**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| **PROGRAMA DE FORMACIÓN** | Seguridad en aplicaciones web |
| --- | --- |

| **COMPETENCIA** | 220501111 - Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica. | **RESULTADOS DE APRENDIZAJE** | 220501111-02 - Comprobar la seguridad web de acuerdo con los indicadores y métricas establecidos. |
| --- | --- | --- | --- |

| **NÚMERO DEL COMPONENTE FORMATIVO** | CF06 |
| --- | --- |
| **NOMBRE DEL COMPONENTE FORMATIVO** | Monitoreo de la Seguridad Web |
| **BREVE DESCRIPCIÓN** | En la construcción de un sistema de información por procesamiento electrónico de datos orientado a la web, se deben implementar los mecanismos que permiten medir el comportamiento de la seguridad, como monitoreo, metodologías, indicadores y métricas, unido a las herramientas de *software*. |
| **PALABRAS CLAVE** | Actividades, Documentación, Implantación, Monitorear, Políticas |

| **ÁREA OCUPACIONAL** | 9 - PROCESAMIENTO, FABRICACIÓN Y ENSAMBLE |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS:**

**Introducción**

**1. Monitorear la seguridad web**

**2. Metodologías, normas y estándares**

**3. Políticas internas de una organización**

**4. Indicadores**

**5. Métricas**

**6. Herramientas de *software***

**7. Informe de monitoreo**

1. **INTRODUCCIÓN**

La seguridad web está relacionada directamente con la vigilancia en todos los aspectos del diseño y uso de un sitio web, es decir, es aquella actividad encargada de proteger sitios web del acceso, uso, modificación, destrucción o interrupción, no autorizados.

Es importante tener en cuenta existen muchos riesgos que se pueden presentar, por solo el hecho de que el sistema de información se encuentre desprotegido y se presenten situaciones como, robo de información, explotación de datos, redireccionamiento a páginas web maliciosas, mostrar anuncios no deseados, entre otros.

Teniendo en cuenta lo anterior, el aprendiz en el presente componente formativo, conocerá sobre las diferentes estrategias para monitorear la seguridad web, para lo cual se invita a observar el siguiente video:



1. **DESARROLLO DE CONTENIDOS**

**1. Monitorear la seguridad web**

Las empresas y organizaciones deben cuidar muy bien sus sistemas y equipos informáticos, dado que en la actualidad existen muchos tipos de ataques que podrían afectar la seguridad de la información y de los datos y no solo basta con tener un antivirus instalado a pesar que sea de pago, este de igual manera está propenso a recibir ataques y a generar bloqueos que afecten todo el sistema operativo, provocando pérdida de la información.

Por tanto, se hace necesario realizar monitoreo activo y permanente de amenazas, donde se lleven a cabo pruebas de verificación del correcto funcionamiento y de la no existencia de brechas de seguridad, amenazas en el sistema o programas obsoletos que se puedan convertir en la entrada de piratas informáticos y finalmente, revisar periódicamente el cumplimiento de las medidas de seguridad, acatando las normas, metodologías y estándares.



**2. Metodologías, normas y estándares**

En el mundo de la seguridad en las aplicaciones Web, se han implementado metodologías, normas y estándares importantes para la detección y prevención de riesgos informáticos, a continuación se describirán los más comunes:

* ***Metodologías:***

El concepto de metodología en el mundo de la informática, se refiere a la acción de detallar, observar y evaluar las páginas Web, cumpliendo con una serie de normas diseñadas para esa área específicamente; la metodología OWASP es la más requerida en la actualidad.

