| PROGRAMA DE FORMACIÓN | Implementación de infraestructura de tecnologías de la información y las comunicaciones |
| --- | --- |

| COMPETENCIA | 220501120 - Controlar el centro de datos de acuerdo con procedimiento técnico y estándares. | RESULTADOS DE APRENDIZAJE | 220501120-4. Ajustar los parámetros y estándares de los dispositivos de la infraestructura TI, según términos de referencia y requerimientos del cliente bajo la normatividad vigente. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 2 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Estándares y normas asociados a infraestructura TI |
| BREVE DESCRIPCIÓN | En esta área se conforman los parámetros y normas que complementan todos los dispositivos que se describen en la infraestructura tecnológica TI teniendo en cuenta el plan de contingencia que describe el diseño y uso para los centros de datos, como utilizar las características de la computación en la nube y la gestión de redes y computadores. |
| PALABRAS CLAVE | Parámetros, dispositivos, T.I, datos, computadores. |

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

**Tabla de contenidos**

**Introducción**

* 1. **Gestión del riesgo informático**

1.1 Niveles y características

1.2 Indicadores y métricas de calidad

1.3 Manuales y procedimientos

1.4. Políticas y normativas

* 1. **Plan de Contingencia**
  2. **Cadena de custodia**
  3. **Gestión de redes de computadoras y recursos tecnológicos**

**Introducción**

| Cuadro de texto |
| --- |
| Estimado aprendiz: en este componente formativo aprenderá sobre la implementación de tecnologías de la información y las comunicaciones, además identificará cómo ajustar los parámetros y estándares de los dispositivos de la infraestructura TI Se tendrán en cuenta definiciones claves sobre el diseño y la implementación del centro de datos alusivo a la infraestructura, la cual deberá ser creada con las consideraciones de diseño de cada cliente. Aprenderá cómo es el funcionamiento del centro de datos, características, normas y estándares con los que podrá seleccionar las conexiones y componentes según su criterio y marcos de referencia ya conocidos; de esta forma, realizará un análisis de medición de riesgos para cumplir con las características del servicio TI  Se desarrollará la capacidad de establecer las conexiones y componentes según las especificaciones técnicas y los marcos de referencia, ejemplificando la parte de infraestructura tecnológica con respecto a la seguridad, con modelos, estándares y normativa que serán implementados para el diseño del centro de datos en función de la infraestructura requerida. Se finalizará con la cuantificación de los riesgos para cumplir con las características del servicio TI, reconociendo las variaciones de ejecución del centro de datos y con base en el desarrollo del proceso. A continuación encontrará un video introductorio donde se amplía la información acerca de las temáticas a desarrollar en el transcurso de todo el componente formativo. |

**Guion de video introductorio**

| **Tipo de recurso** | Video *spot* animado | | | |
| --- | --- | --- | --- | --- |
| **NOTA** | **La totalidad del texto locutado para el video no debe superar las 500 palabras aproximadamente** | | | |
| **Título** | Introducción a Estándares y normas asociados a infraestructura TI | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración (voz en off)** | **Texto** |
| **Escena 1** | Imagen relacionada con la era digital  Dibujado a mano ilustración de metaverso de diseño plano  Fuente: <https://www.freepik.es/vector-gratis/dibujado-mano-ilustracion-metaverso-diseno-plano_22110363.htm#query=era%20digital&position=16&from_view=search&track=aitest>  Imagen: 228116\_i1 | Música de fondo | En la era digital cada vez se tiene más curiosidad sobre cómo brindar soluciones a las necesidades que se presentan. Los tiempos han cambiado y fue notorio cuando se vivió la pandemia de covid-19: todas las costumbres, rutinas y actividades diarias, no fueron lo mismo. Dichos cambios se reflejaron también en el campo laboral, donde el teletrabajo, o modalidad remota, tomó gran relevancia con la utilización de tecnologías y el almacenamiento y trabajo colaborativo como la nube.  Sin embargo, la nube no dio respuesta oportuna a los nuevos desafíos; la poca capacidad de almacenamiento ocasionó la pérdida de mucha información o visibilidad limitada, lo que obstaculizó la sincronización de archivos y ocultó información relevante.  Para nadie es un secreto que tanto personas como empresas no estaban preparadas para tan repentino cambio; algo que pudo generar mayor deserción en la parte laboral y, sobre todo, de los clientes. | Era digital  Cambios repentinos en la actualidad |
| **Escena 2** | Imagen relacionada con infraestructura tecnológica  Composición isométrica del centro de datos  Fuente: <https://www.freepik.es/vector-gratis/composicion-isometrica-centro-datos_4327441.htm#query=infraestructura%20tecnol%C3%B3gica&position=0&from_view=search&track=aitest>  Imagen: 228116\_i2 | Música de fondo | Una solución para el problema mencionado consiste en un esquema de infraestructura que permita ajustar los parámetros y estándares de los dispositivos tecnológicos, según términos de referencia, requerimientos del cliente y la normatividad vigente, es decir, concorde las exigencias que requieran las organizaciones para realizar el diseño y con ayuda de un método que facilite controlar, vigilar y salvaguardar la referencia de las áreas de labor donde la información es recibida por los clientes. Se debe recordar que la infraestructura TI se trata de instrumentos, mejor conocidos como dispositivos, que contienen unos mecanismos, plataformas y también aplicaciones en las que las empresas desarrollan u optimizan todas sus actividades operativas. | Esquema de infraestructura tecnológica |
| **Escena 3** | Imagen relacionada con herramientas de gestión de redes  Hombres con herramientas en  podio  Fuente: <https://www.freepik.es/vector-gratis/hombres-herramientas-podio_1086754.htm#query=herramientas%20de%20gesti%C3%B3n%20de%20redes&position=3&from_view=search&track=aitest>  Imagen: 228116\_i3 | Música de fondo | Dentro de este sistema se debe dirigir a través de las herramientas, por ejemplo, las de gestión de redes, *softwares* y monitoreo; las cuales están configuradas específicamente para cada compañía en específico y asociadas a sus necesidades. Cada nueva tecnología de información tiene un gran impacto en la estrategia sobre los negocios, especialmente de TI, al brindar un soporte a cada estructura definida de trabajo con el usuario o la empresa que adquiere el servicio. Todos los servicios donde se incluye tecnología: sistemas empresariales, aplicaciones, productos inteligentes y registros digitales siempre requieren de la estructura TI como principal objetivo de su eficacia. | Herramientas de gestión de redes |
| **Escena 4** | Imagen relacionada con Infraestructura T.I:  Concepto de vector de red de telecomunicaciones isométrica  Fuente: <https://www.freepik.es/vector-premium/concepto-vector-red-telecomunicaciones-isometrica_18160785.htm#query=infraestructura%20tecnologica&position=5&from_view=search&track=aitest>  Imagen: 228116\_i4 | Música de fondo | La infraestructura TI se asocia a un conjunto de servicios, incluyendo dispositivos físicos con sus respectivas aplicaciones de *software,* que representan cómo cada empresa maneja la información; también se asocia con servicios ágiles para la comunicación con los clientes. | Infraestructura TI  Servicios ágiles para la comunicación con los clientes. |
| **Escena 5** | Imagen relacionada con centro de datos  Ilustración isométrica del centro de datos  Fuente: <https://www.freepik.es/vector-gratis/ilustracion-isometrica-centro-datos_14683454.htm#query=centro%20de%20datos&position=3&from_view=search&track=aitest>  Imagen: 228116\_i5 | Música de fondo | El diseño del centro de datos, o *data center,* consiste en tener el control sobre toda la información enviada y recibida. Teniendo este sistema instalado, cada empresa podrá realizar sin contratiempos las tareas programadas, mantener a sus clientes y controlar el trabajo de los colaboradores. Para ello, la empresa debe adquirir una transformación sobre lo que implica una adaptación de sus recursos y procesos con la finalidad de mejorar la eficiencia y las estructuras y así evitar quedarse atrás en el tiempo y respecto a las nuevas tecnologías que están en pro de beneficiar al usuario y al cliente. | Centro de datos |
| **Nombre del archivo** | 228116\_V1 | | | |

