Evaluación de los controles de ciberseguridad

Breve descripción:

Mediante el estudio de este componente formativo, el aprendiz estará capacitado para reconocer aspectos importantes de la evaluación de las estrategias de ciberseguridad y su aplicación, estimando el diagnóstico, diseño, monitoreo y operación de la misma. Así mismo, podrá realizar un informe basado en la auditoría de dicha operación.

Noviembre 2023

Tabla de contenido

Introducción

Para iniciar el desarrollo temático y conceptual de este componente formativo, es importante tener un contexto sobre lo que se tratará en este, por tal motivo, a continuación, se presenta una breve introducción, que lo contextualizará en este aprendizaje:

Video 1. Evaluación de los controles de ciberseguridad

Enlace de reproducción del video

Síntesis del video: Evaluación de los controles de ciberseguridad
Le damos la bienvenida al componente denominado: Evaluación de los controles de ciberseguridad. Con el estudio de este componente, estará en capacidad de reconocer aspectos importantes sobre la evaluación de las estrategias de ciberseguridad y su aplicación. De la misma manera, obtendrá elementos para la realización de un informe de auditoría sobre la operación de las estrategias aplicadas. El proceso de ejecución de la evaluación de estrategia de ciberseguridad implica, entre otros aspectos, estimar el diagnóstico, el diseño, la aplicación y el monitoreo de la operación de la misma; todo ello, adoptando lineamientos de la metodología de pruebas de efectividad, que son una serie de actividades de suma importancia que ayudarán a medir o comprobar la eficiencia del modelo de seguridad, que tengan establecido las organizaciones. De igual manera, se explorará la realización de un informe basado en la auditoría, que aporta el compendio de vulnerabilidades que puede tener la organización, a nivel informático. Para favorecer una experiencia satisfactoria durante el recorrido por este componente, le sugerimos seguir estas instrucciones: ✓ Explore todos los recursos didácticos que el componente tiene para usted. ✓ Procure llevar un registro de los elementos teóricos, conceptuales y prácticos que va asimilando en el recorrido del componente. Para ello,

tenga a la mano una herramienta de registro: computadora, libreta de notas o cualquier otra que le permita llevar apuntes.

- ✓ Seleccione un buen momento y un espacio oportuno para el estudio de este componente.

1. Finalidad de las pruebas

El enfoque de las pruebas de efectividad, frente a la metodología, es comprobar o medir la eficiencia de la ejecución del modelo de seguridad en organizaciones. Con el fin de ayudar a las organizaciones se han desarrollado metodologías que favorecen la comprensión y el desarrollo de las pruebas, el alcance de objetivos y el beneficio que se gana al identificar sus etapas y gestionarlas.

Tales metodologías se desarrollan en diferentes etapas, ayudando a definir qué tanto ha avanzado la organización con la implementación del modelo. Así pues, por medio de la valoración de diferentes aspectos, se podrán identificar también vulnerabilidades y amenazas, a las cuales está expuesta la organización, de igual manera que las debilidades de los controles implementados.

A continuación, explore el recurso didáctico con el que le presentamos las etapas del procedimiento de las pruebas, según lo estipulado por la Guía metodológica de pruebas de efectividad, del MINTIC:

Etapa de las pruebas de efectividad

Fase de levantamiento de información: etapa en la que la organización ha de hacer recopilación de toda la información requerida para dar inicio a la actividad; tal información podrá estar organizada por el equipo de seguridad con el que cuente la empresa o compañía.

Con la información recogida se buscará identificar los activos de mayor importancia en la organización, activos que tienen relación con los procesos institucionales, que serán de carácter misional o de apoyo. Otro aspecto que debe ser favorecido o facilitado por la información recogida, es el hecho de permitir conocer el contexto de la entidad, en otras palabras, el entorno en donde serán proyectados los objetivos institucionales.

La recolección de la información es realizada por un equipo de personas que debe estar integrado al organigrama de la entidad, al mapa de procesos, política de seguridad, manual de políticas, metodología de riesgos, identificación de riesgos, planes de gestión de riesgos, entre otros. Este compendio de información es cimiento para lograr identificar la brecha de seguridad que tenga la organización.

