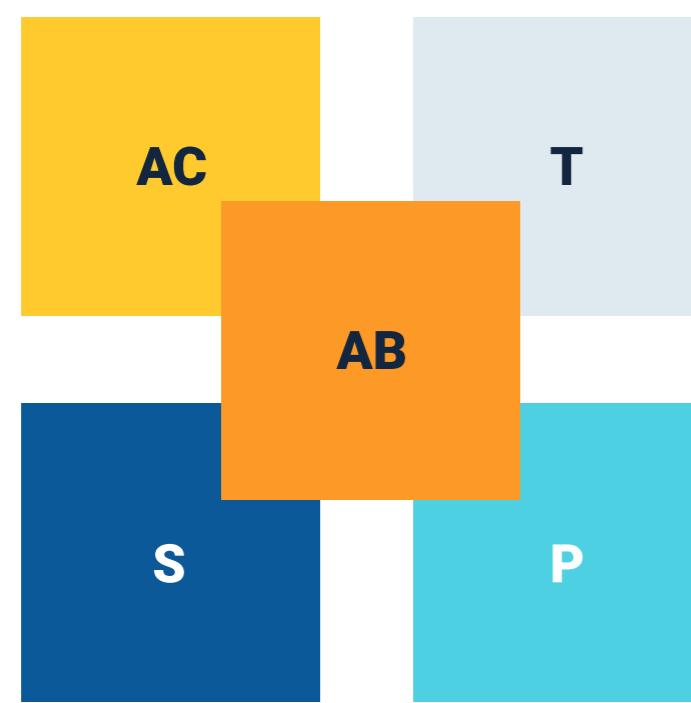


# Monitoreo a la infraestructura T.I según normativa vigente

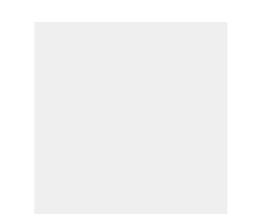
En este componente formativo se abordan los conceptos necesarios para realizar monitoreo al centro de datos cumpliendo con las normativas vigentes.

[Iniciar >](#)

PRIMARIO  
#4DD0E1



SECUNDARIO  
#0B5999



NEUTRAL 1  
#EFEFEF



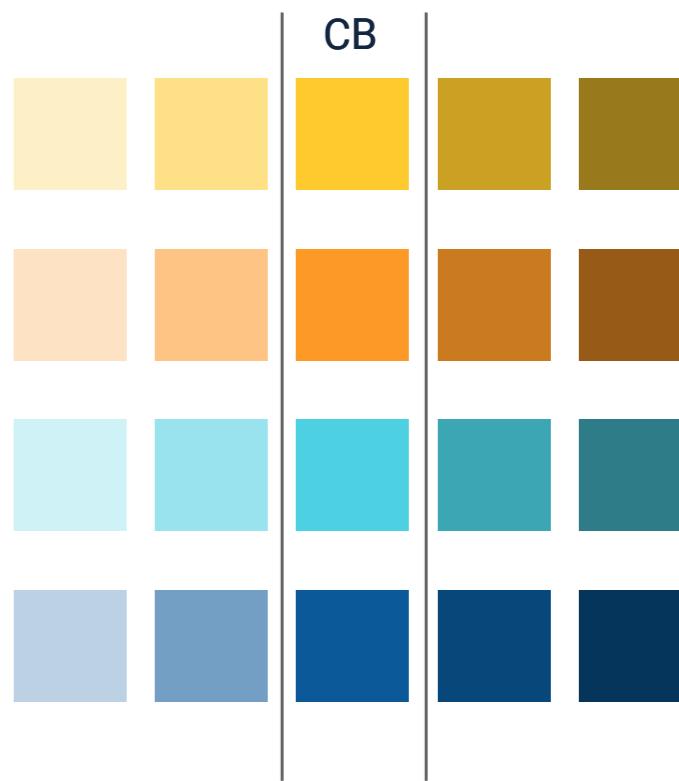
ACENTO CONTENIDO  
#FECA2E



ACENTO BOTONES  
#FD9927



NEUTRAL 2  
#F9F7EC



## i Introducción

Cada edificación posee un diseño que lo hace único, por ello podemos reconocer en fotografías el Burj Khalifa en Emiratos Árabes o el One World Trade Center ubicado en Estados Unidos, cada arquitecto plasma en ellos un patrón que permite integrarlo al contexto en el que se encuentre; de la misma manera diseñará un espacio en el cual se controle toda la parte lógica del edificio en un solo espacio y para ello se deben tener presentes las normativas y estándares internacionales que permitan su administración y control evitando el colapso de todo el sistema de información.

Este componente formativo aborda la temática del monitoreo del centro de datos según la normatividad vigente; a través de la apropiación de conceptos claves, se reconocerán los estándares internacionales que permiten administrar las variables del centro de datos, así evitar caídas del sistema y errores humanos que afecten el normal funcionamiento y operación de la empresa.



Este componente formativo aborda la temática del monitoreo del centro de datos según la normatividad vigente; a través de la apropiación de conceptos claves, se reconocerán los estándares internacionales que permiten administrar las variables del centro de datos, así evitar caídas del sistema y errores humanos que afecten el normal funcionamiento y operación de la empresa.

Comprender la importancia de las contingencias, evaluar las causas de los incidentes, aplicar buenas prácticas en el ejercicio administrativo del centro de datos, llevar bitácoras e inventarios de los equipos que integran la infraestructura TI, además de reconocer el correcto manejo de residuos, son algunos de los temas que serán tratados.