***Metodologías OWASP***

Según esta metodología, comprende el OWASP Top 10 que corresponde a un documento de los diez riesgos de seguridad más importantes en aplicaciones web y por otra parte se deben tratar OWASP con (ASVS)

Dentro del OWASP Top 10 se encuentra el ítem 09 que trata del registro y monitoreo, en donde estos pueden ser desafiantes para ser testeados, implicando la realización de entrevistas o preguntando si los ataques fueron detectados durante las pruebas de penetración. No hay muchos datos de CVE/CVSS para esta categoría, pero realizar detecciones y responder a las brechas es crítico. Aún así, puede tener un gran impacto para la auditabilidad, visibilidad, alertas de incidentes y análisis forense. Esta categoría se expande más allá de CWE-117 Neutralización de salida incorrecta de registros, CWE-223 Omisión de información relevante para la seguridad, y CWE-532 Inserción de información sensible en archivo de registro.

En registros y monitoreo, las brechas no pueden ser detectadas. registros, detecciones, monitoreo y respuestas activas insuficientes pueden ocurrir en cualquier momento; por lo tanto se recomienda recoger información sobre los siguientes eventos, que se presentan a continuación: 

## Para prevenir a los desarrolladores, se deberían implementar algunos o todos los siguientes controles, dependiendo del riesgo de la aplicación:



* ***Normas***

Las normas son documentos que contienen directrices, características o en su defecto requisitos, que se deben tener en cuenta en la elaboración, diseño o utilización de productos, procesos y servicios, de modo que garantice la calidad del mismo. Con relación a esta finalidad, existen las normas ISO, las cuales son estándares internacionales que ayudan a las empresas a establecer criterios de homogeneidad frente a la gestión, prestación de servicios y desarrollo de productos en la industria.

La familia de normas ISO/IEC 27000 hacen parte del conjunto de estándares de seguridad (desarrollados o en fase de desarrollo) que proporcionan un marco para la gestión de la seguridad.

Contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La seguridad de la información, según la ISO 27001, se basa en la preservación de los siguientes conceptos:



En la tabla que se presenta a continuación, se encuentra un resumen de las Normas ISO 27000, *c*on su respectiva descripción:

**Tabla 1**

*Resumen de Normas ISO 27000*

| Norma | Descripción |
| --- | --- |
| ISO/IEC 27000 | Vocabulario estándar para el SGSI para todas las normas de la familia. Se encuentra en desarrollo actualmente. |
| ISO/IEC 27001 | Certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación de SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005. |
| ISO/IEC 27002 | *Information technology- Security techniques-Code of practice for information security management.* Previamente BS 7799 parte 1 y la norma ISO/IEC 17799. Es un código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2002 el 01 de julio de 2007. |
| ISO/IEC 27003 | Directrices para la implementación de un SGSI, es el soporte de la norma ISO/IEC 27001, publicada el 1 de febrero del 2010, no está certificada actualmente. |
| ISO/IEC 27004 | Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente. |
| ISO/IEC 27005 | Normativa dedicada exclusivamente a la gestión de riesgos de seguridad de la información, proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos en seguridad de la información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standar BS 7799 parte 3. Publicada en junio de 2008. |
| ISO/IEC 27006 | Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de seguridad de la información. Esta norma específica de requisitos para la certificación del SGSI es usada en conjunto con la norma 17021-1, la norma genérica de acreditación. |
| ISO/IEC 27007 | Guía para auditar al SGSI. Se encuentra en preparación. |
| ISO/IEC 27709:2008 | Guía para implementar ISO/IEC 27002 en la industria de la salud. |

A continuación, podrá ampliar la información sobre la Ley 1581 de 2012, la cual se constituye en el marco general de la norma de protección de los datos personales en Colombia:

| **Llamado a la acción**    **E**n el siguiente enlace de la página Web de Función Pública, podr**á** ampliar la información sobre la Ley 1581 de 2012, la cual se constituye en el marco general de la norma de protección de los datos personales en Colombia:  <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981> |
| --- |

* ***Estándares***

Continuando con la temática de Metodologías, Normas y Estándares, en este punto se hablará sobre este último, pero haciendo especial énfasis en el estándar OWASP Top 10 en conjunto con el estándar (ASVS) de OWASP. El Proyecto del Estándar de Verificación de Seguridad de Aplicaciones (ASVS) de OWASP proporciona una base para probar los controles técnicos de seguridad de las aplicaciones web y también proporciona a los desarrolladores una lista de requisitos para un desarrollo seguro.