**Desarrollo de contenidos**

* + 1. **Gestión del riesgo informático**

| Cuadro de texto |
| --- |
| Esta área es una organización, por decirlo así, que tiene como objetivo general fortalecer y construir bases muy sólidas para dar cumplimiento a la misión salvaguardando todo activo informático y, sobre todo, la información. Actualmente las empresas deben realizar procesos de adquisición de datos empleando nuevas tecnologías como apoyo en cada una de sus misiones, por esta razón es importante realizar una buena gestión con el objetivo de protegerla de posibles amenazas.  Revisemos a continuación en qué consiste gestionar detalladamente los riesgos en informática y por qué debe existir una buena práctica de ella en todo orden de negocios. |

| **Tipo de recurso** | Acordeón tipo 1 |
| --- | --- |
| **Introducción** | Un riesgo en informática es identificar la gran importancia de gestionarlo para que a futuro se eviten inconvenientes o problemas con los usuarios que incluso terminen en procesos legales. Cuando se realizan estas actividades siempre será más asequible desde la visión de un grupo de colaboradores con conocimiento y expertos; sin embargo, hay ciertas metodologías para prevenir daños en informática que todo responsable del área encargada debe conocer. A continuación se explican: |
| **Fuente:**  **Imagen:** Imagen: 228116\_i6 | |
| **Diseñar controles de seguridad**  Una plataforma informática con controles de seguridad a la medida de la empresa siempre permitirá que se anticipe a los problemas de forma oportuna y efectiva para evitar daños. | |
| **Pruebas de seguridad**  La esencia de la prevención de riesgos informáticos siempre comienza desde la ejecución de pruebas de seguridad para confirmar si están realizando algún daño. Es recomendable hacer con frecuencia cada una de estas pruebas, preferiblemente programadas en el calendario a fin de organizar la información. | |
| **Gestión de los incidentes**  Es importante mantener un historial con cada uno de los riesgos identificados y gestionar estos datos para ser capaces de reaccionar a tiempo y evitar problemas similares a futuro debido a que algunos archivos son afectados desde su raíz. | |
| **Detección y clasificación de vulnerabilidades**  Viéndolo desde un punto más allá, la gestión de seguridad TI, debe ser capaz de detectar y clasificar cada una de las vulnerabilidades a que se expone el sistema de la empresa para reaccionar rápido ante cualquier calamidad. Existen herramientas informáticas capaces de escanear estos riesgos en tiempo real y continuo, entregando reportes constantemente y creando un historial de fallos para identificar la causa que los ocasiona. | |

* 1. **Niveles y características**

| Cuadro de texto |
| --- |
| La gestión del riesgo en la seguridad puede ser dinámica, al serlo permite conocer el estado actual y especificar cada interacción en detalle.  La eficacia del tratamiento del riesgo depende de los resultados de su valoración. Con el paso del tiempo se puede notar que el tratamiento sobre el riesgo no se genera de forma inmediata y el usuario puede no estar conforme con la acción; sin embargo, la constancia de proteger y realizar a diario la actividad hará que mejore con el uso si se realizan cambios en los parámetros del contexto; por ejemplo: criterios para la valoración del riesgo, de aceptación o de impacto. Dentro de la actividad de protección de la información se denota que cuando se realiza la tarea de tratar la seguridad de la información cada movimiento debe estar avalado por la parte directiva, que es la que tiene acceso directo a toda esta información. Esto es especialmente importante en una situación en la que, por costos, la implementación de los controles se omite o se pospone. |

| **Tipo de recurso** | Infografía interactiva Punto caliente | |
| --- | --- | --- |
| **Texto introductorio** | Los niveles de la gestión del riesgo se miden en: | |
| **Fuente:**  **Nota:** rediseñar una imagen similar con 4 personajes para los puntos calientes de la infografía. | | |
| **Código de la imagen** | Imagen: 228116\_i7 | |
| **Punto caliente 1** | Planear: para establecer contexto de lo que se desea proteger realizando una valoración del riesgo al que se expone toda la información. La acción está encaminada a la planificación y aceptación sobre el peligro que se genera en el momento en que la información es subida a la internet. | Persona 1 |
| **Punto caliente 2** | Implementar: se utiliza para realizar la implementación del plan diseñado en el tratamiento de riesgo. | Persona 2 |
| **Punto caliente 3** | Gestionar: en este nivel se debe realizar un monitoreo y la revisión continua de todos los riesgos. | Persona 3 |
| **Punto caliente 4** | Mejora continua: al momento de salvaguardar la información y cuidar los datos nunca será un método o modelo suficiente para mantenerse de una manera estática debido a las posibles amenazas que existen y la vulnerabilidad del proceso de gestión del riesgo en la seguridad de la información (Suscriptor, 2022). | Persona 4 |

