**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Caracterización de componentes en ciberseguridad |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501108 - Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501108-03 - Analizar los riesgos dentro de la organización de acuerdo con procesos, políticas, normas, protocolos y procedimientos internos de la organización. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | CF03 |
| NOMBRE DEL COMPONENTE FORMATIVO | Controles y estándares para el manejo de la seguridad de la información. |
| BREVE DESCRIPCIÓN | En este componente formativo se trabajarán las políticas para el manejo del riesgo y amenazas de seguridad, herramientas para la prevención y cuidado del uso del ciberespacio y el marco de trabajo de ciberseguridad NIST para la gestión de riesgos. |
| PALABRAS CLAVE | Ciberespacio, gestión, NIST, políticas de seguridad, prevención. |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | 6 - VENTAS Y SERVICIOS |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS**

**Introducción**

**1. Riesgo y estimación**

**2. Controles de seguridad en una red**

**3. Seguridad física y políticas de seguridad**

**4. Estándar ISO27001 y estándares para el manejo de la seguridad informática**

**5. Análisis de riesgo y recuperación de desastres**

**Síntesis**

1. **INTRODUCCIÓN**

El componente formativo «Controles y estándares para el manejo de la seguridad de la información» pretende brindar los conocimientos iniciales para realizar una adecuada comprensión sobre los diferentes riesgos y una estimación de estos. El siguiente video expone cada una de las temáticas a desarrollar y su importancia en esta área:

CF03\_Video\_introductorio

1. **DESARROLLO DE CONTENIDOS**

**1. Riesgo y estimación**

En la actualidad el riesgo informático se ha convertido en uno de los temas de mayor conversación a lo largo del mundo, puesto que en tiempos actuales ha generado pánico entre la comunidad internacional. Por ejemplo, se han escuchado de ataques informáticos tales como *Ransomware*, que han desatado la pérdida de millones de dólares a empresas y particulares.

|  |  |
| --- | --- |
|  | Esta realidad lleva a reflexionar que los riesgos están presentes y llegaron para quedarse. No obstante, este tipo de comportamiento ha cambiado a lo largo de los tiempos, ya que los ataques son cada vez más directos y dañinos. |

El riesgo latente es la carencia de seguridad o de tranquilidad que no permite el correcto funcionamiento de los procesos empresariales y personales a lo largo del mundo. De ahí que las compañías hoy día invierten cantidades considerables de millones de dólares para minimizar los riesgos a los cuales están expuestos todos los días.

|  |  |
| --- | --- |
|  |  |
| Cabe decir que la seguridad es una disciplina de constante evolución y permanencia; en otras palabras, es una actividad que se debe realizar de manera continua y permanente para mitigar los problemas y riesgos que se pueden presentar todos los días en contra de la infraestructura de las empresas. | |

Pero bueno, ¿qué se entiende por riesgo y estimación?, a continuación se conocerá un poco de ello:

CF03\_1\_Interactivo\_riesgo y estimación

|  |
| --- |
| Aunque la estimación no es precisa en la mayoría de las ocasiones es importante aclarar que puede ser una herramienta que acompaña al diagnóstico de la infraestructura, ya que se puede predecir, de acuerdo a información de diversas fuentes, un suceso a ocurrir. En la mayoría de los casos, la estimación es utilizada para medir la gravedad del impacto de un ataque y de esta manera determinar el plan de contingencia si este llega a ocurrir. |

El riesgo y la estimación van acompañados, ya que ambos impactan los planes de contingencia y de recuperación de la empresa. La siguiente figura 1 expone la importancia de este balance.