El objetivo principal del Proyecto del Estándar de Verificación de Seguridad de Aplicaciones (ASVS) de OWASP es normalizar el rango en la cobertura y el nivel de rigor disponible en el mercado cuando se trata de realizar la verificación de seguridad de aplicaciones Web utilizando un estándar abierto comercialmente viable. El estándar proporciona una base para probar los controles de seguridad técnica de la aplicación, así como cualquier control de seguridad técnica en el entorno, en los que se confía para proteger contra vulnerabilidades como Cross-Site Scripting (XSS) e inyección de SQL. Este estándar se puede utilizar para establecer un nivel de confianza en la seguridad de las aplicaciones web.

La siguiente tabla muestra cuándo es apropiado utilizar el OWASP Top 10 unido al (ASVS) de OWASP.

**Tabla 2**

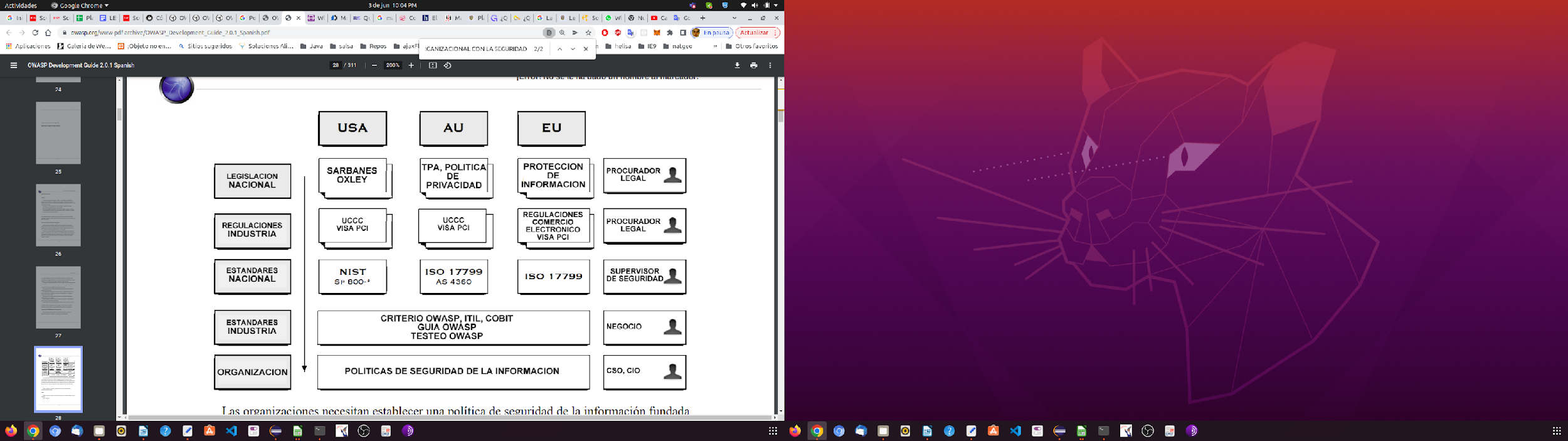
*Otros estándares COBIT e ISO 17799*

| Caso Uso | OWASP Top 10 2021 | Estándar de verificación en seguridad aplicaciones de OWASP (ASVS) |
| --- | --- | --- |
| Concientización | Sí |  |
| Capacitación | Nivel introductorio | Completo |
| Diseño y Arquitectura | Ocasionalmente | Sí |
| Estándar de codificación | Apenas mínimo | Sí |
| Revisión de código seguro | Apenas mínimo | Sí |
| Lista de verificación para la revisión por pares | Apenas mínimo | Sí |
| Pruebas unitarias | Ocasionalmente | Sí |
| Pruebas de integración | Ocasionalmente | Sí |
| Pruebas de penetración | Apenas mínimo | Sí |
| Soporte de herramientas | Apenas mínimo | Sí |
| Cadena de suministro de agua | Ocasionalmente | Sí |

