Diseño y documentación de controles de ciberseguridad

Breve descripción:

Mediante el estudio consciente de este componente, el aprendiz estará en capacidad suficiente para preparar las distintas estrategias de ciberseguridad y seguridad de la información, a la vez que podrá elaborar eficazmente la hoja de ruta, de acuerdo con los controles requeridos y los tipos de documentación.

Noviembre 2023

Grupo de Ejecución de la Formación Virtual

Tabla de contenido

Introducción

En la actualidad, la ciberseguridad y la seguridad de la información han adquirido gran importancia en las organizaciones, lo que conlleva que se desarrollen documentos y directrices que orienten el uso adecuado de tecnologías, favoreciendo así la relativa integridad tanto de la información como de las acciones y desarrollos que tiene lugar en el ciberespacio.

Teniendo en cuenta la importancia de la ciberseguridad en el desarrollo de las actividades de las personas en general, y con mayor razón de las organizaciones, se ha buscado mantener la seguridad de la misma, mediante la traza de estrategias de ciberseguridad y en concordancia con los controles requeridos.

La elaboración de hojas de ruta de las estrategias y documentación de las mismas, es un aspecto característico y necesario, ya que esto contribuye, en buena medida, a la integridad y disponibilidad de la información ante descuidos de los usuarios, ante ataques informáticos e, incluso, frente a desastres de orden natural.

1. Diseño de controles de seguridad

En este contexto de la ciberseguridad, se entiende por controles todas aquellas acciones, medidas o procesos que buscan asegurar el desarrollo normal del ciberespacio o del manejo de los equipos e información dentro de la organización.

El diseño de los controles ayuda a preparar las estrategias de ciberseguridad elaborando una hoja de ruta de acuerdo con normas y documentos requeridos ya establecidos.

Otros aspectos importantes de los controles de seguridad son:

A. **Madurez y capacidad de los sistemas**

   Ayudan a trazar las estrategias para descubrir un camino que permita a la organización alcanzar el estado de madurez y capacidad deseado en todo lo que tiene que ver con seguridad digital.

B. **Responsabilidad del diseño de controles**

   En la organización, quien se encarga de diseñar dichos controles es la oficina de Tecnologías de la Información (TI) o, en su defecto, una persona experta en seguridad que haya sido contratada para tal fin.

C. **Jefatura de sistemas**

   En la mayoría de los casos, cuando la organización cuenta con la posibilidad de tener personal propio para esos propósitos, quien establece el diseño de controles es quien hace las veces de jefe o jefa de sistemas.

2. Pasos para el diseño de controles de seguridad

Para el estudio y profundización de los contenidos de este componente formativo, es importante una previa comprensión y adopción de la guía técnica denominada G.ES.05 (sobre el diseño y las formas de ejecución e implementación de un plan de seguridad de la información), propuesta por MinTIC, con el fin de establecer dicho plan o estrategia.

A continuación, se muestran los pasos y requerimientos clave, indicados por la guía técnica G.ES.05. Se recomienda prestar mucha atención para comprenderlos, asimilarlos y tomar nota atenta de ellos:

- **Paso 1:**

  Identificación del estado actual

  Basado en la clasificación de los activos de información, identifica el estado actual de capacidad o madurez del proceso de seguridad de la información de la compañía u organización.

- **Paso 2:**

  Definición de los objetivos

  Es clave tener en cuenta objetivos establecidos, ya que esto favorece el trazo e implementación de la estrategia de seguridad de la información, según la ISO/IEC 27001-2013.

- **Paso 3:**

  Determinación del estado deseado

  Tener en cuenta el nivel del estado que se desea alcanzar, por medio de llevar a cabo la estrategia de seguridad digital en la organización, partiendo del estado o nivel actual.

- **Paso 4:**

  Determinación del nivel de riesgo aceptable

  Definir el nivel de riesgo aceptable de la seguridad digital que se tendrá en cuenta en la estrategia, con base en la necesidad de riesgo de la organización.

- **Paso 5:**

  Definición y ejecución del plan de acción

  Fijar la hoja de ruta para lograr el estado deseado de la estrategia, teniendo en cuenta personas, tecnologías y procesos, entre otros recursos.