**Figura 1**

*El riesgo y la estimación*

CF03\_1\_Infografía\_riesgo y estimación

La matriz de riesgo es una herramienta que permite establecer cuáles son las amenazas y cuánto es el valor que las coloca en un rango de mayor prioridad. Por ejemplo, un ataque por virus es muy diferente a un ataque de *ransomware*, pues el impacto que este generaría es diferente y la mitigación y manera de prevenirlo es totalmente distinta; para este caso particular se debe tener en cuenta la categorización de impacto: bajo, medio y alto, dependiendo del daño que pueda ocasionar y qué tanto puede hacer que el negocio se detenga, tal como se observa en el ejemplo de la figura 2:

**Figura 2**

*Matriz de riesgo*

CF03\_1\_Gráfico\_matriz de riesgo

|  |  |
| --- | --- |
| Para recordar | La relación que existe entre el riesgo y la estimación siempre será uno de los pilares relevantes de toda empresa, puesto que involucra a todo el personal, como aquellos que deben velar por la seguridad y la información de la misma. |

**2. Controles de seguridad en una red**

|  |  |
| --- | --- |
| La seguridad, como ya se ha evidenciado, es un factor importante en las empresas y organizaciones, y por tanto conlleva una gran responsabilidad, junto con los métodos y procesos que se deben seguir para lograr establecer un nivel óptimo que permita garantizar la seguridad e integridad de la información.  Hoy día existen muchas herramientas que ayudan a realizar este proceso de una manera adecuada. Algunas de ellas se abordan a continuación: |  |

CF03\_2\_acordeon\_herramientas

Uno de los aspectos a tener en cuenta al momento de la implementación o adquisición de estos elementos es la cantidad de usuarios que utilizan estos dispositivos, sobre todo en la solución de *hardware y software*, la cantidad de datos que estos producirán y cómo será el proceso de respaldo de esta información; puesto que es importante no solo pensar en la implementación sino cómo estos nuevos datos deben ser tratados y manipulados.

De igual forma, la manera en la que se establecerá la comunicación entre dos o más equipos en una red también es fundamental. El modelo de referencia OSI refleja los protocolos y fases en las cuales se establece dicha interacción entre las computadoras. Es la referencia en donde se puede observar la transformación de la información, pues cada capa de este modelo realiza su aporte a la comunicación y con base en este estándar se crean las reglas para establecer dicho proceso. Siguiendo esta línea, a continuación, se detalla cada una:

CF03\_2\_interactivo\_modelo OSI

|  |  |
| --- | --- |
| Para recordar | Aunque se han precisado diferentes mecanismos para la seguridad en redes, es importante destacar que la protección de la información y el correcto uso de los sistemas informáticos de una empresa dependen de la cultura informática y de seguridad de las personas que allí laboran, pues son ellas quienes interactúan con estos elementos de la empresa y deben estar siempre alerta y al tanto de todo. |

**3. Seguridad física y políticas de seguridad**

La **seguridad física** es uno de los aspectos fundamentales en una organización. Esta permite crear los mecanismos de barrera para salvaguardar los activos de la misma; sabiendo esto, a continuación, se precisan algunos conceptos en la figura 3:

**Figura 3**

*Conceptos de mecanismos de seguridad*

CF03\_3\_Infografía\_conceptos

|  |  |
| --- | --- |
|  |  |
| Como se puede apreciar la seguridad física se encarga de velar por los controles físicos establecidos para prevenir la intrusión o vulnerabilidades de la infraestructura de una organización. En estos elementos se pueden consagrar dispositivos, personas y toda medida que permita asegurar los bienes de la organización. | |

Existen muchos aspectos a considerar con respecto a la seguridad física, la cual como se ha expresado, es un conjunto de medidas que permiten garantizar el acceso y control de los lugares de la empresa. Si se explora un poco sobre algunos de estos, se verá que estas medidas van desde la instalación de cámaras de seguridad, sensores, tarjetas inteligentes hasta lectores de huella.

|  |
| --- |
| Guardia de seguridad registra a los pasajeros de pie en la cola Foto gratis |
| En este aspecto, cabe decir, que estas medidas, a pesar de contener componentes tecnológicos, también se hace presente el factor humano, es decir: un celador o guarda de seguridad; por ejemplo, que interactúa en la infraestructura de la empresa como un componente de seguridad y que también toma un valor importante en la misma. |