Etapa de revisiones de manuales

Cuando se habla de revisiones, se está haciendo referencia a aquellos procesos de inspección de los distintos manuales que la organización ha de realizar, para lograr la identificación de lo comprendido por los servidores públicos en seguridad, de lo realizado en seguridad en los procesos y, adicionalmente, el estado en que se encuentran las políticas institucionales.

Tales revisiones, se llevan a cabo a la vez que se analiza la documentación, mediante encuentros o reuniones con quienes están a cargo de dichos temas, con los dueños de los procesos. Se trata de una forma bastante efectiva porque mediante las inspecciones se logra hacer identificación del porqué de las implementaciones de seguridad y los controles aplicados en la organización.

Por otra parte, ayuda a hacer comprobación de si las personas y equipos de trabajo, comprenden los distintos procesos de la seguridad institucional y si se ha logrado generar y tomar conciencia de las distintas políticas de seguridad y de privacidad que la empresa tiene.

Etapa de Identificación de amenazas

Se refiere a la evaluación misma del riesgo de seguridad en la organización. En otras palabras, es la evaluación de las distintas acciones y actividad en donde se han visto implicadas las personas, la infraestructura y los procesos. Todo ello, con el objetivo de lograr la identificación de las distintas amenazas que sobre la entidad pueden ocurrir.

Lo que resulte de la aplicación de estas actividades favorece que se desarrollen diferentes planes de mitigación de vulnerabilidades halladas; también ayuda a orientar mejor los recursos y la ayuda a las áreas de la organización que más lo estén necesitando. Buscar estas amenazas se debe dar desde el momento en que se crean los procesos y durante todo el ciclo de vida.

El enfoque que deben tener estas actividades debe ser simple, en otras palabras, se deben descomponer los procesos a través de la evaluación manual, así se podrá

tener conocimiento del funcionamiento y su interrelación con las demás actividades, como:

- ✓ Definir y clasificar los activos de la entidad, evaluando su criticidad, sus posibles vulnerabilidades técnicas, operacionales y de gestión.
- ✓ Desarrollar una matriz con las amenazas potenciales, con sus vectores de ataque.
- ✓ Elaborar planes de mitigación para cada amenaza real.

El resultado de todo esto puede ser una serie de documentos, listas o diagramas, en los cuales se plasma los análisis de riesgo de la entidad y sus planes de mitigación a través de los controles sugeridos.

2. Pruebas y análisis

Mediante las pruebas y análisis, las entidades identifican los diferentes riesgos que se muestran por las debilidades en la implementación del modelo de seguridad y de privacidad de la información y las vulnerabilidades que se manifiestan dada la ausencia de controles de seguridad que logren mitigar riesgos.

Este tipo de pruebas están orientadas a la evaluación de la estructura de seguridad de la organización; para ello, las organizaciones han de revisar diferentes frentes de trabajo como, por ejemplo, el Anexo A de la ISO 27001:2013, el ciclo de vida de la seguridad (PHVA), el nivel y estado de madurez de la organización en correspondencia con los niveles expuestos en el modelo de seguridad y privacidad y las

recomendaciones para que la organización logre plasmar el concepto de **Ciberseguridad**.

3. Tipos de pruebas de efectividad

Existen tres tipos de pruebas de efectividad, basados en el nivel de conocimiento del entorno o de la infraestructura de la organización objetivo, estos tres tipos de prueba son los siguientes:

A. **Pruebas con conocimiento nulo del entorno:** se trata del tipo de prueba en la que simulará a un atacante real, ya que se basa en que cuenta con muy poco conocimiento o quizá nulo conocimiento del objetivo o su infraestructura.
B. **Pruebas con conocimiento medio del entorno:** se refiere a cuando, para la prueba de "pentesting", se cuenta con más información sobre aquel ambiente que será atacado, es decir, direcciones IP, sistemas operativos, arquitectura de red etc. De igual manera es información limitada o media. Esto emula a alguna persona dentro de la red con conocimiento básico de la misma.
C. **Pruebas con conocimiento completo del entorno:** son pruebas en donde el "hacker" cuenta con toda la información disponible y relacionada con el sistema objetivo del ataque. Por lo general, son para asuntos de auditoría.