Finalmente, en la siguiente figura se resume la aplicación de normas y estándares de una organización:

**Figura 1**

*Aplicación de normas y estándares de una organización*



**3. Políticas internas de una organización**

Aquellas organizaciones donde la seguridad cuenta con el soporte de la alta gerencia, generalmente desarrollarán y adquirirán aplicaciones que cumplen con principios básicos de seguridad. En cambio, es muy poco probable que organizaciones que no cuentan con el soporte de la gerencia, o que simplemente no se preocupan por la seguridad, desarrollen aplicaciones seguras. Cada organización segura documenta su apetito por el riesgo en su Política de Seguridad de la información, haciendo de esa manera que sea fácil determinar que riesgos serán aceptados, mitigados o asignados.

Las organizaciones inseguras simplemente no conocen donde se encuentra este límite, por lo tanto es probable que cuando se van a ejecutar proyectos dirigidos por este tipo de organizaciones y seleccionan los controles a implementar, estos terminan siendo inadecuados o insuficientes. La mayoría de las organizaciones produce políticas de Seguridad de la información derivadas de la ISO 17799 o del marco de trabajo COBIT, u ocasionalmente los dos o uno de los estándares. No hay una regla infalible o rápida que dicte cómo crear políticas de seguridad de la información, pero en general se debe tener en cuenta los siguientes aspectos:

* Si la organización cotiza en bolsa en la mayoría de los países, debe tener una política de seguridad de la información.
* Si la organización es propia pero posee cierto número de empleados y desarrolladores, probablemente necesite una política.



**4. Indicadores**

La creación de indicadores de gestión está orientada principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora.

Los objetivos de estos procesos de medición en seguridad de la información son:

1. Evaluar la efectividad de la implementación de los controles de seguridad.
2. Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
3. Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
4. Comunicar valores de seguridad al interior de la entidad.
5. Servir como insumos al plan de análisis y tratamiento de riesgos.

A continuación se profundizará sobre la temática de indicadores:



**5 Métricas**

Las métricas se encuentran divididas en seguridad, red, *software* y calidad, los cuales se describen a continuación:



1. **Herramientas de *software***

Las herramientas de *software* tienen el objetivo de facilitar, optimizar y mejorar el desempeño del trabajo realizado; estas herramientas ofrecen soluciones, las cuales se aplicar en diferentes áreas de una empresa y por tanto ayudan en el desarrollo de tareas desde las más complejas hasta las más simples.

El video a continuación habla de algunas herramientas, que le serán de utilidad en la implementación de aplicaciones web:



1. **Informe de monitoreo**

Con base en las métricas antes descritas ,se deben generar los formatos de indicadores para generar el informe de resultados; a continuación se ilustra un formato de presentación de indicador unido a los reportes generados desde las herramientas de *software.*

**Figura 2**

*Ejemplo de informe de monitoreo*

| INDICADOR 01-ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN | | | | | |
| --- | --- | --- | --- | --- | --- |
| IDENTIFICADOR | | | SGIN01 | | |
| DEFINICIÓN | | | | | |
| El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad. | | | | | |
| OBJETIVO | | | | | |
| Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección. | | | | | |
| TIPO DE INDICADOR | | | | | |
| Indicador de Gestión | | | | | |
| DESCRIPCIÓN DE VARIABLES | | FÓRMULA | | FUENTE DE INFORMACIÓN | |
| VISI01: Número de personas con su respectivo tol definió según el modelo de operación. Capítulo 2. | | (VISI01/VSI02)\*100 | | Capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información | |
| VISI02: Número de personas con su respectivo rol definido después de un año. | | Actas de asignación de personal | |
| METAS | | | | | |
| MÍNIMA | 75-80% | SATISFACTORIA | 80-90% | SOBRESALIENTE | 100% |
| OBSERVACIONES | | | | | |
| De acuerdo a lo establecido en el capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información, es necesario crear nuevos cargos y asignar responsabilidades en los actuales, por lo tanto, el indicador está enfocado, no solo a la contratación de nuevas personas, sino a la asignación de responsabilidades | | | | | |