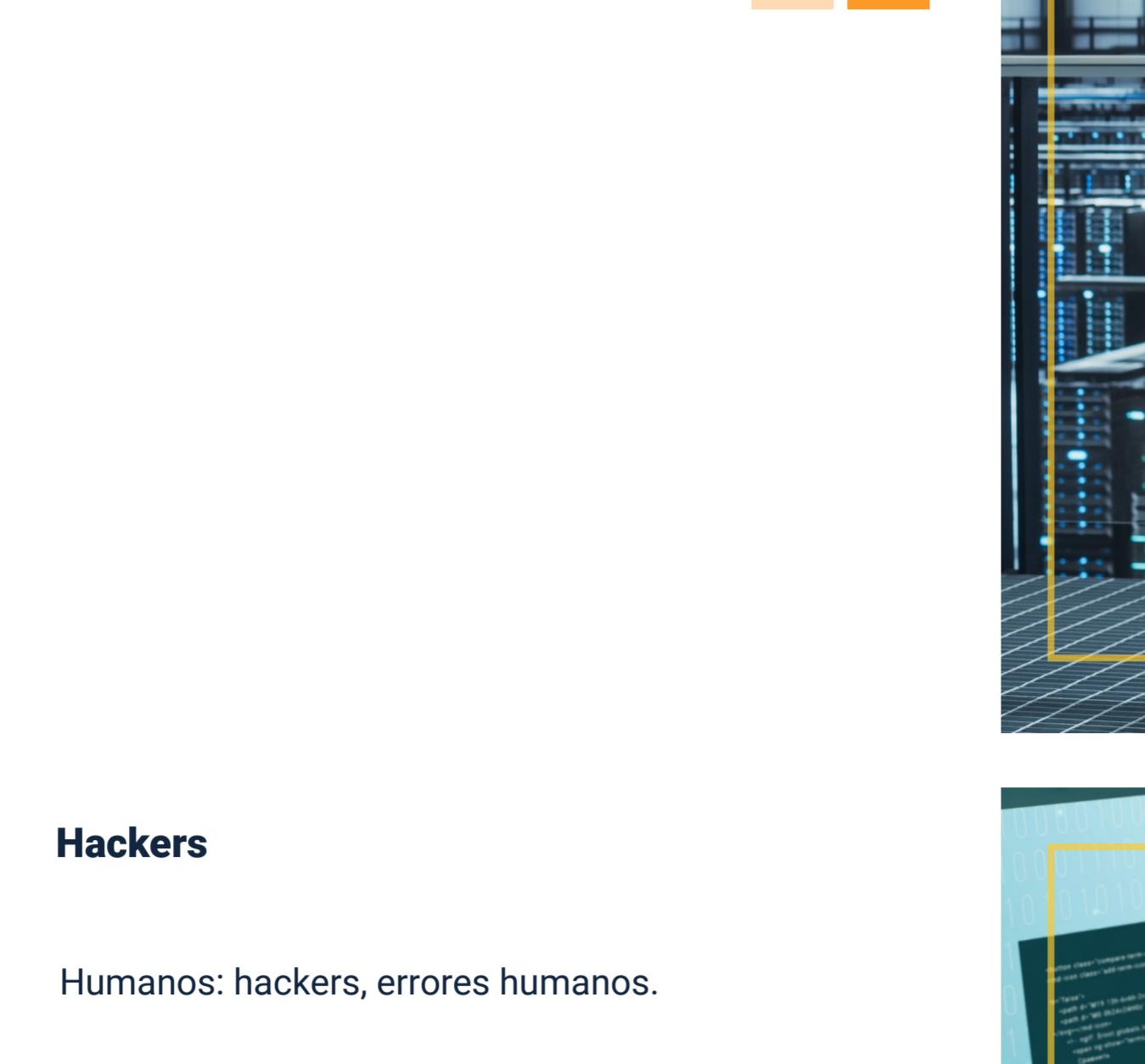
Extendemos una invitación a leer el material y apropiarse de los conceptos aquí inmersos, serán de gran aporte en su formación y le permitirán reconocer y aplicar las normativas vigentes para el monitoreo a los centros de datos, implementar buenas prácticas de seguridad y salud en el trabajo, además del manejo medioambiental de los residuos.

En el siguiente video conocerá, de forma general, la temática que estudiará a lo largo del componente formativo. ¡Muchos éxitos en este proceso de aprendizaje!  
¡Bienvenido!



## 1 Establecer procesos de monitoreo

Conocer las principales causas de fallas en el centro de datos permite prevenirlas y garantizar la continuidad del servicio, según estadísticas del Instituto Ponemon, algunas razones son: "fallas en UPS, hackers, errores humanos, problemas en el aire acondicionado y sistemas climáticos, fallas en la planta de emergencia y fallas en los equipos de TI", todas ellas asociadas a la infraestructura tecnológica.



Se requiere reconocer que el tiempo en el que se encuentre fuera el sistema de información directamente está relacionado con pérdidas y hasta tanto las organizaciones no tengan presente este principio, no darán la importancia que merece el centro de datos como columna vertebral de la infraestructura tecnológica, pues en él se encuentran ubicados todos los componentes que permiten que los sistemas de información operan.

### Clasificación de la información

Ahora, analizando la información de Ponemon, se pueden clasificar las novedades de la siguiente manera:

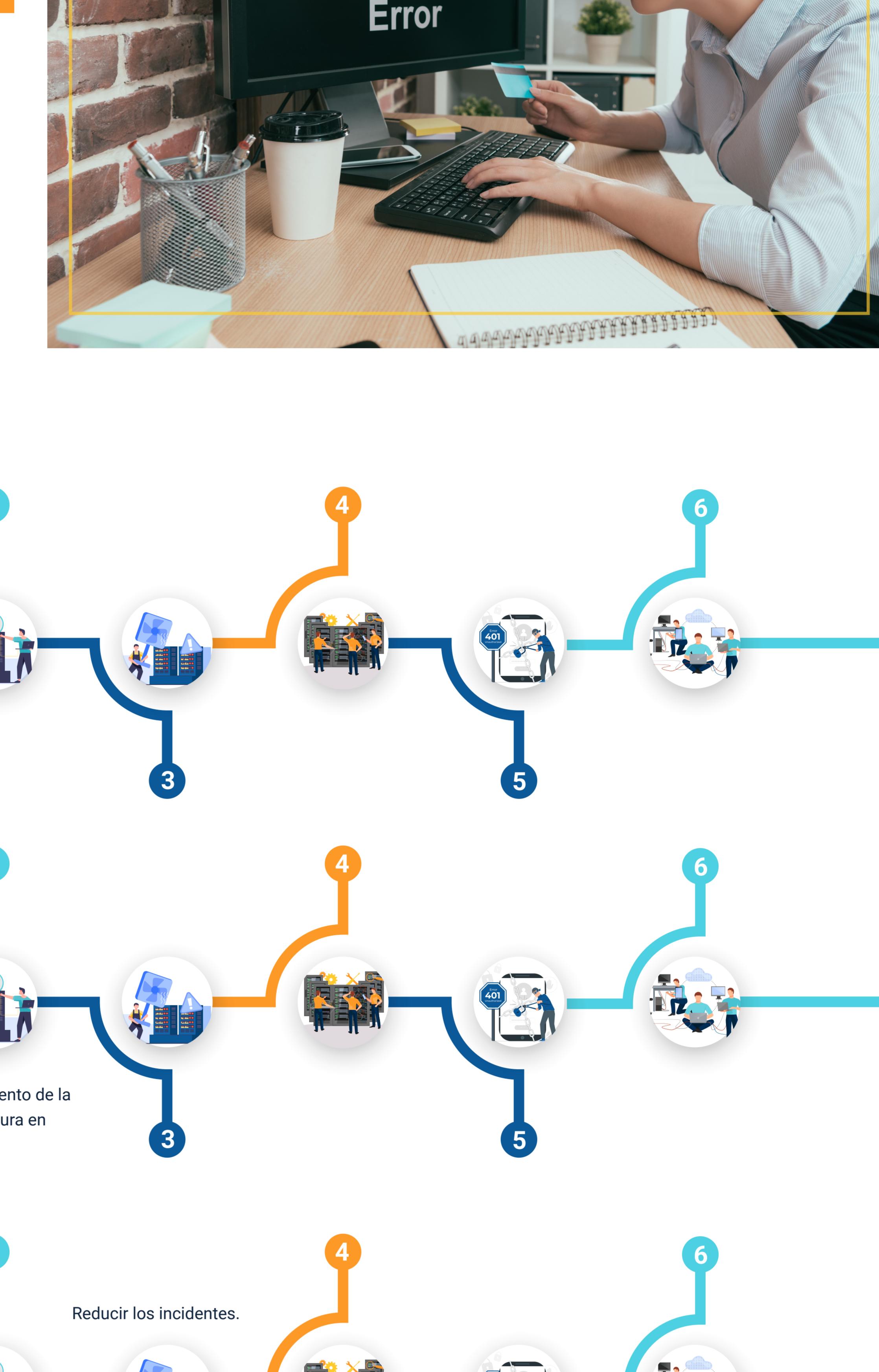
1 / 4



### Hackers

Humanos: hackers, errores humanos.