**1.2. Indicadores y métricas de calidad**

| **Tipo de recurso** | Infografía estática |
| --- | --- |
| **Texto introductorio** | Cuando es implementado un Sistema de Gestión de Seguridad de la Información (SGSI) y se gestionan unos indicadores se pueden medir planes, presupuestos, programas, personas, procesos, incluso prácticas de negocios, productos, servicios, ventas, proveedores y clientes. Un indicador es una medida que permite una estimación o una evaluación de determinados atributos mediante un modelo analítico, y una metodología para satisfacer ciertas necesidades de información. Los indicadores se pueden clasificar en: |
| Elementos infográficos con dispositivos    Fuente:  Realizar una imagen similar donde se muestren 3 clases de indicadores haciendo referencia a sistemas informáticos, de ahí se desprenden los 3 indicadores. Al final colocar el texto que concluye. | |
| **Código de la imagen** | 228116\_i8 |

| **Tipo de recurso** | Tarjetas avatar | |
| --- | --- | --- |
| **Introducción** | Descripción sobre cómo deberían ser los indicadores eficaces: | |
| 1. Solo se debe medir lo que es importante. | | Logotipo con estadísticas  **Fuente:**  **Imagen:** 228116\_i9 |
| 1. No crear demasiados, pues podría ser contraproducente. | | Logotipo con estadísticas  **Fuente:**  **Imagen:** 228116\_i10 |
| 1. Tener en cuenta que no hay un indicador protagonista, todos son importantes. | | Logotipo con estadísticas  **Fuente:**  **Imagen:** 228116\_i11 |
| 1. Los indicadores deben propiciar un entorno de mejora continua y estar vinculados a los objetivos del SGSI. | | Logotipo con estadísticas  **Fuente:**  **Imagen:** 228116\_i12 |
| 1. No olvidar interpretarlos. | | Logotipo con estadísticas  **Fuente:**  **Imagen:** 228116\_i13 |
| 1. Los indicadores deben englobar procesos importantes o críticos. También tienen que ser fáciles de mantener y utilizar. | | Logotipo con estadísticas  **Fuente:**  **Imagen:** 228116\_i14 |
| 1. Deben ser compatibles con el resto de los indicadores. | | Logotipo con estadísticas  **Fuente:**  **Imagen:** 228116\_i15 |
| 1. Los indicadores deben permitir conocer la situación en tiempo real. | | Logotipo con estadísticas  **Fuente:**  **Imagen:** 228116\_i16 |

| Cuadro de texto |
| --- |
| **Llamado a la acción**  **Indicadores**  En el siguiente documento se explican al detalle los indicadores sobre la gestión del riesgo informático:  **Descargar**  Cuidar la información es importante porque esta es el mayor activo de una empresa; por lo tanto se deben tener mecanismos óptimos para asegurarla y tener indicadores de gestión que permitan minimizar el riesgo de seguridad y a la vez ganar confianza ante los clientes, lo que se traducirá en más clientes y mayores ingresos para la empresa.  Cuando se garantiza una óptima gestión de los indicadores, su cálculo y alimentación, es de gran ayuda un *software* de gestión de la seguridad de la información que permita en todo momento mantener un control total de todo lo relacionado para evitar posibles catástrofes (Suscriptor, 2022) |