1. **SÍNTESIS**

En el siguiente mapa conceptual se resumen los conceptos vistos en este componente formativo:



1. **ACTIVIDAD DIDÁCTICA**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la actividad | Identificar lo aprendido sobre Monitoreo |
| Objetivo de la actividad | Afianzar los conocimientos para monitorear la seguridad de aplicaciones web. |
| Tipo de actividad sugerida | Cuestionario |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo3\_ActividadDidactica1\_CF06 |

1. **MATERIAL COMPLEMENTARIO**

| **Tema** | **Referencia APA del Material** | **Tipo de material**  **(Video, capítulo de libro, artículo, otro)** | **Enlace del Recurso o**  **Archivo del documento o material** |
| --- | --- | --- | --- |
| Metodologías, normas y estándares | Caballero, A. [Alonso Caballero]. (2019, 31 de enero). Webinar Gratuito: Guía de Pruebas de OWASP [Video]. YouTube. <https://www.youtube.com/watch?v=kXfZqQY0rcg&ab_channel=AlonsoCaballer> | Video | <https://www.youtube.com/watch?v=kXfZqQY0rcg&ab_channel=AlonsoCaballer> |

1. **GLOSARIO**

| **TÉRMINO** | **SIGNIFICADO** |
| --- | --- |
| ASVS | Estándar de verificación de seguridad de aplicaciones. |
| CVE/CVSS | Vulnerabilidades y exposiciones comunes. |
| *Checklist* | Lista de chequeo qué sirve para registrar un proceso de auditoría. |
| OWASP | Open Web Application Security Project. |
| *Pentesting* | Proceso que imita posibles ataques a una red informática e intenta robar datos. |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

OWASP Top 10. (2021). A09 Fallas en el Registro y Monitoreo - OWASP Top 10:2021. <https://owasp.org/Top10/es/A09_2021-Security_Logging_and_Monitoring_Failures/>

Cec, N. (2020). ISO/IEC 27034: Estándar Internacional para la seguridad de las aplicaciones | noticias.cec.es.<https://noticias.cec.es/index.php/2020/03/20/isoiec-27034-estandar-internacional-para-la-seguridad-de-las-aplicaciones/>

Negocio, IPT. (2018). Indicadores de riesgo en la seguridad de datos. <https://www.informaticaparatunegocio.com/blog/indicadores-riesgo-la-seguridad-datos/>

Normas ISO. (2018). Normas ISO sobre gestión de seguridad de la información | Seguridadnformática.<http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.htm>

l

1. **CONTROL DEL DOCUMENTO**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** |
| --- | --- | --- | --- | --- |
| **Autor (es)** | Carlos Muñoz | Experto Temático | Regional Cauca - Centro de teleinformática y producción industrial. | Junio de 2022 |
| Paula Andrea Taborda Ortiz | Diseñadora Instruccional | Regional Norte de Santander - Centro de la Industria, la Empresa y Los Servicios CIES. | Julio de 2022 |
| Ana Catalina Córdoba Sus | Asesora Metodológica | Regional Distrito Capital – Centro de Diseño y Metrología. | Julio de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo de Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura. | Julio de 2022 |
| Sandra Patricia Hoyos Sepúlveda | Corrección de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Julio de 2022 |

1. **CONTROL DE CAMBIOS**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** | **Razón del** c**ambio** |
| --- | --- | --- | --- | --- | --- |