Ahora bien, por otra parte, también se encuentran **las políticas de seguridad** como un factor primordial y complementario a la seguridad física. Son aspectos que se deben tener en cuenta para el cumplimiento de normas y estatutos orientados a la preservación de los datos e información de una empresa, aunque de igual manera, se debe tener en cuenta que los activos físicos de la compañía se deben proteger en ese mismo sentido.

|  |  |
| --- | --- |
| Personas que participan en eventos de negocios. Foto gratis | Las políticas son implementadas para dar cumplimiento a los procesos misionales de la organización; es decir, deben estar conectados con la misión de la empresa y sirven de apoyo para lograrlo de una manera adecuada y sin ningún percance. |

De todos los procesos que se llevan a cabo en la organización, el establecer políticas es uno de los más complejos puesto que cada usuario dentro de su proceso quiere tener autonomía en lo que realiza dentro de la empresa. Se puede ver a continuación algunos de esos mecanismos de políticas de seguridad que se implementan en las organizaciones:

CF03\_3\_gráfico interactivo\_políticas

Lo anterior refleja el panorama genérico de la importancia de establecer políticas de seguridad que garanticen el correcto funcionamiento de los elementos de tecnología de una organización.

|  |  |
| --- | --- |
| Para recordar | La definición de una adecuada política minimiza el riesgo de comprometer la información y los datos que se ingresan y procesan en un sistema de información. La seguridad física de una organización, por su parte, no solo son elementos tecnológicos sino que también involucra el personal responsable de asegurar y resguardar la información. |

**4. Estándar ISO 27001 y estándares para el manejo de la seguridad informática**

El estándar ISO 27001 es una norma para el aseguramiento de la seguridad de la información en una organización, en el cual se encuentran todos los lineamientos para su almacenamiento, mantenimiento, confidencialidad y uso. Este estándar es muy importante en las organizaciones y es exigido a las empresas para certificar el uso que le dan a los datos e información que estas manipulan.

El propósito de este estándar es garantizar el acceso y protección de la información de acuerdo con los lineamientos establecidos en este mismo estándar. En otras palabras, debe generar confianza y proveer los mecanismos de acceso y tratamiento de la información almacenada. Para ello, se establecen los siguientes riesgos que se pueden revisar en la figura 4:

**Figura 4**

*Tipos de riesgos*

CF03\_4\_Gráfico\_tipos de riesgos

Por su parte, el ciclo PHVA cumple con un propósito específico para la aplicación de la norma ISO 27001. Consiste en brindar los procesos que se deben seguir y su interrelación; es decir, garantiza la continuidad de los procesos establecidos en la norma ISO 27001 y aplica los enfoques de la mejora continua para cada uno de sus procesos (ver figura 5).

**Figura 5**

*Ciclo PHVA*

CF03\_4\_Gráfico\_ciclo PHVA

Ahora bien, así como cualquier norma o estándar establecido, la ISO 27001 debe cumplir con unos procesos o cláusulas que garanticen la aplicabilidad de los procesos dentro de la organización. A continuación, se detalla cada una de ellas:

CF03\_4\_pestañas\_clausulas 1-4

En la cláusula Contexto de la organización, como se mencionó, se deben tener en cuenta los aspectos tanto internos como externos de una empresa, tal como se presenta a continuación en la figura 6:

**Figura 6**

*Aspectos de una organización*

CF03\_4\_Infografía interactiva\_aspectos de una organización

Se continua con la explicación de las cláusulas.

CF03\_4\_pestañas\_clausulas 5-7

En la cláusula 7, también se debe establecer qué información se requiere para la implementación del sistema de gestión de la información, la cual debe ser precisa, entendible para los involucrados en el proceso y apoyada en aspectos legales de la organización. Otros aspectos para tener en cuenta ya garantizar frente a este tema, se aprecian en la figura 7:

**Figura 7**

*Aspectos a garantizar*

CF03\_4\_Infografía\_aspectos a garantizar

Finalmente, se describen las últimas cláusulas.