**1.2. Manuales y procedimientos**

| **Tipo de recurso** | | Pestañas o *tabs* verticales |
| --- | --- | --- |
| **Introducción** | | **Lineamientos del manual de seguridad informática**  Los presentes lineamientos se dictan con el objeto gestionar adecuadamente la tecnología, los sistemas informáticos y el ambiente tecnológico del Ministerio de Educación Nacional (MEN). |
| Concepto de datos de bolsa  **Fuente:**  **Imagen:** 228116\_i17 | | |
| **Del buen uso y de los activos tecnológicos** | a) Los activos tecnológicos definidos y entregados por la OTSI son:  • Los PC de escritorio y portátiles.  • Impresoras.  • Escáner.  • Teléfonos celulares.  • Carteleras digitales.  Toda esta propiedad del MEN.  b) La OTSI asignará a los colaboradores y a las áreas de acuerdo con la necesidad los activos informáticos necesarios para uso de sus funciones y estos serán los únicos responsables de su utilización, así como también de la información contenida en los mismos, por lo que debe evitar compartirlos. En caso de requerir compartirlo o prestar el activo informático, será́ solamente para cuestiones laborales y sin liberarlo de su responsabilidad.  c) Los PC de escritorio y portátiles se encuentran configurados con el *hardware* y el *software* básicos necesarios para su funcionamiento y cumplimiento de las funciones.  • Sistema operativo: Windows, IOS o Linux.  • Ofimática: Office 365 (Access, Excel, OneNote, One Drive, Outlook, Power Point, Publisher, Word.).  • CA  • ISE  • Descomprimir archivos: Winrar.  • Antivirus • Chat: Skype empresarial o Lync.  • Videoconferencias: Webex.  d) Toda movilización del activo informático dentro o fuera de las instalaciones de la entidad es responsabilidad del colaborador asignado a este.  e) Cuando exista algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa un activo informativo del MEN deberá ser notificado de inmediato a la OTSI mediante la Mesa de Ayuda de Tecnología para que esta informe las acciones a tomar.  f) Solo el personal de la Mesa de Ayuda de Tecnología está autorizado a realizar reparaciones, cambios, desarme de los activos informáticos del MEN.  g) La OTSI realizará periódicamente actualizaciones a los sistemas operativos, parches de seguridad, antivirus y de las aplicaciones instaladas en los PC de escritorio y portátiles de los colaboradores del MEN.  h) Todos los activos tecnológicos propiedad del MEN deberán estar incluidos en el dominio mineducacion.gov.co y aplicar las políticas de seguridad definidas por la OTSI, tales como: un fondo de pantalla definido por el Área de Comunicaciones, acceso al activo tecnológico de acuerdo con su perfil, bloqueo a las propiedades del sistema operativos, entre otros. Todo activo tecnológico que no se encuentre dentro del dominio o no cuente con las políticas de seguridad definidas por la OTSI será solicitado al colaborador por medio de los funcionarios de la Mesa de Ayuda de Tecnología donde estos efectuarán las configuraciones necesarias para cumplir los lineamientos. De negarse el colaborador a entregar el activo tecnológico se informará al jefe inmediato para que este tome las acciones pertinentes o comunique a la OTSI el porqué de la necesidad de que el activo tecnológico se encuentre por fuera del dominio del MEN.  i) Los colaboradores con activos tecnológicos no deben cambiar o eliminar la configuración del *software* de antivirus, *antispyware*, *antimalware*, *antispam* que defina por la Oficina de Tecnología y Sistemas de Información; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios. | |
| **Del internet** | a) La OTSI provee el servicio de internet a todos los colaboradores del MEN para adelantar exclusivamente las funciones asignadas a su cargo y con uso austero y eficiente.  b) Abstenerse de publicar Información relevante al MEN independiente de su formato (Word, Excel, Power Point, PDF, avi, mp3, mp4 o cualquier otro formato actual o futuro) o su nivel de clasificación de confidencialidad en sitios de internet no licenciados por el MEN en los denominados discos, nubes, carpetas virtuales o cualquier sistema de publicación de documentos actual o futura dentro o fuera de la entidad.  c) Abstenerse de utilizar aplicaciones que permitan evadir los controles implementados por el MEN.  d) El acceso a páginas web con contenido inapropiado se encuentra restringido. Sin embargo, y si por la naturaleza del cargo se requiere el acceso a páginas de acceso controlado, se debe solicitar a la Mesa de Ayuda su acceso adjuntando la aprobación y justificación por parte del jefe inmediato.  e) Abstenerse de descargar imágenes, sonidos, música y videos, a su vez descargar archivos o instalar programas de sitios web desconocidos o gratuitos.  f) La OTSI se reserva el derecho a bloquear sitios que se detecten como peligrosos (con contenidos no autorizados) para la seguridad de los activos informáticos.”  g) Cada colaborador es responsable del adecuado manejo de los usuarios de autenticación y contraseña a la hora de ingresar a los diferentes sistemas de información que consulte en internet (Ministerio de Educación Nacional, s/f). | |

| Cuadro de texto |
| --- |
| **Llamado a la acción**  **Información descriptiva del manual de seguridad**  Para continuar conociendo la información descriptiva del manual de seguridad se debe revisar el siguiente enlace [articles-322548\_Manual\_de\_Seguridad\_Informatica\_.pdf (mineducacion.gov.co)](https://www.mineducacion.gov.co/1759/articles-322548_Manual_de_Seguridad_Informatica_.pdf) |

**1.4. Políticas y normativas**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Las políticas de seguridad informática serán aplicadas para las personas que trabajen en entidades públicas o privadas. En el caso del servicio público incluye a todo servidor, pasante y contratista que haga parte del Estado. Para ello se manejan todos los datos inherentes a las organizaciones, incluyendo información de entidades relacionadas con las actividades de recopilación de información, análisis, procesamiento, custodia, recuperación.  Es importante recordar la existencia de unas políticas de seguridad sobre la información para analizar, que se actualizan cada año y garantizan a cada una de las personas que hacen parte de la organización en las que existen, unas pertinencias y durabilidad a la hora de hacer cumplir todas las características y componentes institucionales. También se revisan otras situaciones que se presentan, tales como: cambios culturales, organizacionales, de la parte interna o externa; se incluyen también esos cambios normativos u operativos que lleguen a darse en momentos en que surjan afectaciones en la seguridad de la información de la empresa. Dentro de la normativa se implementan lineamientos, controles o procedimientos determinados con cada detalle técnico cada operación.  **Llamado a la acción**  **Marco normativo**  A continuación se referencian las normas y leyes colombianas que se aplican en el ámbito de seguridad de la información; si alguna de las normas descritas llega a perder validez o fuerza obligatoria, sin importar la razón, las demás disposiciones se van a conservar.  **Descargar** | |

**Responsabilidad por contravención de la política de seguridad**

| Cuadro de texto |
| --- |
| El incumplimiento de las políticas de seguridad de la información descritas en este documento se trata de acuerdo con la naturaleza del incidente. Los resultados de su tratamiento e investigación se producirán una vez los responsables de los trámites institucionales evalúen la necesidad de adelantar procesos disciplinarios o legales si se presentan inconvenientes que se relacionan con la seguridad de la información y los delitos que se comenten en la internet y están asociados a la normatividad vigente.  “Los servidores públicos del Departamento Administrativo de Función Pública que generen algún incidente de seguridad de la información por realizar acciones que contravengan o incumplan alguna de las disposiciones descritas en el presente documento, serán reportados por correo electrónico al Jefe inmediato, al Jefe de la Oficina Asesora de Planeación, al Coordinador del Grupo de Gestión Humana y Jefe de la Oficina de Control Interno, para la revisión del caso y la adopción de las medidas respectivas de acuerdo con las políticas aplicables en la entidad. Respecto a los contratistas y pasantes, estos serán reportados al supervisor del contrato y al director(a), subdirector(a) y jefe de Área, para la revisión del caso y tomar las medidas respectivas [sic]”. (Función pública, 2020) |

