**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| **PROGRAMA DE FORMACIÓN** | Tecnología en gestión de redes de datos. |

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPETENCIA** | 220501014 - Administrar hardware y software de seguridad en la red a partir de normas internacionales. | **RESULTADOS DE APRENDIZAJE** | 220501014-03 - Verificar eventos en la infraestructura de red, mediante herramientas y técnicas de análisis  de datos que permitan determinar incidentes de seguridad.  220501014-04 - Gestionar el estado de la seguridad en la red de datos de la organización y su pertinencia según el plan de seguridad. |

|  |  |
| --- | --- |
| **NÚMERO DEL COMPONENTE FORMATIVO** | 12 |
| **NOMBRE DEL COMPONENTE FORMATIVO** | Seguridad en la red. |
| **BREVE DESCRIPCIÓN** | Este componente formativo aborda aspectos generales y claves sobre la gestión de la seguridad de redes informáticas y la información que en ellas circula. Mediante el estudio responsable de todos los temas, el aprendiz se afianzará en seguridad, ataques, clasificación de *software*, políticas de seguridad y normativa. |
| **PALABRAS CLAVE** | Dispositivos, información, redes, seguridad, transmisión. |

|  |  |
| --- | --- |
| **ÁREA OCUPACIONAL** | Ciencias naturales, aplicadas y relacionadas. |
| **IDIOMA** | Español |

1. **TABLA DE CONTENIDOS:**

Introducción

* + - 1. ¿Qué es la seguridad de la red?

1.1 Causas de la inseguridad

* 1. Clasificación de los ataques

*2. Software* malicioso

* 1. Clasificación de *malware*
  2. Ciclo de vida de un virus

1. Servicios de seguridad y mecanismos de seguridad
2. Seguridad en servicios de red
3. Seguridad perimetral
4. Políticas de seguridad
5. **INTRODUCCIÓN:**

Tenga una cordial bienvenida al estudio de este componente denominado **Seguridad en la red**. Comience explorando el video que se propone enseguida, en el cual usted podrá tener una visión general de los temas que se desarrollarán. ¡**Adelante**!

|  |
| --- |
| **DI\_CF12\_0\_Video\_Introduccion** |

1. **DESARROLLO DE CONTENIDOS**
2. **¿Qué es la seguridad de la red?**

La seguridad en la red es un campo especializado que contempla el uso de múltiples herramientas tecnológicas que van desde dispositivos de *hardware* y *software* que, en principio, evitan el ingreso y propagación de una gran variedad de amenazas y ataques.

Las organizaciones, entonces, deben:

|  |  |  |
| --- | --- | --- |
| Promulgar políticas y controles de acceso a los recursos de la red. | Permitir verificar e identificar accesos no autorizados. | Hacer búsqueda permanente de vulnerabilidades que pueda tener la red de datos de la organización. |

El siguiente video, explica en detalle las generalidades más destacadas de la seguridad en la red; preste suma atención:

|  |
| --- |
| **DI\_CF12\_1\_Video\_GeneralidadesSeguridadEnLaRed** |

**1.1. Causas de la inseguridad**

Las organizaciones apuestan por el uso de sistemas de información que se componen de redes e infraestructuras tecnológicas; estas, a su vez, intercambian, de manera constante, datos valiosos, los cuales son vulnerables y pueden sufrir amenazas y ataques que afecten la confidencialidad, integridad y disponibilidad, tanto de datos como de recursos informáticos que preste la organización.

Las siguientes, son las principales vulnerabilidades presentes en un sistema informático:

**Tabla 1**

*Familias de vulnerabilidades*

|  |  |  |
| --- | --- | --- |
| Ámbitos físicos | Ámbitos organizativos | Ámbitos tecnológicos |
| Falta de redundancia y de recursos a nivel de equipo. | Falta de:   * Recursos humanos y personal cualificado. * Comunicaciones. | Fallos en:   * Los servicios y aplicaciones web y las bases de datos. * Recurrencia y falta de supervisión de incidentes. |
| Acceso a salas de informática no seguras. | Falta de:   * Controles periódicos. * Documentos de procedimientos adaptados a la empresa. * Medios relativos a los riesgos. | Falta de:   * Actualizaciones y parches de los sistemas operativos. * Control suficiente sobre los programas malintencionados. |
| Ausencia o mala estrategia de protección de datos. | Complejidadfuncional | Mala utilización del correo. |

Nota: adaptada de Carpentier (2016).