4. Procedimiento de ejecución de pruebas de efectividad

Las pruebas de efectividad pueden realizarse por medio de las siguientes acciones de manera secuencial:

- ✓ Contextualización.
- ✓ Reconocimiento del objetivo.
- ✓ Modelado de amenazas.
- ✓ Evaluación de vulnerabilidades.
- ✓ Explotación.
- ✓ Post explotación.
- ✓ Reporte.

A continuación, se especifican las acciones con las que se aplican las pruebas de efectividad; comprenda los aspectos importantes de cada una de ellas a través de la siguiente información:

A. **Contextualización:** esta acción se basa en identificar los alcances reales de las pruebas y de los procedimientos a ejecutar con base a las necesidades identificadas.
B. **Reconocimiento de objetivo:** esta acción, busca obtener tanta información del objetivo como sea posible para poder ser empleada en la acción de evaluación de vulnerabilidades y la acción de explotación.
C. **Modelado de amenazas:** esta acción establece la relación entre el atacante y el activo, intentando definir el beneficio que puede alcanzar el atacante si logra penetrar el sistema y afectar la información de alguna manera.

D. **Evaluación de vulnerabilidades:** es la acción que descubre falencias en los sistemas y aplicaciones, que pueden llegar a ser aprovechados por un atacante.
E. **Explotación:** es la acción que busca, concretamente, acceder al sistema, apalancando las debilidades identificadas en la etapa anterior o sobrepasando los controles de seguridad existentes.
F. **Post explotación:** acción que busca identificar el tipo de información que se puede obtener, a qué otros sistemas de información se pueden ingresar desde el sistema capturado, las opciones de configuración, información de red, todo esto con el objetivo principal de determinar el valor de la máquina para la organización.
G. **Reporte:** acción con la que se documentan resultados obtenidos en cada anterior acción

De la aplicación procedente, responsable y oportuna de las pruebas, depende en gran medida su efectividad y su potencial aprovechamiento. Las pruebas de efectividad han de realizarse con las acciones mencionadas, siendo cada una de estas, una acción vinculada consecuentemente con las anteriores y/o con las posteriores.

Guía metodológica de pruebas de efectividad

Para ahondar en los aspectos importantes relacionados con pruebas de efectividad y su procedimiento, le recomendamos estudiar la **Guía No 1. Guía metodológica de pruebas de efectividad del MinTIC**.

Enlace del documento

5. Alcance de las pruebas

Deberán existir una serie de reglas y otros elementos importantes para la aplicación de las pruebas de efectividad técnicas, con el fin de asegurar que tales actividades no lleguen a incurrir en fallas mayores y que, también, sea posible la afectación de la infraestructura o de las distintas operaciones de la organización.

Dentro del alcance, es posible definir aspectos como los que se muestran a continuación:

A. **Plan de trabajo:** implica definir la duración en tiempo para la realización de las pruebas, los sistemas que van a hacer parte de estas, las acciones y actividades específicas, los procedimientos de contingencia en caso de alguna afectación, entre otros.
B. **Insumos:** recursos necesarios para realizar las actividades: entre otros, personal adicional, ventanas de tiempo, equipos.
C. **Responsables:** serán los encargados de efectuar las pruebas (sean proveedores o funcionarios de la entidad).
D. **Afectaciones posibles:** tipo de afectación que puede llegar a darse sobre cada sistema, también debe definirse si el objetivo es realizarlo en horario de producción o en horario de baja actividad laboral.
E. **Multas o sanciones:** en caso de incumplir los parámetros anteriormente mencionados, deberán fijarse las sanciones disciplinarias o multas a que haya lugar.

¡Importante!

Estos alcances permitirán controlar internamente el desarrollo de las pruebas, así como manejar los acuerdos de servicio con terceros que pueden llegar a realizar estos procedimientos.

6. La auditoría en la ciberseguridad

Una auditoría de ciberseguridad se considera una de las partes más importantes de un sistema de bloqueo frente a posibles ciberataques, por lo cual percibe especial interés para conocer en qué consiste y cómo proceder para mantener tales ciberataques lejos de los intereses de la organización.