1. **Plan de contingencia**

| Cuadro de texto |
| --- |
| Se refiere a la metodología o los pasos que se deben seguir cuando se detecta una falla en el desarrollo normal del sistema de información de una empresa. El funcionario debe informar a su jefe de área para que a su vez este corrobore con el líder de la oficina de sistemas las posibles fallas presentadas, así se determinará que en efecto se trata de una falla informática y no de una falsa alarma. El área de trabajo de la oficina de sistemas evaluará y realizará un dictamen sobre si el daño se presenta en una parte o en la totalidad de la red e informará a los jefes de cada zona, centro y/o líderes de los procesos afectados para que comiencen el uso de los procedimientos y formatos manuales que se describen en las políticas privadas de cada organización y con base en la naturaleza de la tarea que se desarrolle. En caso de un siniestro, un desastre natural o de la pérdida total de comunicación, los coordinadores de centro o líderes de proceso tienen la autonomía para definir en qué momento se deben comenzar a utilizar los procedimientos y formatos manuales en pro de recuperar y salvaguardar la información que aún no haya sido afectada, en aras de empezar el proceso de recuperación de aquella en la que se han generado daños. |

| **Tipo de recurso** | Carrusel de tarjetas | |
| --- | --- | --- |
| **Introducción** | Para concluir, se dice que el plan de contingencia es un documento formal que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC) cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo en la organización. Este plan permite reaccionar sobre las posibles consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible de forma eficiente y oportuna. Así mismo, establecen las acciones a realizar en las siguientes etapas: | |
| Robar el concepto de datos  **Fuente:**  **Imagen:** 228116\_i18 | | |
| - Antes, como un plan de prevención para mitigar los incidentes. | | Icono de prevención  exclamation mark icon vector  **Fuente:**  **Imagen:** 228116\_i19 |
| - Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente. | | Icono de prevención  exclamation mark icon vector  **Fuente:**  **Imagen:** 228116\_i20 |
| - Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia. | | Icono de prevención  exclamation mark icon vector  **Fuente:**  **Imagen:** 228116\_i21 |

1. **Cadena de custodia**

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| **Conceptos, usos y las tendencias del ecosistema tecnológico**  Se asocia a un sistema de control y registro de todo el material utilizado como evidencia de alguna actividad que se considere delictiva. Por ejemplo, la ubicación: en caso de hacer algo incorrecto, existe la cadena de custodia que delata todas las pruebas que confirman la acción mal realizada. Se conocen cinco pasos principales que definen la cadena de custodia.  El proceso de cadena de custodia es uno de los más relevantes en la tecnología ya que es cuando se deben identificar las diferentes responsabilidades y medidas de control relacionadas con el personal que tiene contacto con las evidencias. Para dar cumplimiento hay que redactar un documento donde se indiquen los datos personales completos de todos los involucrados en la manipulación de las copias, desde el momento en que hayan sido creadas a partir de la evidencia, hasta el momento de almacenamiento. Dicho documento debe contener información del cómo, el cuándo, el dónde y el quién tuvo contacto con la evidencia, también sus nombres completos, su cargo, las fechas y horas exactas; en efecto se debe también tener en cuenta registrar los datos de la persona que tuvo bajo custodia la evidencia, el tiempo que esta estuvo bajo su poder y dónde fue guardada. Para tener un consecutivo de trayectoria también es importante que al momento de cambiar de custodio se debe registrar cuándo y cómo se produjo el intercambio, así como los datos de la persona que transportó la evidencia. Todos estos paso a paso son muy importantes y por esta razón debe existir registro completo de toda la actividad.  Por último, la cadena de custodia no es más que mantener y preservar la integridad lógica y física de una posible prueba o evidencia. Esta metodología se debe llevar a cabo desde el mismo instante de la recopilación o registro, su almacenamiento, transporte y análisis hasta culminar con su entrega a las entidades judiciales o a quien corresponda. Es importante tener en cuenta que, en la mayoría de los casos, para que la cadena de custodia sea tomada como válida es necesario que un perito o alguna entidad judicial o del estado certifique que el proceso de custodia se ha llevado de manera correcta. | |

1. **Gestión de redes de computadores y recursos de tecnológicos**

| **Tipo de recurso** | Video *motion* | | | |
| --- | --- | --- | --- | --- |
| **NOTA** | **La totalidad del texto locutado para el video no debe superar las 500 palabras aproximadamente** | | | |
| **Título** | **Tipos de respaldo de información** | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración** | **Texto** |
| **Escena 1** | Imagen relacionada con recuperación de información    Fuente:  Imagen: 228116\_i22 | Música de fondo | En la gestión de respaldo y recuperación de la información es importante identificar y conocer la norma ISO 27000 y ISO/IEC13335-1:2004. Partiendo de este concepto, nos referimos a la información como uno de los activos más importantes para una empresa. Así mismo se relaciona lo que comprende la información, bases de datos y archivos de data, contratos y acuerdos, documentación del sistema, información de investigaciones, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, acuerdos para contingencias, rastros de auditoría e información archivada. Por ello, la información tiene tres pilares importantes, los cuales hay que cuidar y mantener. Estos son confidencialidad, integridad y disponibilidad. (ISO/IEC 13335-1:2004). | Gestión de respaldo y recuperación de la información |
| **Escena 2** | Una imagen relacionada con tipos de almacenamiento informático  Ilustración de estilo isométrico sobre el servicio de notificación y el almacenamiento del servidor en la nube Fuente:  Imagen: 228116\_i23 | Música de fondo | Según las necesidades de cada empresa, se dispone de varios tipos de almacenamiento. A continuación se nombran: | Tipos de almacenamiento |
| **Escena 3** | Imagen relacionada con copia de seguridad  Diseño de fondo de negocios  Fuente:  Imagen: 228116\_i24 | Música de fondo | **Copia de seguridad completa**: se realiza la copia de toda la información que el usuario desee guardar. Esta copia de seguridad requiere mayor capacidad y espacio de almacenamiento. Se recomienda realizar copias de preferencia completas de forma periódica; por ejemplo, cada semana, o cada tres días; dependerá de las necesidades que tenga cada usuario. Cuando pasa mucho tiempo desde la copia de seguridad que recién fue guardada muy probablemente muchos archivos hayan cambiado. Por eso hay que llegar a un equilibrio, para evitar que las copias intermedias acaben siendo tan grandes como una copia completa. | Copia de seguridad completa |
| **Escena 4** | Imagen relacionada con copia de seguridad  Delegar deberes y responsabilidades a los compañeros  Fuente:  Imagen: 228116\_i25 | Música de fondo | **Copia de seguridad incremental:** consiste en laoperación de respaldo que se genera de forma incremental. Copia solamente la información que ha cambiado con respecto al último trabajo, el último *backup* (copia de seguridad) de cualquier referencia. Casi siempre se usa la fecha y hora de la última modificación realizada. Todos esos procesos que brindan el respaldo sirven para identificar aquellos registros sobre la realización de las operaciones. | Copia de seguridad incremental |
| **Escena 5** | Imagen relacionada con copia de seguridad    Fuente:  Imagen: 228116\_i26 | Colocar si habrá un sonido o música de fondo | **Copia de seguridad diferencial**: es cuando se guardan los últimos cambios realizados en los trasuntos completos de datos, entonces solo tiene dependencia de los respaldos completos.  Es decir, que una operación de recuperación, en el momento que es diferencial, se comporta de una forma muy parecida al respaldo incremental en el primer momento debido a que se realizan réplicas de todos los datos que en los últimos segundos se añadieron desde su última copia de seguridad. Es importante tener presente que, cuando se comienza a ejecutar, continuará copiando todos los datos que hayan cambiado desde el respaldo completo anterior. Por esta razón, las acciones consiguientes van a almacenar más información con una recuperación que incrementa, aunque normalmente sea menos que un completo *backup* incremental y mucho menos que un *backup* completo. | Copia de seguridad diferencial |
| **Escena 6** | Imagen relacionada con *backup*  Sincronización del servidor en la nube con todos los dispositivos, teléfono, tableta, computadora portátil, aislado en blanco  Fuente:  Imagen: 228116\_i27 | Música de fondo | Cada copia de seguridad suele funcionar de distinta manera. Las compañías deben realizar una copia de seguridad completa al menos una vez al año debido a la cantidad de información que se maneja. Después podrán generar respaldos diferenciales, completos o incluso parciales cada mes, por ejemplo. Cuando se genera el primer *backup* de forma parcial, incremental o diferencial, siempre se van a guardar los mismos datos. | *Backup* |
| **Nombre del archivo** | 228116\_v2 | | |  |