La inseguridad en los sistemas informáticos incluye el estudio de los activos, las amenazas y los riegos. Para definir y demarcar el concepto de inseguridad informática, tenga en cuenta la especificación de los siguientes elementos:

|  |
| --- |
| **DI\_CF12\_1\_Slide\_DefinicionInseguridadSistemasInformaticos** |

**1.2. Clasificación de los ataques**

La mayoría de las amenazas en la red se encargan de revelar las vulnerabilidades de la seguridad en la red de datos. Las agresiones a las redes de comunicaciones se pueden determinar cómo acciones deliberadas en aras de corromper o violar su seguridad.

El intruso emplea algún tipo de ataque informático a la hora de establecer un acceso no autorizado al sistema y estas agresiones se pueden clasificar en dos grupos, así:

|  |  |
| --- | --- |
| **Ataques pasivos**  Este tipo de ataque consiste en monitorear los canales de comunicación sin alterar información alguna. | **Ataques activos**  Este tipo de ataque engloba alguna modificación del flujo de datos o la creación de datos falsos. |

Los ataques pasivos están relacionados, principalmente, con el contenido del paquete y con el monitoreo del tráfico en red. El objetivo del ataque es capturar la información que está siendo transmitida, donde su principal objetivo es la vigilancia de la red a fin de descubrir vulnerabilidades a través del mapeo de la red y de los servicios prestados.

Este tipo de ataques también pueden ser llamados ataques de reconocimiento, los cuales suelen ser un requisito previo para que otros ataques obtengan acceso no autorizado a la red o interrumpan sus operaciones.

Entre las herramientas de ataque de reconocimiento están las siguientes:

|  |
| --- |
| **DI\_CF12\_1\_Pestañas\_HerramientasDeAtaqueDeReconocimiento** |

**Ataques de activos**

En este tipo de ataque, principalmente, se busca la alteración de los recursos donde se intenta borrar, añadir o modificar los datos que se transmiten en la red; igualmente se afecta la prestación de los servicios de la organización. Un atacante activo amenaza los tres pilares de la seguridad (confidencialidad, integridad y disponibilidad).

Los tipos de ataques activos más comunes son:

|  |
| --- |
| **DI\_CF12\_1\_LineaDeTiempo\_AtaquesActivos** |

**Atacantes**

Soriano (2014), define al atacante como el “Individuo que obtiene, o trata de obtener, permisos o acceso no autorizado al sistema de información”. Se debe resaltar que no solo existen atacantes externos o intrusos, sino también se deben considerar a los individuos internos a la organización.



Un atacante interno puede ser representado por cualquier usuario que pertenece a la organización y tiene acceso al sistema de información y a la infraestructura tecnológica de la red.

En relación con los atacantes, tenga en cuenta algunos aspectos destacados como:

|  |
| --- |
| **DI\_CF12\_1\_Acordeón\_Atacantes** |

1. ***Software* malicioso**

Mantener la seguridad de la red y de la información que comparten los usuarios, requiere de vigilancia por parte de los profesionales responsables de la seguridad en redes, donde es de vital importancia estar atentos a los diferentes ataques y evolución de las amenazas.



El estudio de las diferentes vulnerabilidades de los dispositivos de red y sus correspondientes aplicaciones requieren una atención especial a fin de estar preparados de los posibles ataques que provengan desde el exterior, así como el interior de las organizaciones, captando errores y falencias en las conexiones en la red. Según Ariganello (2020), “las principales vulnerabilidades de los dispositivos finales son los ataques de virus, gusanos y troyanos” (p. 291).

Tenga en cuenta:

* Estos programas maliciosos son solo una pequeña gota en el inmenso océano de amenazas a una red de información.
* Se hace necesario entonces la implementación de todo tipo de mecanismo de seguridad de acceso a la red.
* Los piratas informáticos solo requieren de un computador y *software* especializado para inmiscuirse en la red de información.
* No es necesario ningún contacto físico en ella.
* El *malware* o *software* malicioso se refiere a todos aquellos programas cuyo único propósito es realizar tareas dañinas afectando el software del sistema y averiando el correcto uso del hardware.
* El *malware* o *software* malicioso se instala en la máquina objetivo sin consentimiento del usuario.
* Cuando un *malware* se ejecuta puede alterar algunas prestaciones de la máquina infectada como lo puede ser la velocidad, las tareas que el usuario desea realizar y obtener información crítica del sistema.