Es importante realizar este tipo de auditoría, tanto interna como externa, para verificar el estado de la seguridad de la organización. En estas auditorías se inspeccionan los sistemas frente a los ataques o posibles brechas de seguridad que puedan existir.

Las siguientes, son algunas particularidades importantes que se han de tener en cuenta, en lo referente a periodicidad e intensidad, en procesos de auditorías de ciberseguridad, esto es:

A. **Periodicidad de las auditorías:** se debe tratar de una comprobación cíclica o periódica, ya que de esta manera aporta nueva información cada espacio breve de tiempo.
B. **Importancia del ejercicio cíclico:** realizar auditorías periódicas no es obligatorio en todas las organizaciones, sobre todo de perfil privado, pero

sí que es bastante recomendable, con el fin de prevenir o ver a tiempo los posibles problemas acaecidos en los sistemas de seguridad.

C. **Promoción de la mejora y buenas prácticas:** este tipo de auditoría de ciberseguridad promueve la mejora de los sistemas, en cuanto a buenas prácticas, sobre todo en estos tiempos de constantes cambios y renovaciones tecnológicas.

7. Pasos de la auditoría en ciberseguridad

Las auditorías de los sistemas de gestión de la seguridad de la información, deben ser establecidas teniendo en cuenta algunas condiciones que favorecen, rotundamente, tanto su construcción como su desarrollo.

Profundice en los pasos que se deben seguir para la auditoría en ciberseguridad, explorando la información que se expone a continuación:

A. **Marcar objetivo:** se debe establecer el objetivo de la auditoría de ciberseguridad a realizar. No es lo mismo hacer una auditoría para validar una norma, que realizar una, para comprobar que se está cumpliendo la política de ciberseguridad exigida.
B. **Planificación:** con objetivos de auditoría claros, se proyectan los pasos por seguir. Se establecen servicios por auditar y se identifican los sistemas operativos instalados en la organización.
C. **Obtener información:** recopilar toda la información posible para valorar funcionamiento en el área de TI de la organización, las tecnologías, políticas y protocolos que son el objetivo de la auditoría de ciberseguridad.

Pueden aplicarse entrevistas con empleados, analizando las especificaciones del "software" y el "hardware", revisando documentación, utilizando herramientas para medir la seguridad de los sistemas y vulnerabilidades con los que cuenta la organización.

D. **Análisis de la situación:** se examina la información recolectada para encontrar las vulnerabilidades y fallos en los sistemas de la organización.
E. **Informe de resultados:** hecho todo el análisis y conociendo el estado real de la organización, se produce un informe detallado de los resultados extraídos de la auditoría. En este informe se explican vulnerabilidades de ciberseguridad halladas y se proponen soluciones y recomendaciones.

Cumplidos estos pasos, se explicarán, además, las acciones recomendadas que debe realizar la empresa u organización en cada uno de los puntos críticos (ante ciberataques) que se han encontrado.

8. Tipos de auditorías

Las auditorías pueden ser de tipo externas o internas. Se diferencian dependiendo de quién realiza la auditoría; si lo realizan compañías independientes de la organización se consideran auditorías externas y cuando son realizadas por personas que trabajan en la propia organización se denominan auditorías internas.

Las auditorías en ciberseguridad pueden clasificarse según el objetivo que persiguen o según la información proporcionada, esto es:

Auditoría según el objetivo

Este tipo de auditorías las puede revisar más detalladamente a continuación:

1. **Auditoría forense:** Son auditorías de ciberseguridad que se realizan tras haberse producido un incidente de seguridad. Tiene como objetivo identificar y recopilar evidencias digitales para establecer las causas que lo han producido.
2. **Auditoría web:** se trata de auditorías que tienen como objetivo conocer la seguridad de aplicaciones y páginas web que nos permitan descubrir cualquier tipo de fallo o vulnerabilidad en la implementación de los mismos.
3. **Auditoría de código:** una parte, las auditorías de código son pruebas de calidad sobre aplicaciones informáticas (a nivel de código fuente) que permiten conocer e identificar posibles vulnerabilidades en cualquier tipo de "software".
4. **Auditoria de "hacking" ético:** son un "test" de intrusión que intenta utilizar las mismas técnicas de "hacking" y herramientas que los atacantes para, de esta manera, poner a prueba la seguridad informática. La forma de comprobar las medidas de seguridad es poniéndolas a prueba y para ello surge este servicio.
5. **Auditoría de análisis de vulnerabilidades:** son auditorías de ciberseguridad que tienen como objetivo detectar los posibles agujeros de seguridad de las aplicaciones, en busca de vulnerabilidades; también se encargará de poner a prueba la robustez de las contraseñas.