Configuración de pasos para el diseño de controles

Cada paso requerido para lograr el diseño de los controles de seguridad cuenta con una tríada de elementos constitutivos:

Entradas / Salidas / Actividades

2.1. Entradas y salidas

Se entiende como una entrada aquel o aquellos elementos ya existentes que serán de gran utilidad para instalar el paso. Se trata de elementos que ya tiene la organización en su haber y en su quehacer y que **favorecen la instauración de cualquiera de los cinco pasos** para cumplir con el diseño del plan de controles de seguridad.

En esta misma línea, están las salidas. Cuando se habla de salidas, se está haciendo referencia a las herramientas de registro o de documentación que se tendrán luego de haber analizado, ajustado o intervenido los documentos o registros ya

existentes relacionados con objetivos, planes de acción, estados de ciberseguridad de la compañía o clasificación de los activos de información, entre otros.

En términos más concretos, las salidas son aquellas herramientas documentales o de registro, que se dejan actualizadas luego de otra anterior.

Ambos elementos, entradas y salidas, son parte de la configuración de los pasos que se siguen para el diseño de los controles de seguridad.

2.2. Actividades

Los pasos que se siguen para el diseño de los controles de seguridad, además de estar estructurados y orientados por las **entradas** y las **salidas**, requieren el cumplimiento de algunas acciones o actividades, según el paso, que darán sentido, cumplimiento y efectividad a cada paso y, en consecuencia, a los controles.

El desarrollo de esas actividades deberá contemplar tiempos, responsables, herramientas, entradas y salidas de cada paso, propósitos de cada paso e intención de cada control.

2.3. Paso uno: identificación del estado actual

Este procedimiento es el primero de los pasos para el diseño de los controles de seguridad y está basado en la clasificación de los activos de información. Con este, se identifica el estado actual de capacidad o madurez que tiene el proceso de seguridad de la información en la organización.

A continuación, la estructuración de este primer paso, con sus respectivas entradas, salidas y actividades:

- **Entradas**

  La identificación del estado actual cuenta con entradas, como los inventarios de los activos de información y/o la metodología evaluativa y de categorización de tales activos de información.

- **Salidas**

  Algunas salidas de este paso son los activos de información ya categorizados o clasificados, incluyendo elementos como criticidad y sensibilidad, también la meta implantada de seguridad digital o el estado presente de la seguridad informática en la empresa u organización.

- **Algunas actividades**

  - ✓ Fijar el estado presente de la seguridad informática o digital.
  - ✓ Valuación y análisis de madurez o de capacidad del proceso de seguridad digital.
  - ✓ Establecer los activos de información y hacer su respectiva valoración, cuantitativa y cualitativa.
  - ✓ Clasificar los activos informáticos teniendo como base el nivel de criticidad y, por supuesto, el nivel de sensibilidad.

2.4. Paso dos: definición de los objetivos

Se trata del segundo de los pasos para cumplir con el diseño de los controles de seguridad dentro de la organización y, con él, se han de tener en cuenta los objetivos establecidos para trazar e implementar la estrategia de seguridad de la información, con el debido cumplimiento de los criterios establecidos por la normativa. No olvide que la norma vigente y sobre la cual estamos haciendo énfasis en este componente formativo es la **ISO/IEC 27001-2013**.

Profundice en las entradas, salidas y actividades de este segundo paso en la información que, a continuación, se presenta:

I. Entradas

Algunas entradas de este paso son: el plan estratégico de la compañía, el inventario de los activos de información ya categorizados, las metas establecidas con respecto a la seguridad digital, la determinación de negocio y/o medios tecnológicos que afectan el logro de objetivos, el compendio de normas y estatutos o leyes, decretos, etc., que regulan la clasificación de información.

Otras entradas importantes de este paso son:

- ✓ **Las inspecciones o controles, entre los que es posible enunciar:** de accesos, sistemas de descubrimiento o detección de intrusos, etc.
- ✓ **Las contramedidas:** se trata de aquellos mecanismos de control o de inspección que son implementados para dar respuestas específicas a las distintas amenazas; podrían ser de orden preventivo, de detección o de carácter correctivo.