CF03\_4\_pestañas\_clausulas 8-10

|  |  |
| --- | --- |
| Para recordar | La norma ISO 27001, junto con sus cláusulas, permite establecer los lineamientos para realizar una correcta administración de los sistemas y del personal encargado de manipularlos. |

**5. Análisis de riesgo y recuperación de desastres**

Se denomina desastre a cualquier evento que sucede de manera repentina y que ocasiona que los procesos que realiza una organización se detengan por completo; esto implica toda actividad, sea de índole económica o social. En el caso específico de la seguridad de la información son sucesos que afectan el correcto funcionamiento hasta llegar a la interrupción de la disponibilidad de los servicios informáticos.

El plan de recuperación de desastres, también denominado DRP, por sus siglas en inglés, es un mecanismo para establecer la prioridad de los eventos causados y la responsabilidad que esto implica en la organización.

|  |  |
| --- | --- |
|  | Los planes de recuperación de desastres establecen procedimientos y métricas para analizar los posibles desastres y cómo se puede recuperar el sistema después de ocurridos estos eventos, dentro de los cuales pueden existir causas que no son predecibles en momentos determinados como son los desastres naturales. |

Como en toda organización deben existir responsables de los procesos que se llevan a cabo. El caso de la recuperación de desastres no es la excepción a la regla, de hecho en este proceso no solo se debe establecer **el grupo de responsables**, quienes deben velar porque los planes de recuperación funcionen, sino que deben establecer un **comité específico para su vigilancia y supervisión**. Este comité está en la facultad de determinar la validez del plan de recuperación de desastres con base en la evaluación de incidentes presentados o que pueden llegar a presentarse. Adicional a ello, se establece la aprobación para la adquisición de recursos que pueden ser tecnológicos o humanos para velar por el cumplimiento y ejecución del plan de recuperación de desastres.

Cada grupo tiene a su cargo la implementación del plan de recuperación de desastres de acuerdo con las responsabilidades establecidas y equivalentes a los tiempos de respuesta establecidos para el cumplimiento de los planes, tal como se expone en la siguiente figura 8:

**Figura 8**

*Responsabilidades de los responsables*

CF03\_5\_gráfico\_responsables

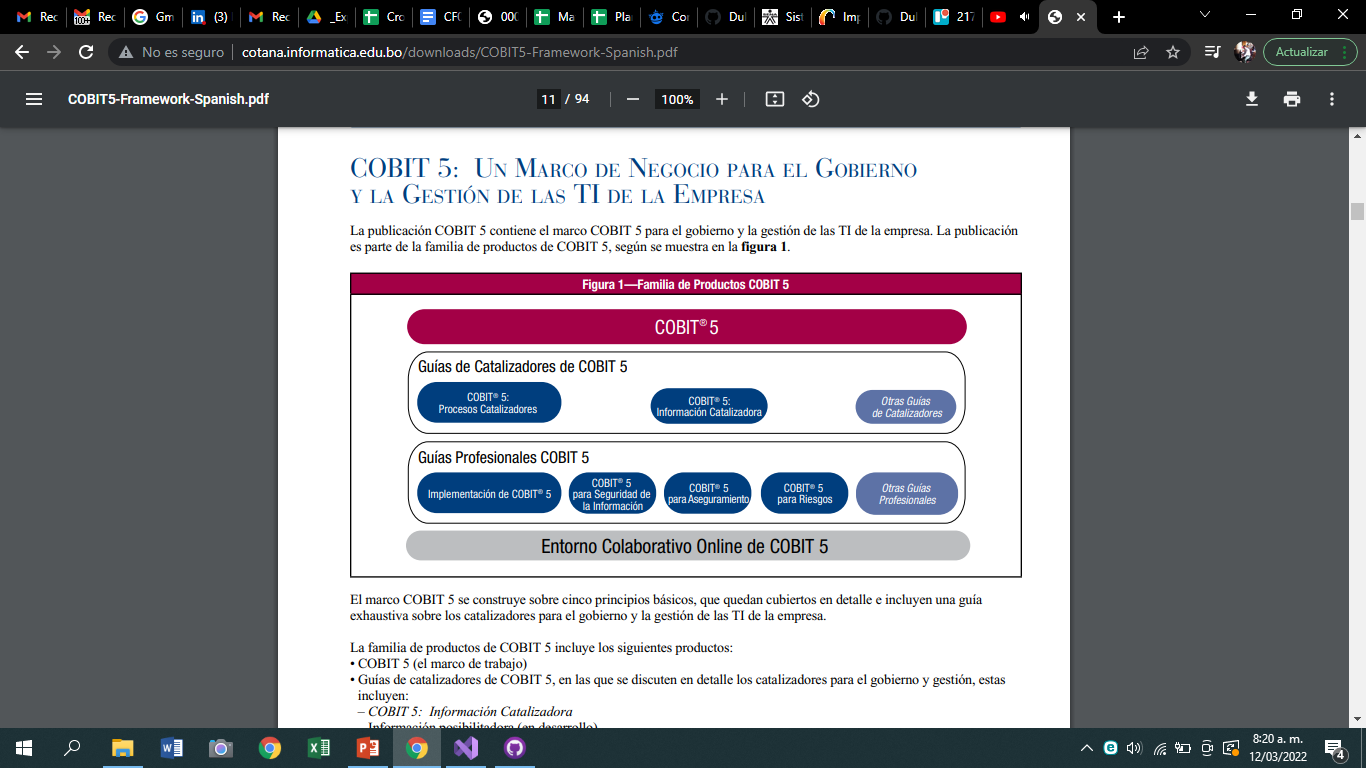
Cabe destacar que la implementación de un plan de recuperación de desastres contiene varios aspectos para tener en cuenta, a continuación se pueden conocer:

CF03\_5\_acordeon\_aspectos DRP

Ahora bien, para la gestión de todos esos procesos se encuentra lo que se conoce como Cobit, el cual es un marco de trabajo establecido para garantizar el gobierno de tecnología a través del establecimiento de guías y procesos que aseguren un correcto manejo de la información en las organizaciones (ver figura 10).

**Figura 10**

*Entorno Cobit*

****

Nota. Tomado de ISACA (s.f.).

Ya sabiendo lo anterior, es preciso saber que Cobit comprende cinco principios de trabajo que estipulan la manera en cómo interactúan los procesos dentro de una organización. A continuación se pueden reconocer:

CF03\_5\_tarjetas\_principios

Cabe destacar que Cobit es válido en su aplicación para cualquier organización teniendo grandes beneficios en la optimización de procesos y mejorando los niveles de riesgo de los recursos tecnológicos. Es una herramienta esencial para el gobierno de tecnología en una organización, ya que este entrega las guías que se deben tener en cuenta para realizar un proceso de gestión de la tecnología y la información de manera adecuada, permitiendo, además, que la infraestructura como la información funcionen de una manera armónica.

|  |  |
| --- | --- |
|  |  |
| Los principios de Cobit son aplicados independientemente del tamaño de la organización y genera cultura organizacional y buenas prácticas en la organización. | |

1. **SÍNTESIS**

Se ha llegado al final de este componente. A continuación, conozca una gráfica que sintetiza las temáticas desarrolladas:

*Síntesis*

CF03\_gráfico\_síntesis

1. **ACTIVIDADES DIDÁCTICAS**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | Seguridad de la información |
| Objetivo de la actividad | Validar conocimientos y conceptos aprendidos en el componente. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | *Formatos DI: CF03\_Actividad didáctica* |