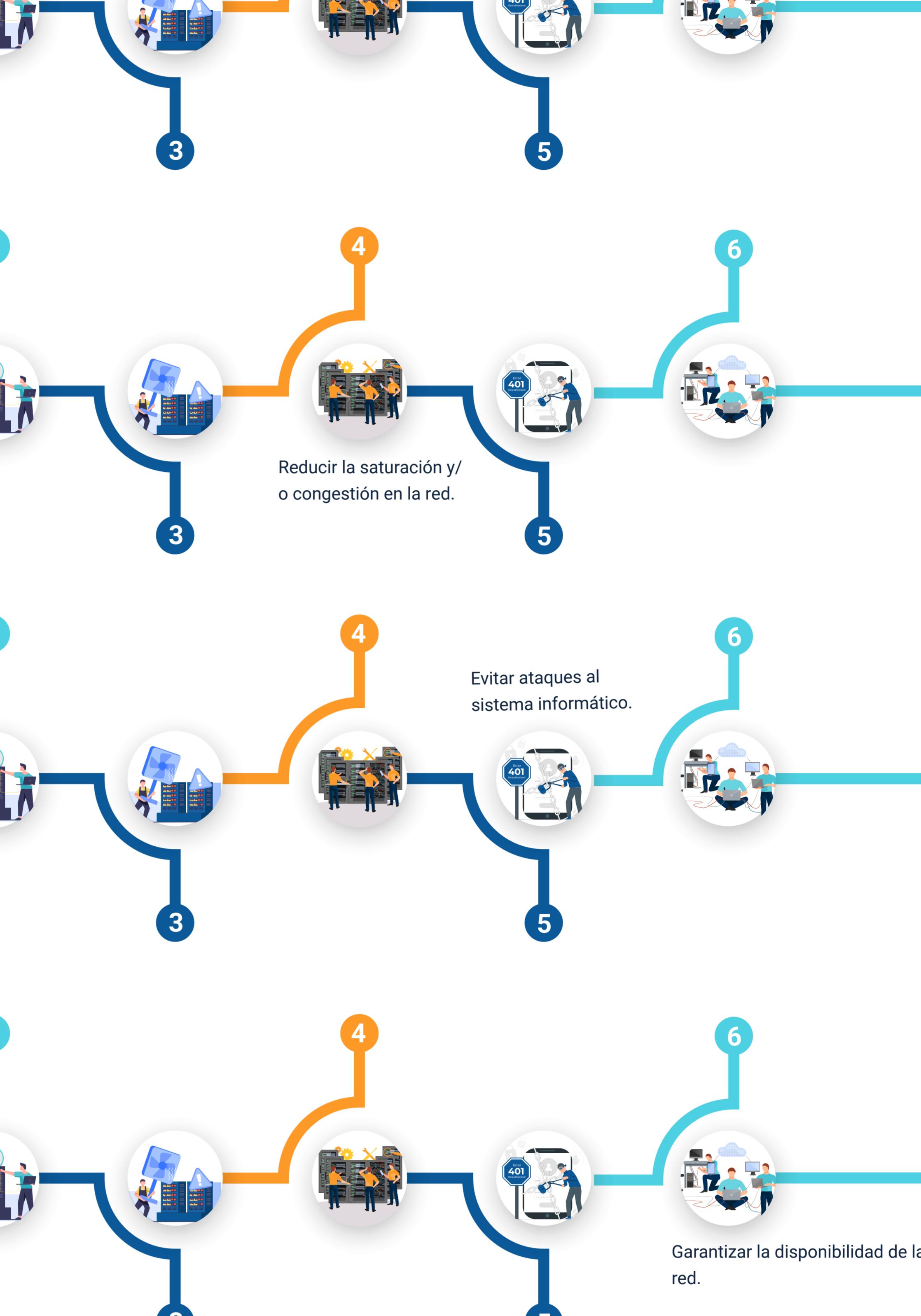
2 / 4



### Infraestructura

Infraestructura: UPS, aire acondicionado, planta de emergencia, fallas en los equipos TI.