II. Salidas

En este caso, las salidas más destacadas son los objetivos establecidos de la estrategia misma.

III. Algunas actividades

- ✓ Determinar los objetivos de alineación estratégica: el cumplimiento de estos permite ajustar los objetivos de seguridad informática con los de la organización.

- ✓ Determinar los objetivos de gestión de riesgos: el logro de estos objetivos es la implementación de medidas para mitigar riesgos y reducir el posible impacto.
- ✓ Determinar los objetivos de entrega de valor: su función es permitir la optimización de las inversiones en cuanto a la seguridad informática, apoyando los objetivos de la organización.

Otras actividades de suma importancia

- ✓ Determinar los objetivos de gestión de recursos: su función es permitir la utilización del conocimiento y la infraestructura de seguridad digital con eficiencia y efectividad.
- ✓ Determinar los objetivos de medición del desempeño: la finalidad de cumplir estos objetivos debe posibilitar monitorear y reportar todos los procesos de la seguridad digital.

2.5. Paso tres: determinación del estado deseado

Determinar el estado de seguridad que se desea alcanzar es el tercer paso que se sigue en el diseño de controles de seguridad. En este paso, hay que tener en cuenta el nivel del estado que se desea alcanzar con la aplicación y desarrollo de la estrategia de seguridad digital de la organización. Desde luego, este paso debe contemplar también el estado actual y partir de él.

Entérese, a continuación, de las entradas, salidas y actividades que estructuran este tercer paso en el diseño de controles de seguridad:

a. **Entradas**

Algunas entradas para la determinación del estado deseado son: los objetivos de la estrategia de seguridad digital ya establecidos, el estado actual del proceso de seguridad digital y los estándares y/o mejores prácticas, como, por ejemplo, la ISO 27001:2013 y la ISO 27002:2013.

b. **Salidas**

En la determinación del estado deseado, una salida necesaria es, justamente, la mirada al estado deseado. Ha de ser una herramienta organizada y en correspondencia lógica con el actual.

c. **Actividades**

- ✓ Determinar el estado deseado del proceso de seguridad digital dentro de la organización, en términos cualitativos de atributos, resultados y características.
- ✓ Reconocer el nivel de madurez deseado.
- ✓ Definir, de la mano de la alta gerencia de la organización, el nivel de madurez deseado, determinando el proceso para que cumpla con sus objetivos y satisfaga las necesidades de la organización.

Para ampliar su saber sobre otros estándares que contribuyen en la determinación del estado deseado, se recomienda revisar el siguiente material: CMMI, COBIT, ITIL. ISO/IEC 20000 y COSO, el cual puede encontrar en:

https://www.globalbit.co/2019/07/22/modelo-cmmi-calidad-y-buenas-practicas-en-el-desarrollo-de-software/

https://www.emagister.com/blog/que-es-itil/

https://www.globalsuitesolutions.com/es/que-es-modelo-coso/

2.6. Paso cuatro: determinación del nivel de riesgo aceptable

Se trata del cuarto paso en el diseño de controles de seguridad y consiste en definir el nivel de riesgo máximo que la organización considera aceptable en lo referente a la seguridad digital. Este nivel de riesgo aceptable se tendrá en cuenta en la estrategia, con base en la necesidad de riesgo de la organización.

- **Entradas**
  - Objetivos de la estrategia ya establecidos.
  - Estado actual del proceso de seguridad digital.
  - Estado deseado del proceso de seguridad digital.
  - Necesidad de riesgo de la organización: es de suma importancia que la alta dirección de una organización establezca y formalice su necesidad de riesgo. Esta necesidad de riesgo hace referencia al riesgo que una organización está dispuesta a afrontar para lograr sus objetivos.
  - Metodología de gestión de riesgos.
- **Salidas**
  - Niveles de riesgo admisibles.
  - Mapa de riesgos de TI.
  - Estrategia actualizada y/o ajustada de la seguridad de la información.