**2.1. Clasificación de *malware***

Para realizar una categorización del *malware* y de la proliferación de las amenazas presentes en la red, es necesario conocerlos, estos son:

|  |
| --- |
| **DI\_CF12\_2\_InfografiaInteractiva\_ClasificacionDeMalware** |

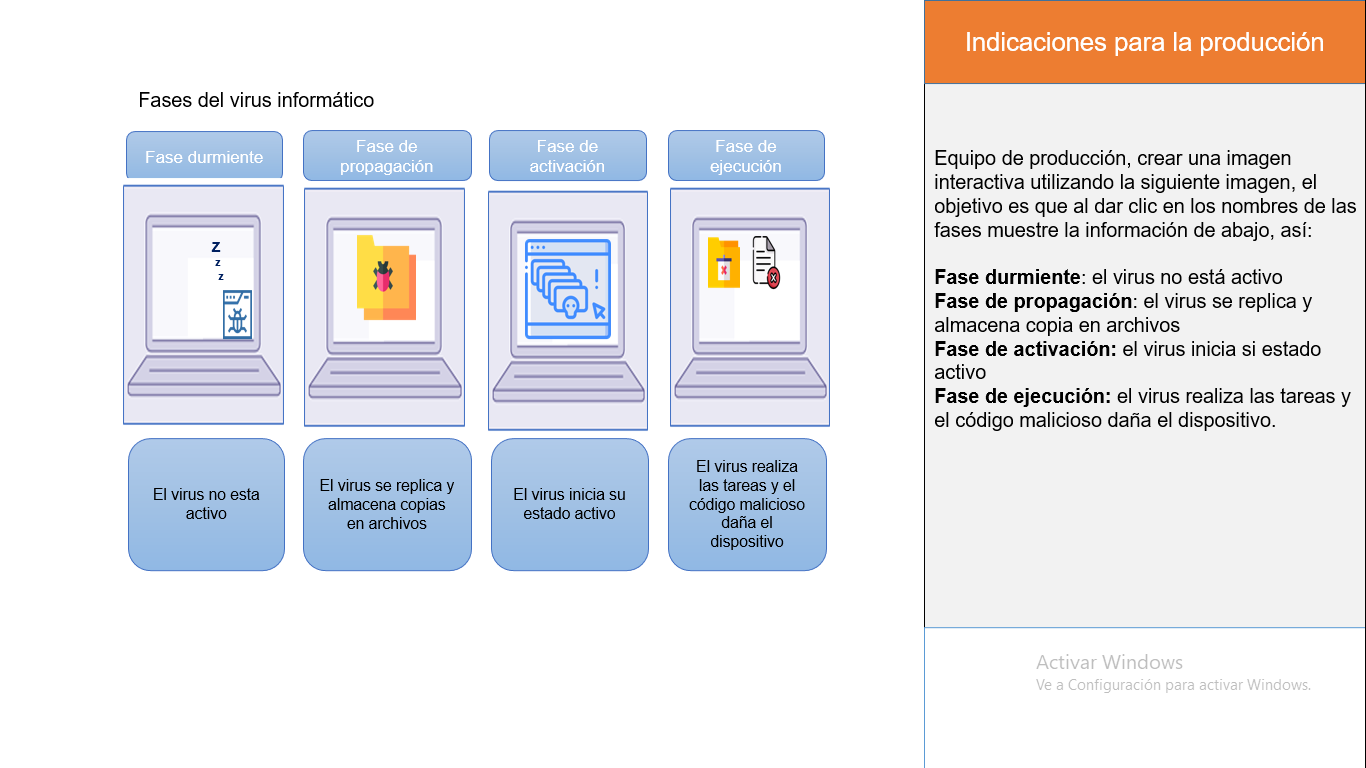
**2.2. Ciclo de vida de un virus**

Con la proliferación de diversidad de virus informáticos, la seguridad del sistema se ha vuelto prioritaria. Los virus tienden a ser destructivos y se propagan a través de las redes haciendo copias de sí mismo, cuando llegan a un dispositivo, los virus normalmente empiezan a infectar y replicarse en el equipo destino del ataque o puede permanecer inactivo a la espera de que el usuario ejecute el programa infectado.