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 |
| 3. Seguridad física y políticas de seguridad | Presidencia de la República. (2020). Manual de políticas de seguridad de la información. https://dapre.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Politicas-Seguridad-Informacion.pdf | Manual | <https://dapre.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Politicas-Seguridad-Informacion.pdf> |
| 4. Estándar ISO27001 y estándares para el manejo de la seguridad informática | NQA. (s.f.). *ISO 27001:2013.* *Guía de implantación para la seguridad de la información.* <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf> | Guía | <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf> |
| 4. Estándar ISO27001 y estándares para el manejo de la seguridad informática | Jiménez, A. & Salazar, L. X. (2016). *Análisis de riesgos, amenazas y vulnerabilidades de la Compañía pinzón pinzón & asociados en su área de TI.* [Trabajo de grado, Ingeniería de Sistemas Universidad Piloto de Colombia]. <http://polux.unipiloto.edu.co:8080/00003291.pdf> | Trabajo de grado | <http://polux.unipiloto.edu.co:8080/00003291.pdf> |
| 4. Estándar ISO27001 y estándares para el manejo de la seguridad informática | CRA. (2009). Norma NTC-ISO/IEC 27001 Sistema de gestión de seguridad de información. https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena\_virtualprovpro4403&vid=SENA&search\_scope=sena\_completo&tab=sena\_completo&lang=es\_ES&context=L | Libro | <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_virtualprovpro4403&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L> |
| 4. Estándar ISO27001 y estándares para el manejo de la seguridad informática | Merino Bada, C. & Cañizares Sales, R. (2011). *Implantación de un sistema de gestión de seguridad de la información según ISO 27001: un enfoque práctico.* Fundación Confemetal. <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_aleph000069696&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L> | Libro | <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_aleph000069696&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L> |
| 5. Análisis de riesgo y recuperación de desastres | ESAP. (2018). *Plan de recuperación de desastres*. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Recuperaci%C3%B3n-de-Desastres-v1.pdf | Documento | <https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Recuperaci%C3%B3n-de-Desastres-v1.pdf> |
| 5. Análisis de riesgo y recuperación de desastres | ISACA. (s.f.). *Cobit 5. http://cotana.informatica.edu.bo/downloads/COBIT5-Framework-Spanish.pdf* | Documento | <http://cotana.informatica.edu.bo/downloads/COBIT5-Framework-Spanish.pdf> |

1. **GLOSARIO**

|  |  |
| --- | --- |
| Término | Significado |
| Cobit | Es un estándar de buenas prácticas para generar cultura organizacional y administrar los procesos que involucren tecnología, personas y procesos. |
| Contingencia | Componente que se establece cuando se generan situaciones de riesgo que pueden colocar en peligro la información o procesos de una organización. |
| ISO 27001 | Es un estándar que permite la administración de la tecnología y los procesos que conlleva el aseguramiento de la seguridad de la información. |
| Modelo OSI | Es un estándar establecido para la comunicación entre dispositivos en todo el mundo. |
| PHVA | Es un enfoque de trabajo que permite gestionar procesos empresariales y realizar procesos de mejora continua. |
| Planificación | Es la manera como se debe estructurar la ruta de trabajo para que los procesos en una organización funcionen de manera correcta. |
| Riesgo | Posibilidad de que suceda un inconveniente que no permita el correcto funcionamiento del sistema. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

ESAP. (2018). *Plan de recuperación de desastres*. <https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Recuperaci%C3%B3n-de-Desastres-v1.pdf>

ISACA. (s.f.). *Cobit 5.* <http://cotana.informatica.edu.bo/downloads/COBIT5-Framework-Spanish.pdf>

NQA. (s.f.). *ISO 27001:2013*. *Guía de implantación para la seguridad de la información.* <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Dulfran Antonio Montaño Montaño | Experto Temático | Regional Distrito Capital - Centro de Diseño y Metrología | Marzo 2022 |
| Miroslava González Hernández | Diseñadora y Evaluadora Instruccional | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Marzo 2022 |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Regional Distrito Capital - Centro de Diseño y Metrología | Marzo 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Marzo 2022 |
| Jhon Jairo Rodríguez Pérez | Diseñador y evaluador instruccional | Regional Distrito Capital - Centro de Diseño y Metrología | Marzo 2022 |

1. **CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| Autor (es) |  |  |  |  |  |