- **Actividades**

- Determinar la necesidad de riesgo de la organización: es el riesgo que la organización está dispuesta a correr por obtener beneficios.
- Establecer el nivel de riesgo aceptable para la seguridad digital: con base en este nivel de riesgo es posible, entonces, realizar la gestión de todos los riesgos que se asocian con el proceso de seguridad digital o de información.
- Adaptar una metodología de gestión de riesgos a la organización: con la finalidad de determinar sus riesgos e impedir, lo más posible, la materialización de tales riesgos, iniciar su tratamiento.
- Dirigir la estrategia de gestión de los riesgos críticos que hayan sido hallados.

2.7. Paso cinco: definición y ejecución del plan de acción

Como quinto paso en el diseño de controles de seguridad, se encuentra la definición y ejecución del plan de acción. Se trata de fijar la hoja de ruta para lograr el estado deseado de la estrategia, teniendo en cuenta personas, tecnologías y procesos, entre otros recursos.

Se presentan ahora las entradas, salidas y actividades que estructuran el paso de definición y ejecución del plan de acción:

1) **Entradas**

   Son entradas de la definición y ejecución del plan de acción: los objetivos establecidos en la estrategia, la situación o estado actual del proceso de seguridad digital, la situación o estado deseados del proceso de seguridad digital y, desde luego, los activos de Información.

2) Salidas

- ✓ La agenda u hoja de ruta correspondiente al mismo plan de trabajo en pos de la instauración de la seguridad digital, por medio de la cual se da prevalencia al conjunto de iniciativas por aplicar para clausurar la brecha y lograr el nivel o estado deseado.
- ✓ Bitácora o plan de uso y apropiación de la estrategia.
- ✓ Métricas y mecanismos de monitoreo de la estrategia.

3) Actividades

- ✓ Evaluar, para cada una de las acciones determinadas en la estrategia, recursos solicitados y el costo para su ejecución.
- ✓ Para la cuantificación, se pueden adoptar lineamientos sugeridos por la normatividad vigente, antes mencionada, adoptando el modelo de seguridad y privacidad de la información.
- ✓ Identificar limitaciones.

¡Importante!

La actividad **"Identificar limitaciones"** supone que estas pueden ser:

- ✓ Éticas
- ✓ Personales
- ✓ Culturales
- ✓ De costos
- ✓ De estructura organizacional
- ✓ De tolerancia al riesgo
- ✓ De capacidades
- ✓ De recursos
- ✓ Físicas

- ✓ Legales

3. Controles: características

La estrategia de ciberseguridad y seguridad de la información de una organización ha de encaminarse y enfocarse en lograr la construcción de un ciberespacio seguro y resistente, que se alcanza, entre otras maneras, trazando las estrategias de acuerdo con los controles requeridos y, como se ha dicho ya, elaborando una hoja de ruta para mejorar el nivel de la ciberseguridad.

En ese sentido, los controles de seguridad pueden caracterizarse con tres atributos constitutivos, que se presentan a continuación:

- **Prevenir errores:** el carácter preventivo de los controles otorga al plan de seguridad un enfoque que favorece la intervención de los riesgos, antes de que estos se materialicen o, como es de esperarse, previniendo que estos sucedan con el mismo rigor y afectación que si no se previeran.
- **Detectar errores:** es, básicamente, lograr ampliar el espectro de seguridad de los sistemas de información y, por tanto, generar con más acierto, en tiempo y forma, los mecanismos de intervención y atención a la materialización de los riesgos y/o errores detectados.
- **Corregir errores:** la corrección de errores se presume como una acción necesaria cuando la prevención y la detección no han sido suficientes o no se han aplicado con el cuidado justo y pertinente. La corrección de los errores, siempre ofrecerá la posibilidad de generar

mecanismos o acciones de prevención para nuevos riesgos o errores potenciales.

4. Recomendaciones importantes sobre controles

Después de identificar el **"estado actual"** y el **"estado deseado"** del proceso de seguridad digital, se requiere analizar la brecha actual entre los dos estados, determinando la brecha por cerrar con la implementación de la estrategia.