Estas son las fases por las que puede pasar un virus informático:

**Figura 1**

*Fases del virus informático*



Conozca otros aspectos clave sobre los virus informáticos, consultando el video que se, a continuación, se propone:

<https://www.youtube.com/watch?v=x56FT_OVARQ>

1. **Servicios de seguridad y mecanismos de seguridad**

Un servicio de seguridad, es una prestación que avala que todos los procesos que involucran la transferencia de datos e información, tendrán la seguridad apropiada. Esto se logra por medio de políticas establecidas en cuanto a seguridad de la información se refiere.



Según Dordoigne (2020), dentro de los servicios de seguridad que se deben mantener están:

|  |
| --- |
| **DI\_CF12\_3\_Acordeon\_ServiciosDeSeguridad** |

1. **Seguridad en servicios de red**

La interconexión de redes presenta una amenaza que requiere de atención a la hora de establecer la seguridad en el ingreso y salida de información a la red interna privada.

Se pueden aplicar diferentes herramientas de protección, entre las que se encuentran:

|  |
| --- |
| **DI\_CF12\_4\_Slide\_SeguridadEnServiciosDeRed** |

1. **Seguridad perimetral**

Como medida de seguridad perimetral por implementar, está el denominado cortafuegos o *firewall*, el cual se encarga de convertir las diversas redes a las que se conecta, en independientes. Al contrario que un *router*, no se conforma con transmitir la petición. Un cortafuegos segmenta los flujos asumiendo él mismo las peticiones. Para esto, establece dos conexiones y puede realizar una acción de autentificación.



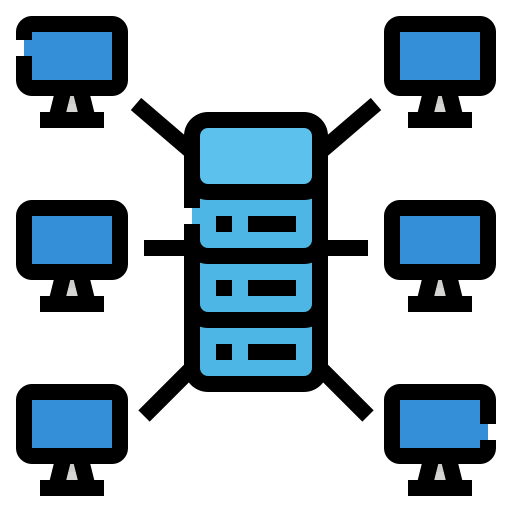
El cortafuegos de infraestructura suele ir acompañado de un cortafuegos personal, instalado en los equipos de trabajo. Así, los equipos se protegen de ataques que podrían proceder, incluso, de dentro de la red local.

**Figura 2**

*Conexión, en red, del firewall*



Internet



LAN



*Router*

*Firewall*



Nota: adaptado de Dordoigne (2020)

La primera generación de estos equipos permitía distintos análisis en las cabeceras de los paquetes, de manera equivalente a los *routers* filtrantes. El cortafuegos de tabla de estado (*State full inspection*), más reciente, conserva en memoria una tabla de las conexiones establecidas. Así, las comunicaciones entre clientes, autorizadas después de la autentificación, pueden continuar sin problema.

La nueva generación de cortafuegos, llamada de aplicación, es capaz de analizar algunos cuerpos de paquetes, como los de los protocolos SMTP, HTTP. Este nivel de análisis permite atenuar las nuevas formas de ataque que se aprovechan de los fallos de las aplicaciones estándar.

Un complemento del cortafuegos es el servidor *proxy*; se utiliza particularmente en el ámbito del tráfico *Hyper Text Transfer Protocol* (HTTP) o, incluso, con *File Transfer Protocol* (FTP), en la red LAN e Internet. El servidor *proxy* intercepta una petición hacia el exterior, la redirecciona como si fuera suya y, seguidamente, almacena los datos recibidos. Por último, este los envía al solicitante inicial.