6. **Auditorías de redes:** la seguridad de la red, ha de ser una prioridad para la organización, más aún en un internet que se encuentra plagado de ataques externos. Hacer un mapeo de la red, con el fin de descubrir todos los dispositivos conectados, es en lo que se centrará este tipo de auditoría.

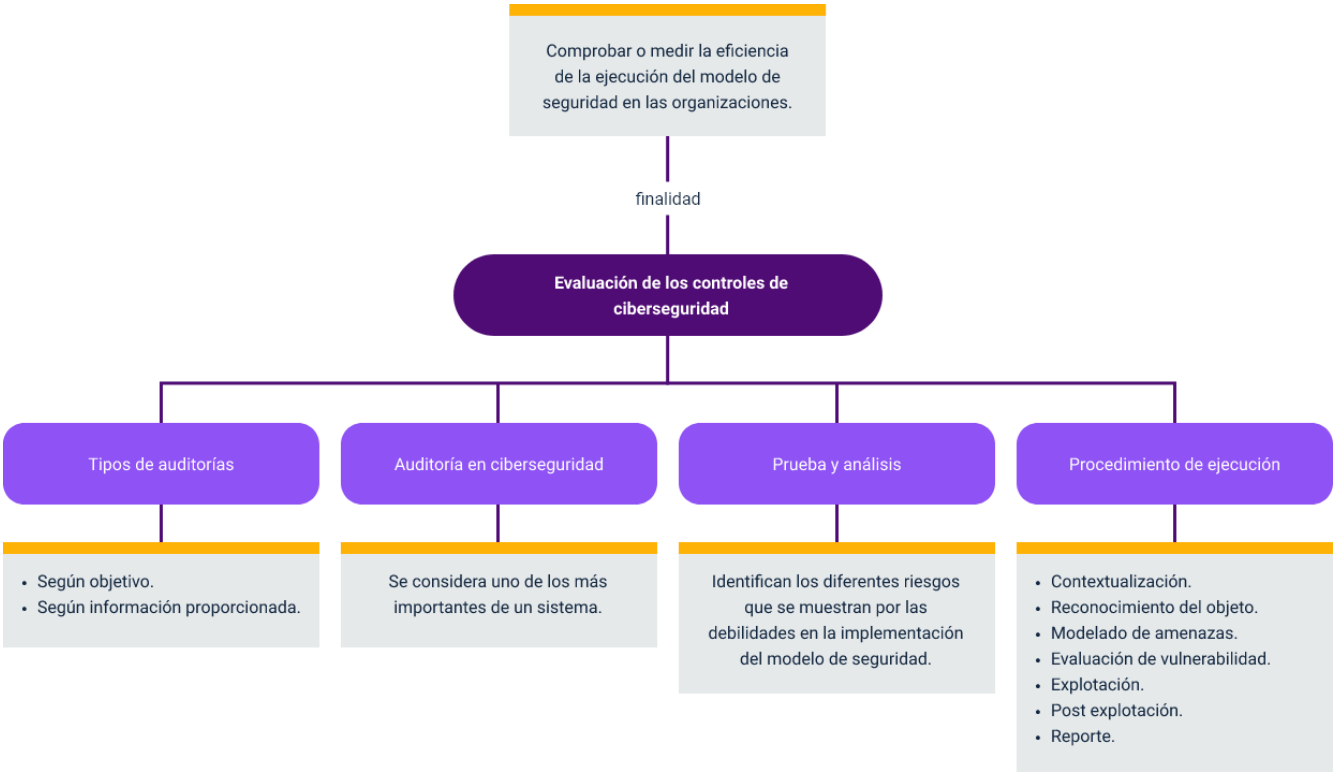
Auditorías según información proporcionada