Así, se requiere la ejecución de acciones complementarias que optimizarán los controles generados, como las que se sugieren en el siguiente listado:

- ✓ Disponer de planes de trabajo y proyectos para cerrar la brecha y así poder llegar al estado deseado.
- ✓ Acoger estándares de seguridad digital que soporten la política.
- ✓ Apoyar las acciones de la organización en las orientaciones de las normas técnicas existentes.
- ✓ Para este punto concreto, por ejemplo, se sugiere utilizar la ISO/IEC 27002:2013.
- ✓ Realizar un programa constante de sensibilización y capacitación en seguridad digital que posibilite implementar y adoptar, por todos los miembros de la organización, una estrategia eficaz.

5. Documentación

La documentación ha sido determinada por la FID (Federación Internacional de Información y Documentación) como "la colección, recopilación, almacenamiento, clasificación, selección, difusión, y utilización de todo tipo de información, cualquiera que sea su soporte".

A continuación, podrá profundizar en los aspectos fundamentales sobre procesamiento de la información en relación con la documentación que integra estos procesos, esto es:

Video 1. Diseño y documentación de controles de ciberseguridad: documentación

Enlace de reproducción del video

Síntesis del video: Diseño y documentación de controles de ciberseguridad: documentación
Es de vital importancia el procesamiento de la información encontrada, por medio de evidencias y hallazgos que se generan mediante el proceso del diseño de controles de ciberseguridad. Es decir, los distintos registros o herramientas documentales que no sólo orientan el proceso sino que lo soportan.

Se identifican los siguientes tipos de documentación:

- **Formatos:** Los formatos suministran evidencias objetivas del resultado alcanzado. Pueden encontrarse en medio escrito o magnético y se convierten en registros después de ser diligenciados.
- **Manuales**: son elementos que contribuyen con el funcionamiento de la organización, ya que contienen información referente o relacionada con funciones, políticas, estructura orgánica, objetivos, bases jurídicas, atribuciones y actividades de la misma.
- **Procedimiento:** es la manera puntual para llevar a cabo una actividad o un proceso.
- **Procesos:** conjunto de actividades relacionadas entre sí que transforman elementos de entrada en salidas o resultados.
- **Instructivos:** contienen las ilustraciones detalladas para que una persona pueda ejecutar una operación o actividad.
- **Registros:** son los encargados de documentar la trayectoria de los procesos y proporcionan evidencia de verificaciones, acciones preventivas y acciones correctivas.
- **Actas:** se refiere al documento escrito en el que se relaciona lo acontecido, tratado o acordado en una junta o reunión.

Características de la documentación requerida

Toda la documentación que acompaña o da soporte a las acciones, procesos y desarrollo de procesos reúne una serie de características que le otorgan no sólo utilidad y validez, sino que, además, le aportan a su efectividad dentro de las necesidades de la organización.

Subjetividad

La documentación tiene fuerte afinidad humana y humanística, es decir, subjetividad, implicaciones personales que pueden llegar a influir.

Evidencia

Contar con información documentada es la mejor manera de justificar el cumplimiento con los requisitos de la norma.

Historial y constancia

No es suficiente afirmar que se realiza una tarea de una determinada forma. Es necesario que existan registros que dejen constancia de lo que se hace.

6. Generalidades de los activos de información

Los activos de información relacionados con la seguridad de la información hacen referencia a cualquier información o dispositivo que tenga que ver con el tratamiento de esta y que sea de valor para la organización.

Los activos de información cuentan con un sistema de clasificación, el cual se enfoca en las propiedades de confidencialidad, integridad y disponibilidad como

elementos para el tratamiento de los datos. Además, evalúa el impacto que se tendría en caso de no cumplir con alguno de estos fundamentos.

Algunos tipos de activos

- Las distintas políticas establecidas.
- El conjunto de estándares.
- Cada uno de los procedimientos.
- Todo el compendio de directrices.
- La o las arquitecturas.
- El conjunto de inspecciones o controles, tanto físicos como tecnológicos y de procedimientos.
- Tecnologías.
- Los roles y las distintas responsabilidades.
- Los proveedores de los servicios desde el exterior de la organización.
- El conjunto de instalaciones.

