planeación y Sistemas, identifica y sugiere temáticas de capacitación sobre aspectos de TI, al inicio de año, para el plan de capacitaciones liderado por la Oficina de talento humano."*

3. *La Oficina de Planeación y Sistemas y los ingenieros de gestión tecnológica, mantienen vigente el servicio de acceso remoto a los servicios de TI, mediante red privada virtual (VPN), con asignación de credenciales de acceso por demanda mediante el dispositivo de seguridad Unificada UTM y bajo las directrices del documento denominado Políticas de TI en lo concerniente a teletrabajo. (Este control sirve para la causa 7 del riesgo #2)*

4*. La Oficina Asesora de Planeación y Sistemas, elabora estudios de mercado y estudios previos para la adquisición de bienes y servicios de tecnología y su posterior seguimiento, basándose para ello en el procedimiento denominado para gestión de proveedores de tecnología. La evidencia se puede observar en la integración de las recomendaciones del procedimiento en los estudios previos.*
4.1. *La Oficina Asesora de Planeación y Sistemas, escala ante la Oficina Asesora Jurídica, los casos en los que se evidencia obligaciones no atendidas por el contratista, con el propósito de análisis y acciones jurídicas, mediante memorando y los soportes del caso como evidencia del suceso. Se cuenta con el cumplimiento de niveles de servicios con dos proveedores y pólizas de cumplimiento."*

5. *La oficina de planeación y sistemas, incluye cada 4 años en el plan PETI, los proyectos de actualización tecnológica que se hayan considerado, de acuerdo con el ciclo de vida de cada componente (hardware y software). (Este control sirve para la causa 7 del riesgo #1)*

6. *Los ingenieros que administran la operación del centro de datos y la entrega de servicios de TI, realizan paso a producción de nuevas versiones de software o hardware de forma controlada, basándose en la aplicación del procedimiento denominado PASO A PRODUCCIÓN COMPONENTES DE TECNOLOGÍAS DE INFORMACIÓN, documento que requiere la firma de quienes intervienen y se constituye en evidencia. (Este control sirve para la causa 2 del riesgo #1)*

7. *La Oficina Asesora de Planeación y Sistemas, mantiene vigente y actualizado, el plan de continuidad de negocio BCP, que incluye el plan de recuperación de desastres tecnológicos DRP, con pruebas anuales, llevadas a cabo por los ingenieros de gestión tecnológica para el caso del DRP y por el Jefe de planeación para el caso del BCP. Se evidencia con el informe de las pruebas anuales. (Este control sirve para las causas 1 y 3 del riesgo #2)*

8.1. *La Oficina Asesora de Planeación y Sistemas, socializa el documento de Políticas de TI, de forma que sea conocido lo relacionado al uso de equipos y cómo actuar en caso de pérdida, en cuyo caso el reporte de perdida ante las instancias del caso. Se cuenta con pólizas de activos compartidos.*
8.2*. La Oficina Asesora de Planeación y Sistemas, adelanta los procedimientos del caso, para efectos de reporte del caso ante la Sub Dirección Administrativa y Financiera, para que se realice lo pertinente en el caso en que este amparo se encuentre vigente en la Entidad."*

9.1. *La Oficina Asesora de Planeación y Sistemas, gestiona el estudio de mercado, aprobación y adquisición de licencias y garantías extendidas en los casos que sean requeridos para los equipos del centro de datos, de acuerdo a la vigencia periódica de cada activo.*

6.FORMATOS Y ANEXOS

- *Formato de paso a producción que forma parte del procedimiento de gestión de cambios*