1. **Políticas de seguridad**

La organización debe integrar a sus mecanismos de seguridad, las políticas que rigen el correcto uso de los recursos de red, el uso de la información y el intercambio de la misma. Los usuarios de los equipos (estaciones de trabajo, servidores, centros de datos, entre otros) deben hacerse cargo y responsabilizarse de sus actividades en el marco de la utilización de herramientas informáticas.

El establecimiento de las políticas de seguridad de la información se encuentra ampliamente contemplado en la norma ISO 27001 que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La misma, le permite a las organizaciones que adopten e implementen la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

Las fases de la metodología expuesta por el **Sistema de Gestión de La Seguridad de la Información** (SGSI) de la norma ISO 27001, se pueden resumir así:

**Figura 3**

*Método de evaluación y tratamiento de riesgos*

Identificación de Activos

Amenazas

Vulnerabilidades

Requisitos Legales

Análisis de Impacto

Seleccionar e implementar controles

Tratamiento del riesgo

Asumir el riesgo

Reducir el riesgo

Eliminar el riesgo

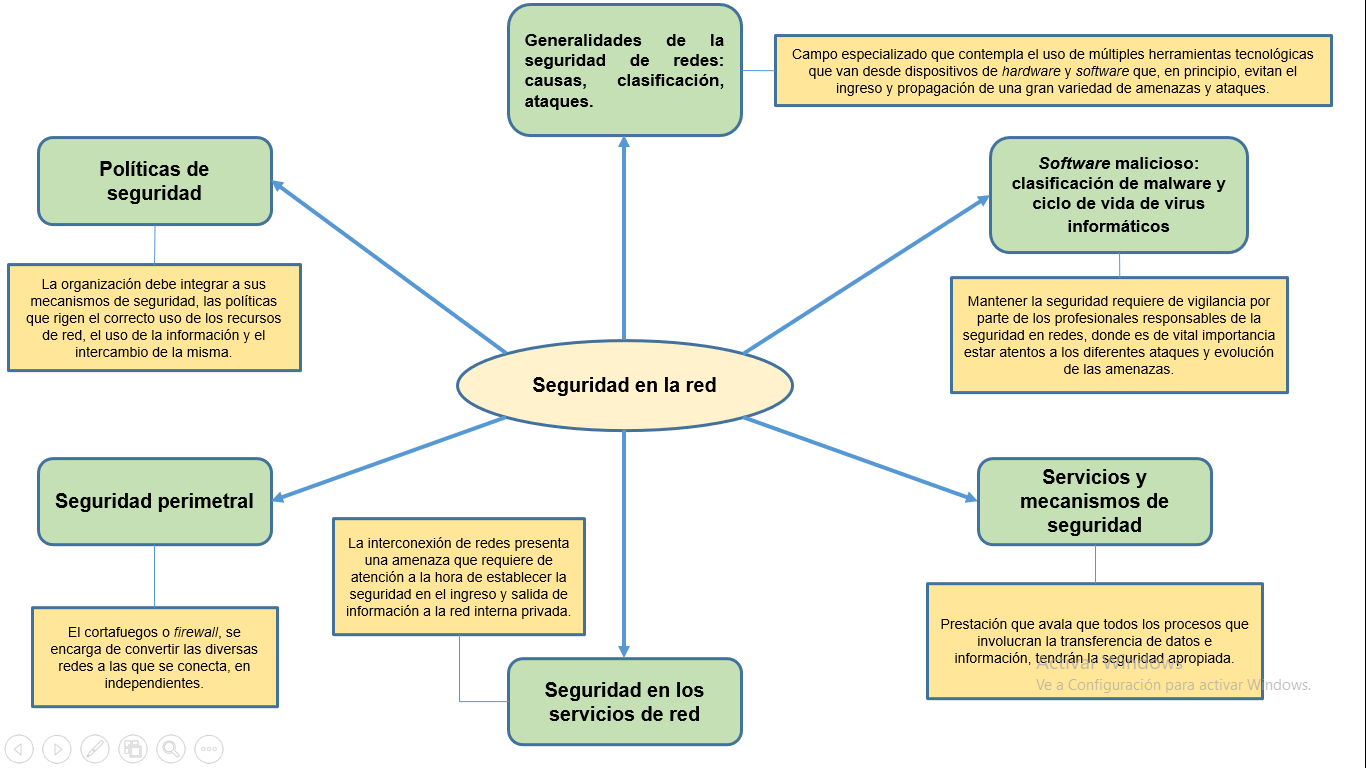
Transferir el riesgo

Para definir una política robusta, eficiente y práctica, es necesario involucrar a todos aquellos usuarios que hacen uso de la red de datos, pues son ellos los que se enfrentarán a los posibles inconvenientes que puedan surgir.