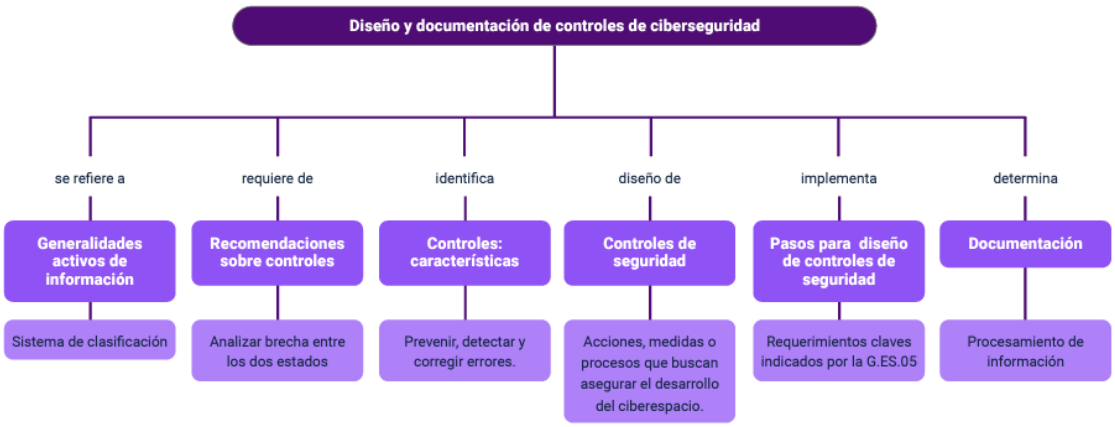
Ámbitos o elementos afectados por los activos y que hacen parte del proceso de la seguridad digital:

- ✓ Seguridad en el entorno.
- ✓ Contramedidas.
- ✓ Seguridad del personal.
- ✓ Conciencia y formación.
- ✓ Auditorías.
- ✓ Cumplimiento.
- ✓ Evaluación de amenazas.

- ✓ Análisis de vulnerabilidades.
- ✓ Evaluación de riesgos.

Síntesis

Los controles de seguridad deben ser una política constante de la organización, por lo que se requiere suficiente conocimiento sobre estrategias, seguridad de la información, control de seguridad y los pasos requeridos, sus características y generalidades de activos de información, todo este conocimiento generará la elaboración de las hojas de ruta a implementar para obtener la integridad de la información.



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
2. Pasos para el diseño de controles de seguridad	Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2011). *Gestión del riesgo. Principios y directrices (NTC-ISO 3100).*	Norma técnica	https://www.unipamplona.edu.co/unipamplona/portalIG/home_224/recursos/general/11072023/ntc-iso31000_gestionriesgo.pdf
2. Pasos para el diseño de controles de seguridad	Organización Internacional de Normalización [ISO]. (2013). *Information Technology – Security Techniques – Code of Practices for Information Security Controls* (ISO 27002:2013).	Norma técnica	https://www.iso.org/standard/54533.html
6. Generalidades de los activos de información	Organización Internacional de Normalización [ISO]. (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad*. (ISO 27001:2013)	Norma técnica	https://normaiso27001.es/

Glosario

Análisis de vulnerabilidades: metodología por medio de la cual se valoran los sistemas y servicios de tecnología de la información en una organización y se comprueba la presencia de vulnerabilidades.

Contramedidas: controles propios para riesgos específicos.

Control: se trata de las acciones que se deben implementar bajo un proceso o procedimiento, para garantizar los objetivos de seguridad de la organización.

Directrices: determinan las características generales de actuación. La directriz cuenta con un lineamiento normativo, lo que conlleva que sea general en su contenido y ámbito.

Entrada: se trata de elementos que ya tiene la organización en su haber y en su quehacer y que favorecen la instauración de cualquiera de los cinco pasos para cumplir con el diseño del plan de controles de seguridad.

Integridad: principio que sugiere que la información se mantenga intacta y sin alteraciones luego de sufrir un incidente.

Plan de acción: en el establecimiento de los controles de seguridad, el plan de acción se trata de la acción de fijar la hoja de ruta para lograr el estado deseado de la estrategia, teniendo en cuenta personas, tecnologías y procesos, entre otros recursos.