Este tipo de auditorías están clasificadas en tres y las puede detallar a mayor profundidad a continuación:

A. **Auditoría de caja blanca:** en este tipo de auditorías, los auditores tienen todo el conocimiento y los accesos por adelantado de los elementos e infraestructuras que se van a analizar.
B. **Auditorías de caja gris:** los auditores tienen un acceso limitado a los sistemas y datos de la organización. Para realizar este tipo de auditorías lo que se hace es simular un ciberataque interno (como si fuera un empleado) con malas intenciones.
C. **Auditorías de caja negra:** no se tiene conocimiento de ningún tipo de información ni de acceso. Aquí el auditor parte desde el principio y va a intentar descubrir las posibles formas de lograr entrar en el sistema interno desde fuera de la empresa. En este caso el ciberataque que se va a simular es externo.

Síntesis

La ciberseguridad es un aspecto muy importante en cualquier organización, por lo que es de suma importancia tener una evaluación constante de los riesgos de algún tipo de ataque, en este sentido, se debe conocer muy bien el tipo de estrategias a utilizar, con el fin de detectar las posibles amenazas y con esto implementar acciones que permitan mitigar o corregir los controles de ciberseguridad establecidos por la empresa u organización. Al igual que reconocer los diferentes tipos de auditorías y sus respectivos informes que permitan una mejor toma de decisiones en este aspecto.



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
4. Procedimiento de ejecución de pruebas de efectividad.	Ministerio de Tecnologías de la Información y Comunicaciones (2016). *Guía Metodológica de Pruebas de Efectividad*.	Guía técnica	https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

Glosario

Auditoría: una auditoría es un proceso de verificación y/o validación del cumplimiento de una actividad según lo planeado y las directrices estipuladas.

Auditoría externa: auditoría realizada por compañías independientes de la organización o aquellas que son realizadas por personas ajenas a la empresa, contratadas para ello.

Levantamiento de información: etapa de las pruebas de efectividad en la que la organización ha de hacer recopilación de toda la información requerida para dar inicio a la actividad; tal información podrá estar organizada por el equipo de seguridad con el que cuente la empresa o compañía.

Modelado de amenazas: esta acción establece la relación entre el atacante y el activo, intentando definir el beneficio que puede alcanzar el atacante si logra penetrar el sistema y afectar la información de alguna manera.

Pruebas de efectividad: acciones que se enfocan en establecer una línea base del estado de seguridad de la organización, con el fin de facilitar la identificación de la brecha en la implementación del modelo de seguridad.

Referencias bibliográficas

Ciberseguridad y riesgos digitales (2020). *Normas ISO en auditoría informática: Cuáles son las más importantes*. EALDE. https://www.ealde.es/iso-auditoria-informatica/

Ministerio de Tecnologías de la Información y Comunicaciones (2016). *Guía de Auditoría*. https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

Ministerio de Tecnologías de la Información y Comunicaciones (2016). *Guía Metodológica de Pruebas de Efectividad*. https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

Organización Internacional de Normalización (ISO 2013). *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos*. (ISO 27001). https://www.iso.org/standard/27001

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	Diseño instruccional	Regional Tolima - Centro agropecuario La Granja
Carolina Coca Salazar	Revisor Metodológico y pedagógico	Regional Distrito Capital - Centro de Diseño y Metrología
Sandra Patricia Hoyos Sepúlveda	Corrección de estilo	Regional Distrito Capital - Centro para la Industria de la Comunicación Gráfica
Gloria Amparo López Escudero	Adecuación instruccional	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Alix Cecilia Chinchilla Rueda	Metodología para la formación virtual	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Yazmin Rocio Figueroa Pacheco	Diseño web	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información

Nombre	Cargo	Regional y Centro de Formación
Luis Jesús Pérez Madariaga	Desarrollo Fullstack	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Ernesto Navarro Jaimes	Animación y Producción audiovisual	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Lady Adriana Ariza Luque	Animación y Producción audiovisual	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Laura Gisselle Murcia Pardo	Animación y Producción audiovisual	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
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