| Cuadro de texto |
| --- |
| Cuando se presenta un tercer movimiento u operación de respaldo, aquella información que se copia de forma incremental limitará esos cambios realizados en el último respaldo incremental. Sin embargo, cuando se presenta el tercer *backup,* donde está ese respaldo diferencial, siempre se copiará con referencia al primer *backup*.  En conclusión, la tecnología día a día brinda mayores soluciones a las necesidades de cada persona, siendo parte de las actividades cotidianas y, principalmente, de nuestro trabajo. Desde que se produjo la pandemia, el cambio a los trabajos remotos aumentó de manera exponencial, por esa razón las redes tecnológicas están siempre renovando y actualizando su portafolio para brindar un mejor servicio a sus clientes.  Tener el control de la información permite operar y gestionar los entornos TI empresariales, incluidos todos los elementos de red, *software, hardware* y, en especial, el almacenamiento de datos; así se ofrecen al cliente servicios y soluciones con alternativa tecnológica, que se ajustan a los parámetros y estándares basados en las normas que conforman los dispositivos y que utilizan plataformas y entornos que ayudan a la gestión de los datos obtenidos. La simplicidad es la clave de un ecosistema de TI más seguro y eficiente cuando se implementa una infraestructura basada en las tecnologías de fácil acceso y comunicación con la empresa y el cliente.  Con estos métodos se garantizan mayor efectividad y rapidez al obtener la información y se consolida un apoyo en torno a las organizaciones al velar por sus intereses con un sistema automatizado que permita confiar cuando se deba subir información y se necesite tener retroalimentación efectiva para la utilización de los datos.  Estimado aprendiz: ha culminado satisfactoriamente el estudio del componente Estándares y normas asociados a infraestructura TI, lo invitamos a que revise los materiales complementarios y a realizar la actividad didáctica para que afiance sus conocimientos frente a los contenidos vistos. |

**Síntesis**

| **Tipo de recurso** | Síntesis |
| --- | --- |
| Implementación de infraestructura de tecnologías de la información y las comunicaciones.  Síntesis: Estándares y normas asociados a infraestructura TI | |
| **Introducción** | A continuación encontrará una síntesis que le permitirá hacer un repaso general de todas las temáticas vistas. |
| Textos de la síntesis | |