Riesgo: toda posibilidad de sufrir una afectación por causa de factores externos o internos. El riesgo es un peligro latente que puede o no materializarse. En el orden informático y de ciberseguridad, los riesgos no son distintos, contemplan las

vulnerabilidades y las amenazas y pueden ser controlados, tratados, mitigados, prevenidos y, en algunos casos, eliminados.

Salida: herramientas de registro o de documentación que se tendrán luego de haber analizado, ajustado o intervenido los documentos o registros ya existentes, relacionados con objetivos, planes de acción, estados de ciberseguridad de la compañía o clasificación de los activos de información, entre otros.

Referencias bibliográficas

Consejo Nacional de Política Económica y Social. (2011). *Lineamientos de políticas para Ciberseguridad y Ciberdefensa* (CONPES 3701). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

EcuRed. (s. f.). *Documentación*. https://www.ecured.cu/Documentaci%C3%B3n

Ministerio de Hacienda y Administraciones Públicas. (2013). MAGERIT – *versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (2011). Modelo de Seguridad y Privacidad de la Información. https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf .

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal Gutiérrez	Responsable del equipo	Dirección General
Liliana Victoria Morales Gualdrón	Responsable de línea de producción	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Rafael Neftalí Lizcano Reyes	Asesoría metodológica y pedagógica	Regional Santander - Centro Industrial del Diseño y la Manufactura
Pablo Cesar Pardo Ortiz	Experto Temático	Regional Cauca - Centro de Teleinformática y Producción Industrial
Fabián Leonardo Correa Díaz	Diseñador Instruccional	Regional Tolima - Centro agropecuario La Granja
Andrés Felipe Velandia Espitia	Asesoría metodológica y pedagógica	Regional Distrito Capital - Centro de Diseño y Metrología
Darío González	Corrección de estilo	Regional Tolima - Centro agropecuario La Granja
Gloria Amparo López Escudero	Adecuación instruccional - 2023	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Alix Cecilia Chinchilla Rueda	Metodología para la formación virtual - 2023	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Francisco José Lizcano Reyes	Responsable del equipo	Regional Santander - Centro Industrial del Diseño y la Manufactura
Leyson Fabián Castaño Pérez	Soporte organizacional	Regional Tolima - Centro de Comercio y Servicios

Nombre	Cargo	Regional y Centro de Formación
Carlos Julián Ramírez Benítez	Diseño web	Regional Santander - Centro Industrial del Diseño y la Manufactura
Luis Jesús Pérez Madariaga	Desarrollo front-end	Regional Santander - Centro Industrial del Diseño y la Manufactura
Ángela María Maldonado Jaime	Producción audiovisual	Regional Santander - Centro Industrial del Diseño y la Manufactura
Arnulfo Beltrán Mojica	Producción audiovisual	Regional Santander - Centro Industrial del Diseño y la Manufactura
Camilo Andrés Bolaño Rey	Producción audiovisual	Regional Santander - Centro Industrial del Diseño y la Manufactura
Gilberto Junior Rodriguez Rodriguez	Producción audiovisual	Regional Santander - Centro Industrial del Diseño y la Manufactura
Wilson Andrés Arenales Caceres	Producción audiovisual	Regional Santander - Centro Industrial del Diseño y la Manufactura
Zuleidy Maria Ruiz Torres	Producción audiovisual	Regional Santander - Centro Industrial del Diseño y la Manufactura
Yenny Patricia Ulloa Villamizar	Validación de diseño y contenido	Regional Santander - Centro Industrial del Diseño y la Manufactura
Jhon Jairo Urueta Álvarez	Desarrollo fullstack - 2023	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Manuel Felipe Echavarría Orozco	Desarrollo fullstack - 2023	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Carolina Coca Salazar	Evaluación de contenidos inclusivos y accesibles	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información

Nombre	Cargo	Regional y Centro de Formación
Lina Marcela Pérez Manchego	Validación de recursos educativos digitales	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información
Leyson Fabián Castaño Pérez	Validación de recursos educativos digitales y vinculación LMS	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información