3 / 4



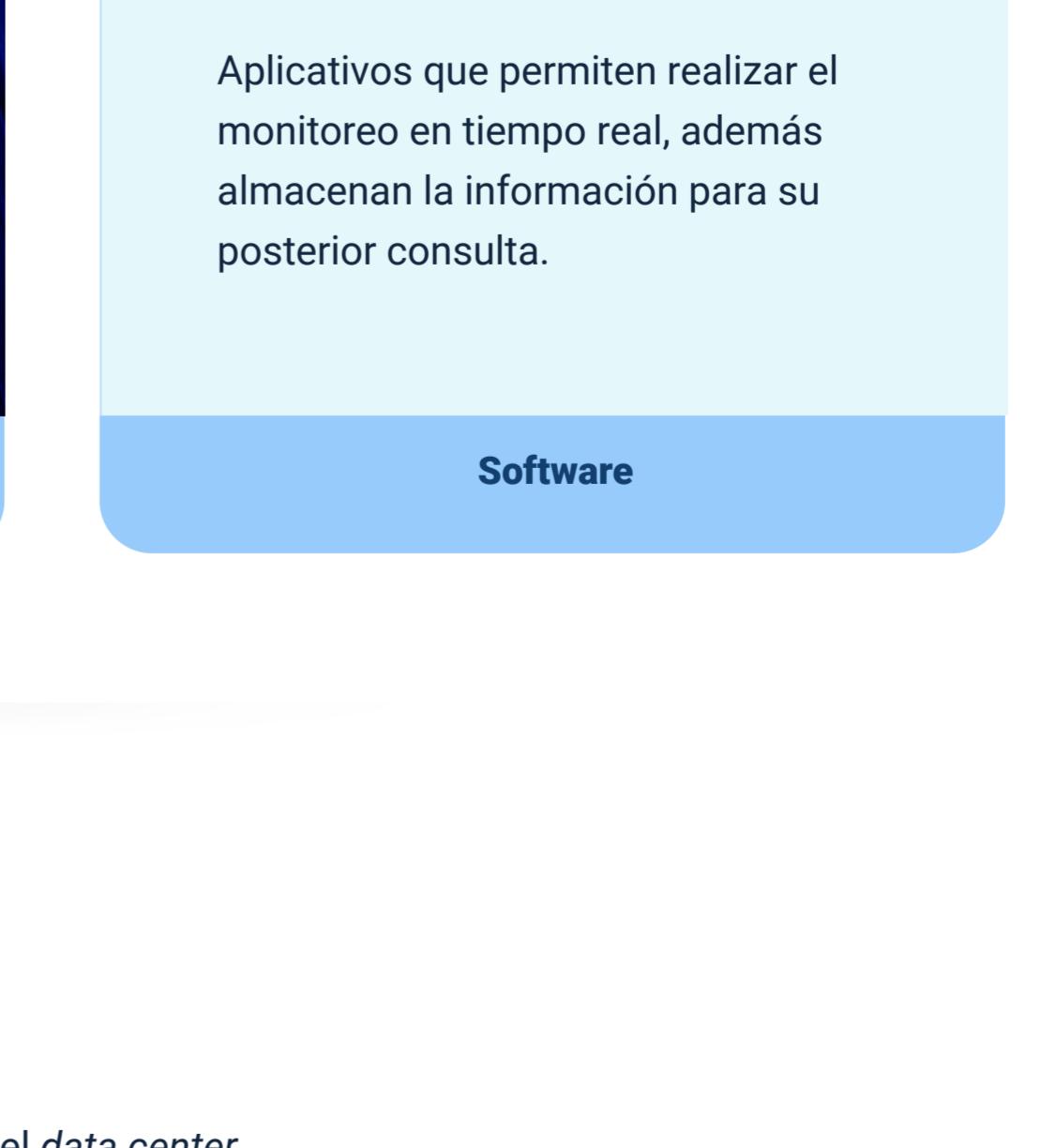
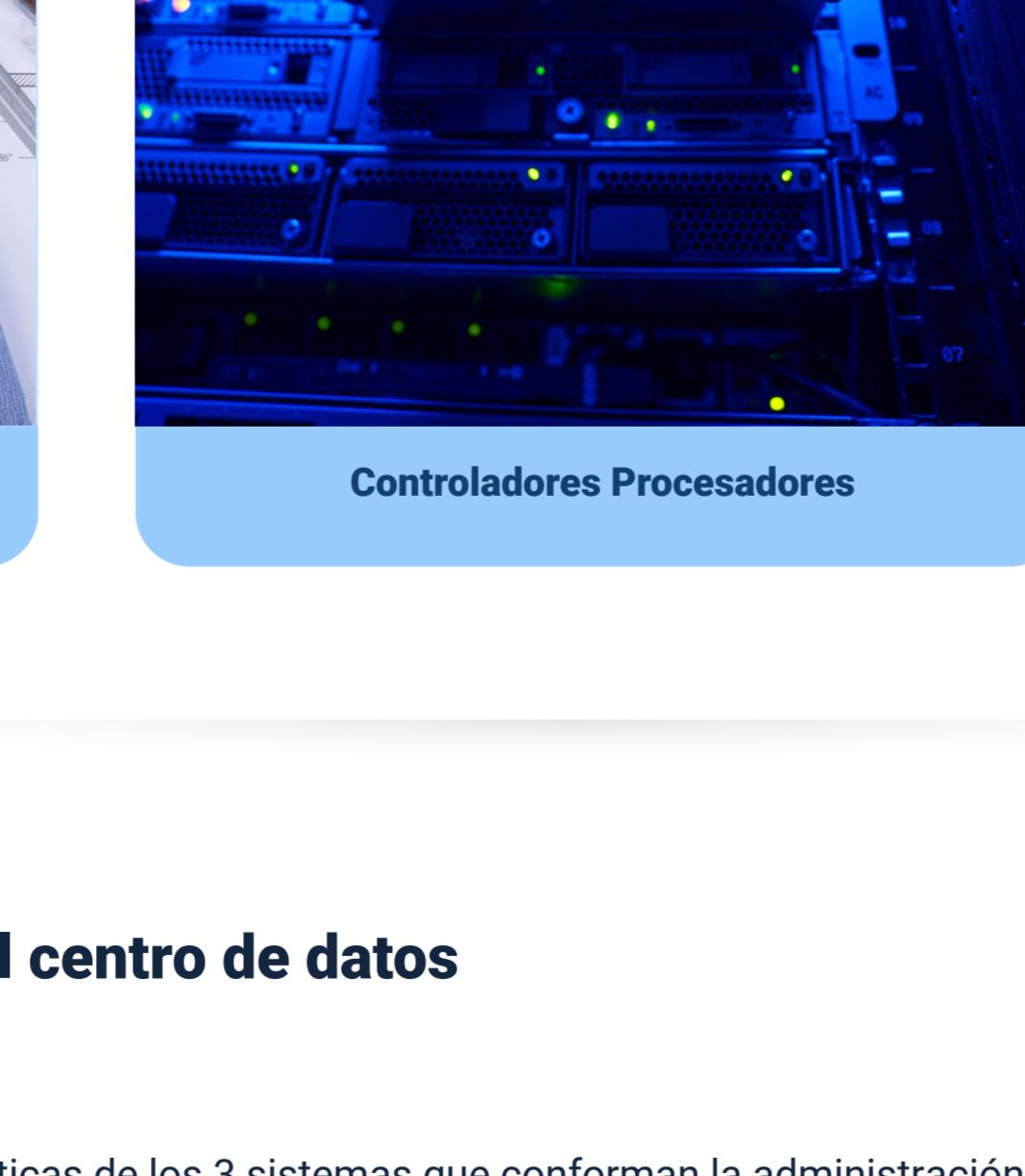