**Actividad didáctica**

| **Tipo de recurso** | Actividad didáctica. Opción múltiple | |
| --- | --- | --- |
| Con esta actividad didáctica podrá afianzar sus conocimientos relacionados con los Estándares y normas asociados a infraestructura TI. ¡Mucho ánimo! | | Imagen relacionada con normas y estándares tecnológicos    Fuente:  **Imagen:** 228116\_i28 |
| 1. ¿Cuáles son las metodologías para prevenir daños informáticos?  Retroalimentación positiva:  **¡Muy bien!** Realizar pruebas de seguridad y diseñar controles de seguridaden una plataforma informática a la medida de la empresa siempre permitirá que se anticipe a los problemas de forma oportuna y efectiva para evitar daños.  Retroalimentación negativa:  **La respuesta es incorrecta.** Entre las metodologías para prevenir los daños informáticos se encuentran las pruebas de seguridad, diseño de controles de seguridad, gestión de los incidentes, detección y clasificación de vulnerabilidades. Lo invitamos a seguir repasando el componente formativo. | | La misma imagen |
| 1. Pruebas de seguridad, diseñar controles de seguridad, gestión de los incidentes, detección y clasificación de vulnerabilidades. (correcta) | | 1. Clasificación de los virus, gestión de los incidentes, asistencia remota. |
| 1. Detección y clasificación de vulnerabilidades, controles de seguridad, asistencia telepresencial. | | 1. Ninguna de las anteriores. |
| 2. ¿Qué es un nivel y característica en gestión del riesgo?  Retroalimentación positiva:  **¡Muy bien!** La eficacia del tratamiento de tratamiento del riesgo depende de los resultados de su valoración. Con el paso del tiempo se puede llegar a notar que el tratamiento sobre el riesgo no se genera de forma inmediata, de manera que el usuario no estará conforme con la acción.  Retroalimentación negativa:  **La respuesta es incorrecta.** La eficacia del tratamiento del riesgo depende de los resultados de su valoración. Con el paso del tiempo se puede llegar a notar que el tratamiento sobre el riesgo no se genera de forma inmediata, de manera que el usuario no estará conforme con la acción. Lo invitamos a seguir repasando el componente formativo. | | La misma imagen |
| 1. Depende siempre del resultado de valoración que permite realizar un protocolo, identificando la posición de cada amenaza que ponga en riesgo la información. (correcta) | | 1. Sirve para identificar para qué se utiliza la gestión del riesgo. |
| 1. Funciona como identificador de riesgo en la empresa. | | 1. Ninguna de las anteriores. |
| 3. ¿Cuáles son los elementos con los que se miden los niveles de la gestión del riesgo?  Retroalimentación positiva:  **¡Muy bien!** Los elementos indispensables para medir los niveles de la gestión de riesgo son planear, gestionar, implementar, mejora continua.  Retroalimentación negativa:  **La respuesta es incorrecta.** Los elementos indispensables para medir los niveles de la gestión de riesgo son planear, gestionar, implementar, mejora continua. Lo invitamos a seguir repasando el componente formativo. | | La misma imagen |
| 1. Gestionar, comprar, identificar y comparar. | | 1. Implementar, comunicar, conocer y saber. |
| 1. Planear, gestionar, implementar, mejora continua. (correcta) | | 1. Recomendar, gestionar, implementar, conocer. |
| 4. ¿Qué característica tiene un indicador de calidad?  Retroalimentación positiva:  **¡Muy bien!** Cuando es implementado un sistema de gestión de seguridad de la información (SGSI), y se gestionan unos indicadores, se pueden medir planes, presupuestos, programas, personas, procesos, incluso prácticas de negocios, productos, servicios, ventas, proveedores y clientes.  Retroalimentación negativa:  **La respuesta es incorrecta.** Cuando es implementado un sistema de gestión de seguridad de la información (SGSI), y se gestionan unos indicadores, se pueden medir planes, presupuestos, programas, personas, procesos, incluso prácticas de negocios, productos, servicios, ventas, proveedores y clientes. Lo invitamos a seguir repasando el componente formativo. | | La misma imagen |
| 1. Permite medir la cantidad de amenazas que se presentan. | | 1. Indica qué está bien y mal en la gestión del riesgo. |
| 1. Permite medir planes, presupuestos, programas, procesos y prácticas de negocios. (correcta) | | 1. Ninguna de las anteriores. |
| 1. El plan de contingencia sirve para:   Retroalimentación positiva:  **¡Muy bien!** El plan de contingencia sirve paradetectar una falla en el desarrollo normal del sistema de información de una empresa. El funcionario debe informar a su jefe de área para que a su vez este confirme con el líder de la oficina de sistemas las posibles fallas presentadas; así se podrá corroborar que efectivamente se trata de una falla informática y no de una falsa alarma.  Retroalimentación negativa:  **La respuesta es incorrecta.** El plan de contingencia sirve paradetectar una falla en el desarrollo normal del sistema de información de una empresa. El funcionario debe informar a su jefe de área para que a su vez este confirme con el líder de la oficina de sistemas las posibles fallas presentadas; así se podrá corroborar que efectivamente se trata de una falla informática y no de una falsa alarma. Lo invitamos a seguir repasando el componente formativo. | | La misma imagen |
| 1. Acomodar las posibles herramientas para la gestión del riesgo que se presenta en las empresas. | | 1. Detectar una falla que se presenta en el sistema con un archivo determinado que contiene información. (correcta) |
| 1. Generar códigos de protección con base en todo lo realizado en gestión. | | 1. Incluir los pasos que se realizan para desproteger el sistema cuando se presenta una amenaza. |
| 1. La cadena de custodia es:   Retroalimentación positiva:  **¡Muy bien!** La cadena de custodia es el control y registro de todo el material probatorio. Está asociada a un sistema de control y registro de todo el material utilizado como evidencia de alguna actividad que se considere delictiva.  Retroalimentación negativa:  **La respuesta es incorrecta.** La cadena de custodia es el control y registro de todo el material probatorio. Está asociada a un sistema de control y registro de todo el material utilizado como evidencia de alguna actividad que se considere delictiva. Lo invitamos a seguir repasando el componente formativo. | | La misma imagen |
| 1. Todo material probatorio que sirva como evidencia para explicar qué es gestión de riesgo. | | 1. De uso general de materiales probatorios para ser más eficiente en la gestión. |
| 1. El manual de uso de los programas. | | 1. El control y registro de todo el material probatorio que permita usarse como evidencia. (correcta) |
| 1. Los tipos de respaldos que existen son:   Retroalimentación positiva:  **¡Muy bien!** Los tipos de respaldo que existen son copia de seguridad completa, copia de seguridad diferencial y copia de seguridad incremental.  Retroalimentación negativa:  **La respuesta es incorrecta.** Los tipos de respaldo que existen son copia de seguridad completa, copia de seguridad diferencial y copia de seguridad incremental. Lo invitamos a seguir repasando el componente formativo. | | La misma imagen |
| 1. Copia de seguridad medio llena, copia de seguridad completa y copia de seguridad incremental. | | 1. Copia de seguridad diferencial, copia de seguridad incremental y copia de seguridad integral. |
| 1. Copia de seguridad completa, copia de seguridad diferencial y copia de seguridad incremental. (correcta) | | 1. Ninguna de las anteriores. |
| 1. La copia diferencial es:   Retroalimentación positiva:  **¡Muy bien!** La copia de seguridad diferencial es cuando se guardan los últimos cambios realizados en los trasuntos completos de datos, entonces solo tiene dependencia de los respaldos completos.  Retroalimentación negativa:  **La respuesta es incorrecta.** La copia de seguridad diferencial es cuando se guardan los últimos cambios realizados en los trasuntos completos de datos, entonces solo tiene dependencia de los respaldos completos.  Lo invitamos a seguir repasando el componente formativo. | | La misma imagen |
| 1. Cuando se guardan los últimos cambios realizados en un archivo. (correcta) | | 1. La copia general de todos los archivos del sistema. |
| 1. Un tercio de la información de un archivo. | | 1. La copia de seguridad parcial. |
| 1. ¿Qué es la gestión de incidentes?   Retroalimentación positiva:  **¡Muy bien!** En la gestión de incidentes es importante mantener un historial con cada uno de los riesgos identificados. Gestionar estos datos permitirá reaccionar a tiempo y evitar problemas similares a futuro.  Retroalimentación negativa:  **La respuesta es incorrecta.** En la gestión de incidentes es importante mantener un historial con cada uno de los riesgos identificados. Gestionar estos datos permitirá reaccionar a tiempo y evitar problemas similares a futuro. Lo invitamos a seguir repasando el componente formativo. | | La misma imagen |
| 1. Es la vulnerabilidad que se presenta cuando se conecta a la red. | | 1. Tener precaución para no cometer errores. |
| 1. Mantener el historial de gestión del riesgo y saberlo gestionar a tiempo. (correcta) | | 1. Todas las anteriores. |
| 1. La prueba de seguridad sirve para:   Retroalimentación positiva:  **¡Muy bien!** La esencia de la prevención de riesgos informáticos siempre comienza desde la ejecución de pruebas de seguridad para confirmar si están realizando algún daño. Es recomendable hacer con frecuencia cada una de estas pruebas, preferiblemente programadas en el calendario para que se pueda organizar la información.  Retroalimentación negativa:  **La respuesta es incorrecta.** La esencia de la prevención de riesgos informáticos siempre comienza desde la ejecución de pruebas de seguridad para confirmar si están realizando algún daño. Es recomendable hacer con frecuencia cada una de estas pruebas, preferiblemente programadas en el calendario para que se pueda organizar la información. Lo invitamos a seguir repasando el componente formativo. | | La misma imagen |
| 1. Confirmar si efectivamente se está presentando un daño. (correcta) | | 1. Realizar los controles de seguridad. |
| 1. Monitorear el sistema. | | 1. Todas las anteriores. |