Así mismo, estas políticas o indicaciones deben ser afines a las diligencias que realice la empresa y deben ser indicadas en un lenguaje que pueda ser interpretado o entendido por los usuarios de la malla.

1. **SÍNTESIS**

Uste ha finalizado el estudio de los temas de este componente formativo. En este punto, haga un análisis del mapa conceptual que se muestra enseguida y realice su propia síntesis de los contenidos. ¡**Adelante**!



1. **Actividades didácticas (opcionales si son sugeridas)**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | Asegurando la red |
| Objetivo de la actividad | Reforzar los conceptos, acciones y procedimientos de la gestión de seguridad en la red, con base en los temas desarrollados en el componente formativo. |
| Tipo de actividad sugerida | Falso y verdadero |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Formatos\_DI  Actividad\_didáctica\_1 |

1. **MATERIAL COMPLEMENTARIO:**

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, articulo, otro) | Enlace del Recurso o  Archivo del documento o material |
| 6. Políticas de seguridad | ISOTools. (s.f.). *La norma ISO 27001.* <https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf> | Informe - guía | <https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf> |
| 6. Políticas de seguridad | Procem Consultores. (2018, diciembre 3*). ISO 27001 - Seguridad de la Información*. [Video]. YouTube. <https://youtu.be/BNdPQU32p2Y> | Vídeo | <https://www.youtube.com/watch?v=BNdPQU32p2Y> |

1. **Glosario**

**Agente:** *software* programado para realizar una función específica.

***Cracking*:** acceso no autorizado y/o vandalismo contra los sistemas informáticos.

**Dirección IP:** representado por 32 bits que identifican a un equipo en una red. Se representa en notación decimal o binaria punteada.

**Dispositivo:** pieza de un equipo informático que realiza una función específica.

***Hardware*:** dispositivo, equipo, aparato. Parte física o tangible del ordenador.

***Host*:** dispositivo que participa directamente en la comunicación de la red.

**SNMP:** es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

1. **Referencias bibliográficas**

Ariganello, E. (2020). *Redes cisco - Guía de estudio para la certificación CCNA 200-301*. (1ª Ed.). RAMA.

Beekman, G. (2005). *Introducción a la informática* (traductor Díaz Martín, José Manuel). Pearson educación.

Carpentier, J. F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Ediciones Eni.

Dordoigne, J. (2020). *Redes informáticas: nociones fundamentales (protocolos, arquitecturas, redes inalámbricas, virtualización, seguridad, IPv6...).* Cornellà De Llobregat, Ediciones Eni.

‌MinTIC. (2021). *Hackear*. <https://www.mintic.gov.co/portal/inicio/5307:Hackear>

Soriano, M. (2014). *Seguridad en redes y seguridad de la información*. <https://www.academia.edu/40156122/Seguridad_en_redes_y_seguridad_de_la_informaci%C3%B3n>

Valdivia, C. (2017). *Informática Industrial* 1.ª edición. Ediciones Paraninfo, S.A.

1. **Control del documento**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha |
| Autor (es) | Jorge Eliécer Loaiza Muñoz | Instructor | Regional Antioquia - Centro de Servicios y Gestión Empresarial | Noviembre 2020 |
| Carlos Mauricio Tovar Artunduaga | Instructor | Regional Antioquia - Centro de Servicios y Gestión Empresarial | Noviembre 2020 |
| Cinthia Rocío Trejos Chacón | Experta  Temática | Regional Norte de Santander – Centro de la Industria, la Empresa y los Servicios | Agosto 2021 |
| Fabián Leonardo Correa Díaz | Diseñador instruccional | Regional Santander - Centro Industrial de Diseño y la Manufactura | Septiembre 2023 |
| Rafael Neftalí Lizcano Reyes | Responsable desarrollo curricular Ecosistema RED Santander | Regional Santander - Centro Industrial de Diseño y la Manufactura | Septiembre 2023 |

1. **CONTROL DE CAMBIOS**

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