**Material complementario**

| **Tipo de recurso** | **Material complementario** | | |
| --- | --- | --- | --- |
| **Tema** | **Referencia APA del material** | **tipo** | **Enlace** |
| Introducción a las redes de datos | (S/a-a). Com.ar. Recuperado el22 de octubre de 2022, de <https://docer.com.ar/doc/s0s0n50> | Manual | <https://docer.com.ar/doc/s0s0n50> |
| Conceptos de redes de computadoras | (S/a-b). Com.ar. Recuperado el 22 de octubre de 2022, de <https://docer.com.ar/doc/s0s0n1c> | Artículo | <https://docer.com.ar/doc/s0s0n1c> |
| Introducción a la informática *hardware* y *software*. | (S/a-c). Edu.ar. Recuperado el 18de agosto de 2022, de <https://economicas.unsa.edu.ar/sigeco/archivos/semi_material/U1-DT-IntroduccionalaInformatica.pdf> | Manual | <https://economicas.unsa.edu.ar/sigeco/archivos/semi_material/U1-DT-IntroduccionalaInformatica.pdf> |
| Documento - versión actualizada del modelo de gestión it4+ | (S/a-d). Gov.co. Recuperado el 18 de agosto de 2022, de <https://www.mintic.gov.co/arquitecturati/630/propertyvalues-8170_documento_pdf.pdf> | Manual | <https://www.mintic.gov.co/arquitecturati/630/propertyvalues-8170_documento_pdf.pdf> |
| Data Center una mirada por dentro. | (S/a-e). Researchgate.net. Recuperado el 18 de agosto de 2022, de <https://www.researchgate.net/publication/282611136_DATACENTER_-_UNA_MIRADA_POR_DENTRO> | Manual | <https://www.researchgate.net/publication/282611136_DATACENTER_-_UNA_MIRADA_POR_DENTRO> |

**Glosario**

| **Tipo de recurso** | Glosario |
| --- | --- |
| Activo: | cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.), que tenga valor para la organización. |
| Activo de Información: | recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso, o que tiene relación directa o indirecta con las funciones de la entidad: *software*, *hardware*, personas (roles), físicos (instalaciones, áreas de almacenamiento de expedientes, centros de procesamiento de datos), intangibles (imagen y reputación). |
| Amenaza: | causa potencial de un incidente no deseado que pueda provocar daños a un sistema o a la organización. |
| Contingencia: | se asocia a la posibilidad de que una acción suceda o no. |
| *Data center*: | centro de proceso de información. Lugar físico donde se guardan los datos e información relevante. |
| DNS: | sistema de nombre de dominios. |
| *Firewalls:* | sistema diseñado para proteger redes privadas. |
| LAN: | red de área local. |
| *Racks:* | soportes metálicos para guardar y almacenar centros de información. |
| RRHH: | recursos humanos. |
| Salvaguardar: | proteger algo que requiera protección. |

**Referentes bibliográficos**

| **Tipo de recurso** | Bibliografía |
| --- | --- |
| Cloudflare. (s.f.). *Cloudflare.com.* Recuperado el 8 de octubre de 2022, de https://www.cloudflare.com/learning/network-layer/what-is-routing/ | |
| Función Pública. (marzo de 2020). *Funcionpublica.gov.co.* Recuperado el 21 de octubre de 2022, de <https://www.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?t=1586355315672> | |
| Importancia de la gestión de riesgos informáticos. (2019, agosto 26). Hacknoid. <https://www.hacknoid.com/hacknoid/importancia-de-la-gestion-de-riesgos-informaticos/> | |
| Ministerio de Educación Nacional. (s.f.). *Manual de seguridad informática.* Bogotá, Colombia. Recuperado el 29 de octubre de 2022, de <https://www.mineducacion.gov.co/1759/articles-322548_Manual_de_Seguridad_Informatica_.pdf> | |
| Ramírez Riveros , D. A., & Castro Serrato, E. F. (2018). Recuperado el 22 de octubre de 2022, de <https://repository.unad.edu.co/bitstream/handle/10596/17370/86078250.pdf?sequence=1&isAllowed=y> | |
| Suscriptor. (2022, mayo 13). *Indicadores más útiles para un sistema de gestión de seguridad de la información*. Software ISO. [https://www.isotools.org/2022/05/13/indicadores-mas-utiles-para-un-siUn indicador stema-de-gestion-de-seguridad-de-la-informacion/](https://www.isotools.org/2022/05/13/indicadores-mas-utiles-para-un-siUn%20indicador%20stema-de-gestion-de-seguridad-de-la-informacion/) | |