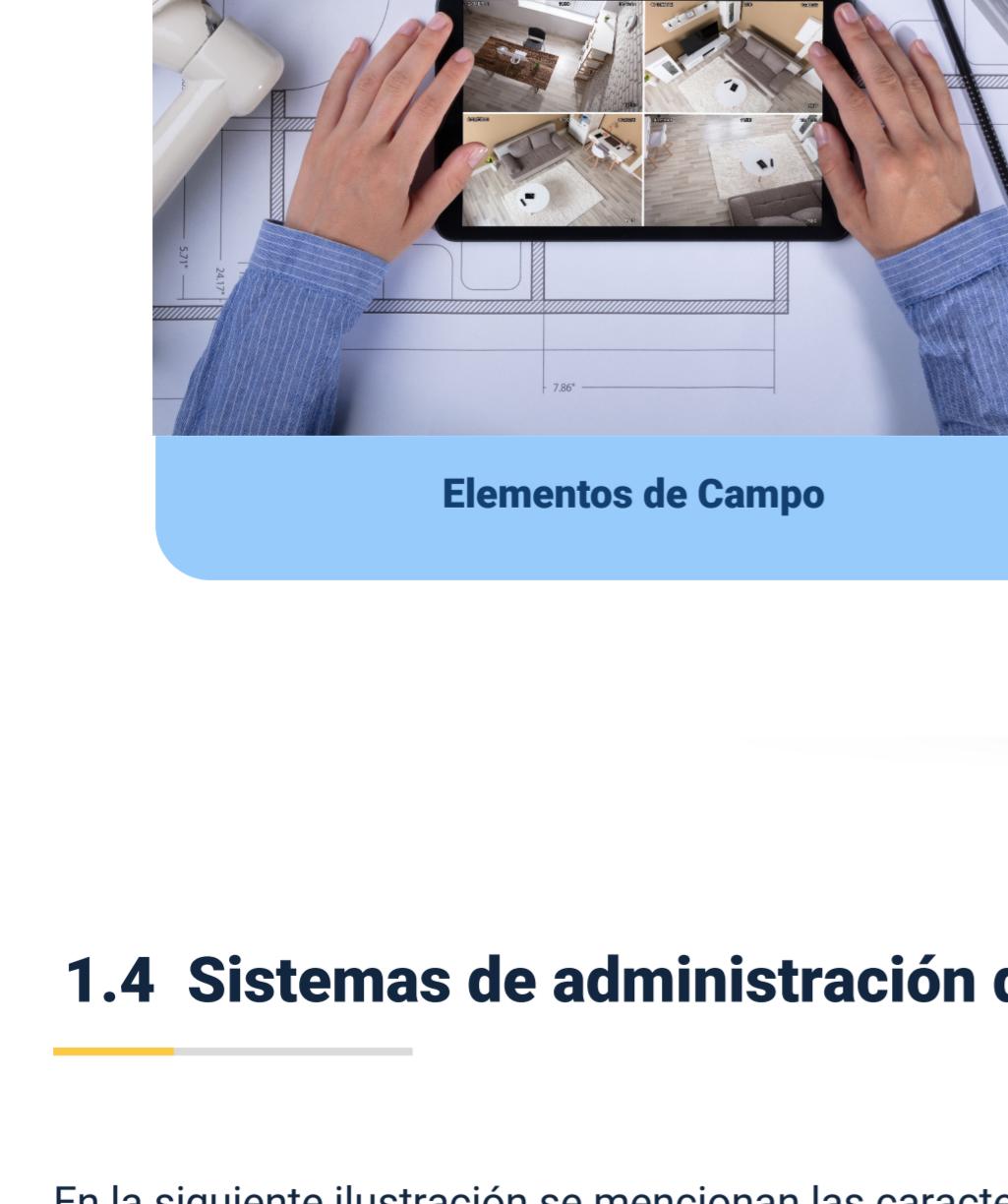
La supervisión y control del centro de datos permite:

- 1. Controlar y administrar el centro de datos.
- 2. Verificar el funcionamiento de la infraestructura en todo momento.
- 3. Reducir los incidentes.
- 4. Reducir la saturación y/o congestión en la red.
- 5. Evitar ataques al sistema informático.
- 6. Garantizar la disponibilidad de la red.



### 1.1 Componentes administrativos del centro de datos

El monitoreo de los centros de datos se puede dividir en tres componentes que permiten su administración y control de la siguiente manera:



### Monitoreo

Para conocer más sobre Monitoreo, principio básico para la disponibilidad de un centro de datos, consulte:

Enlace web. Ago. P. (2016). Monitoreo, principio básico para la disponibilidad de un centro de datos. ComputerWeekly.es, TechTarget.

### 1.2 Técnicas y procedimientos para el monitoreo del centro de datos y gestión de información.

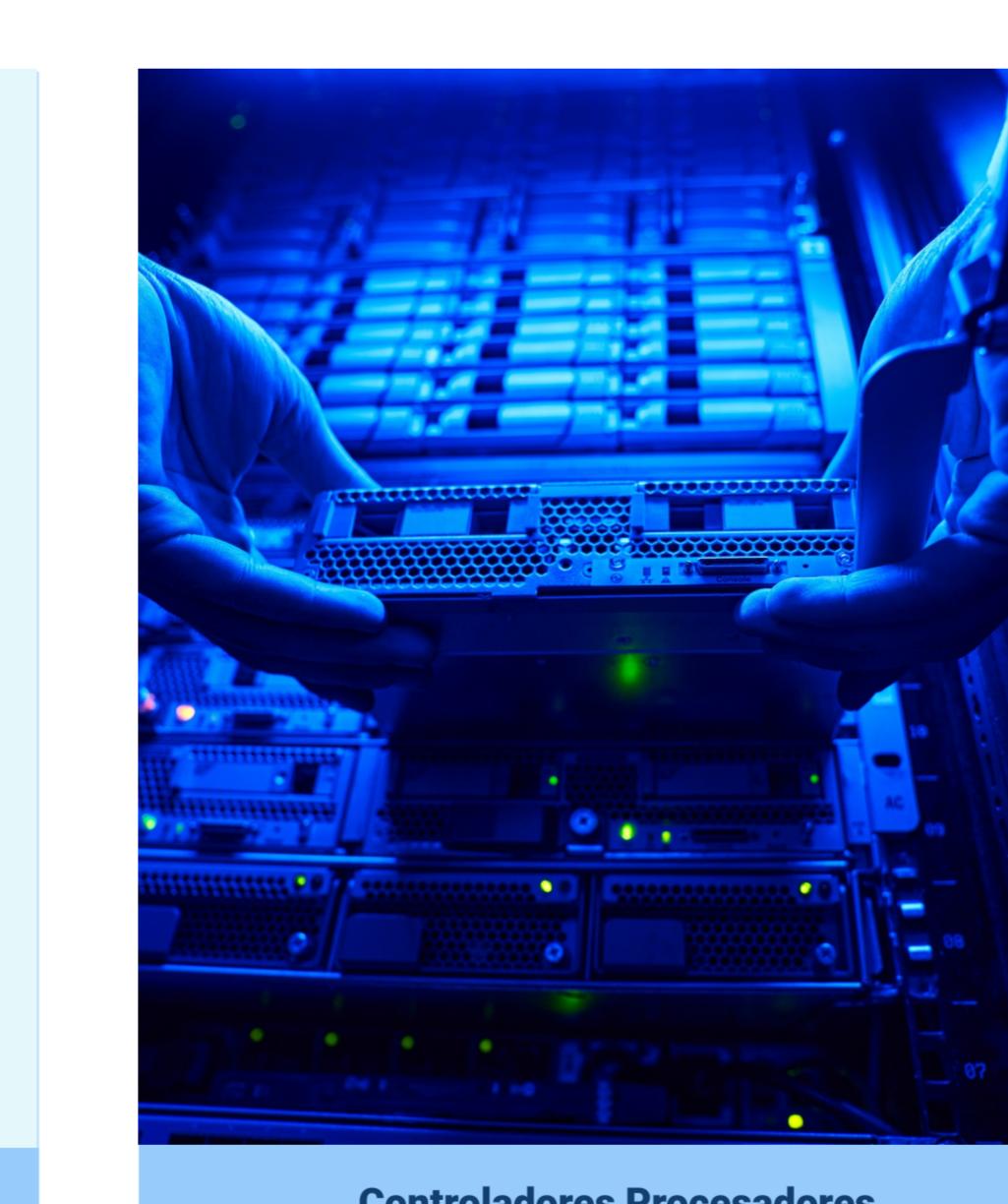
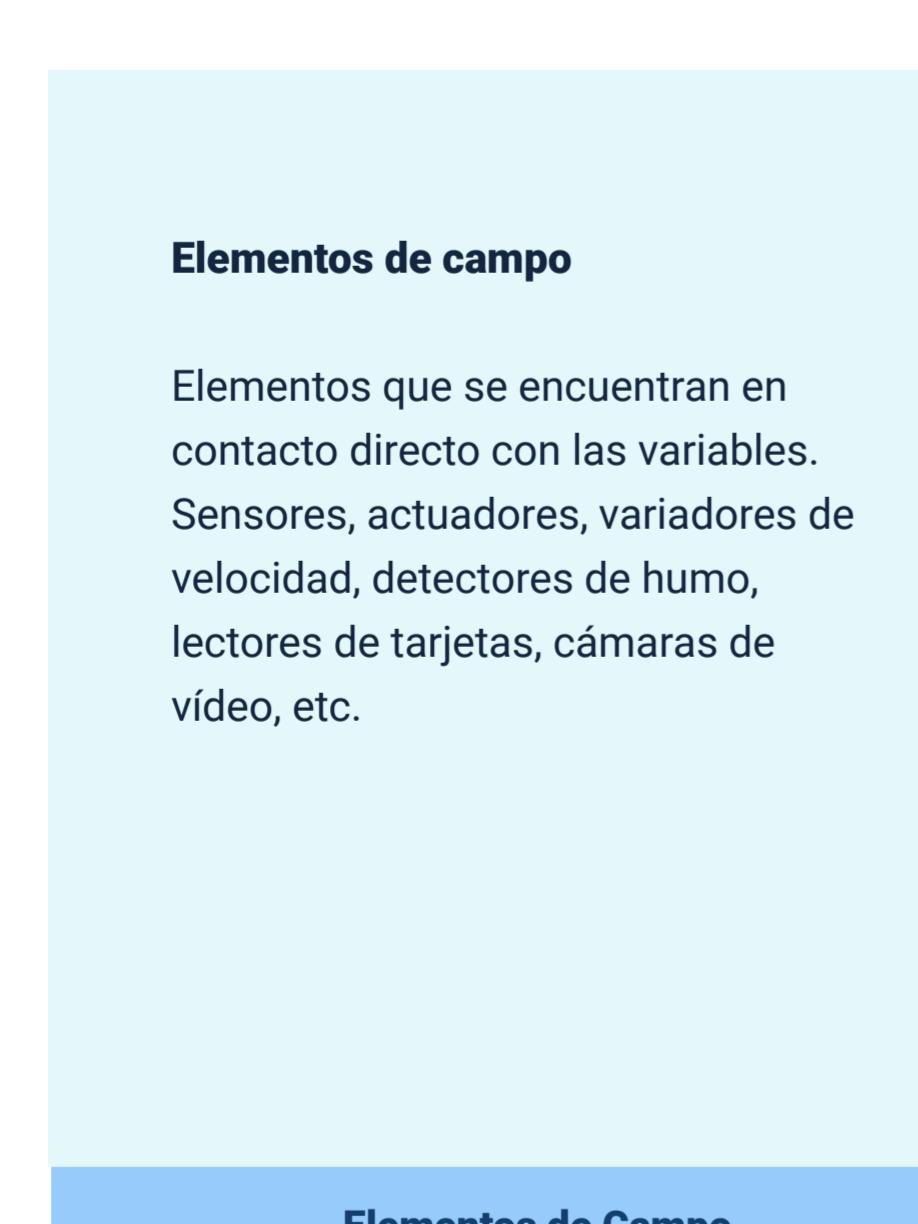
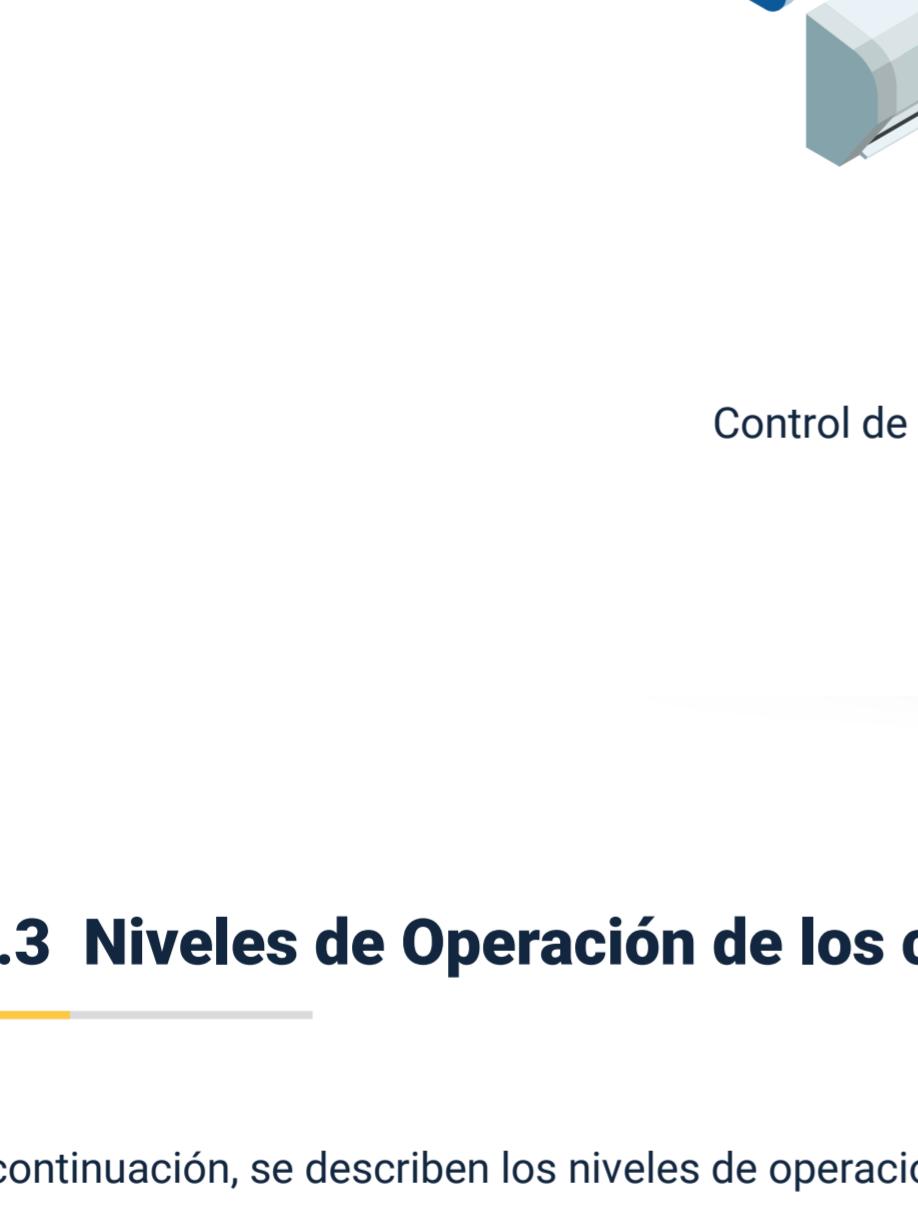
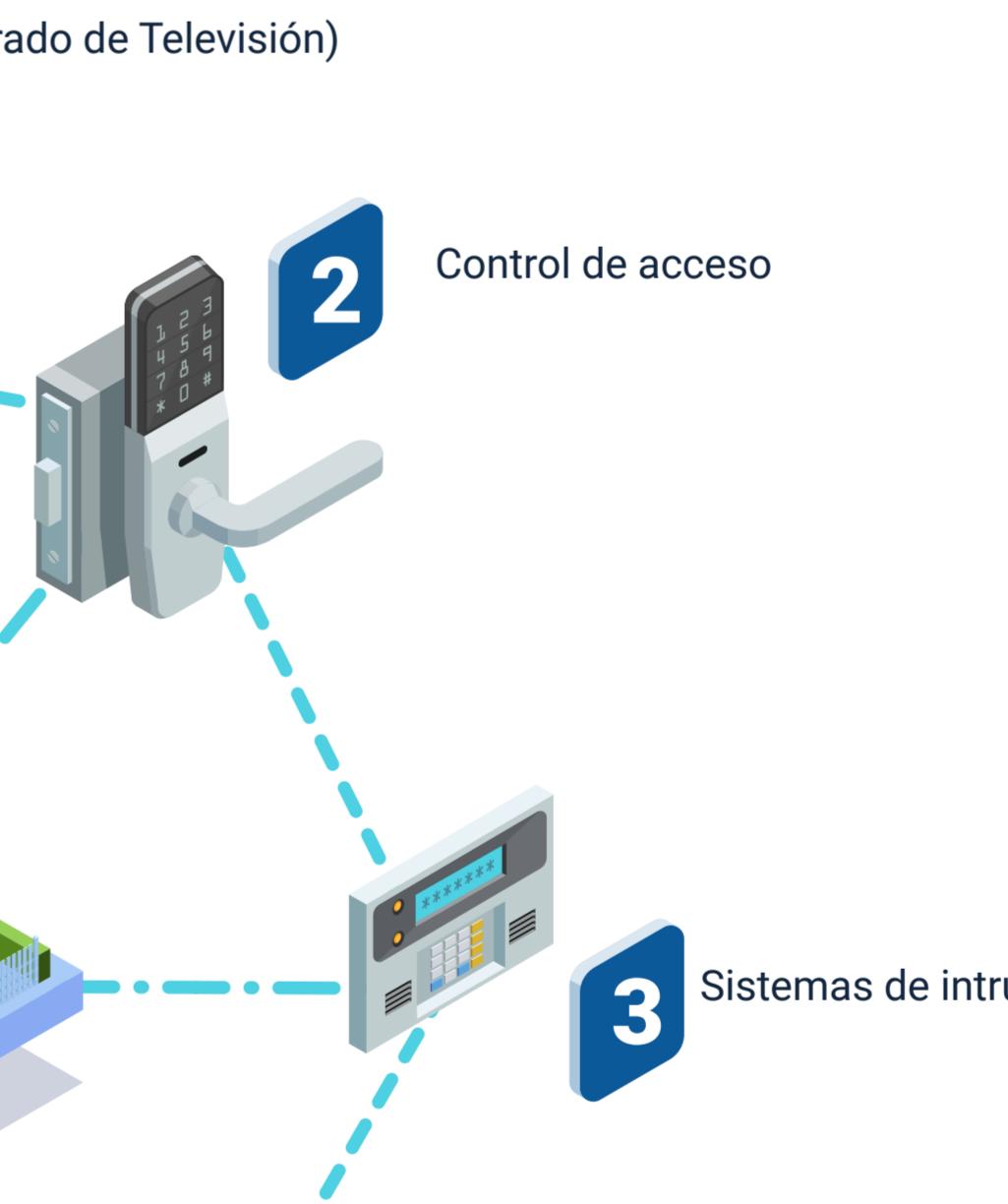
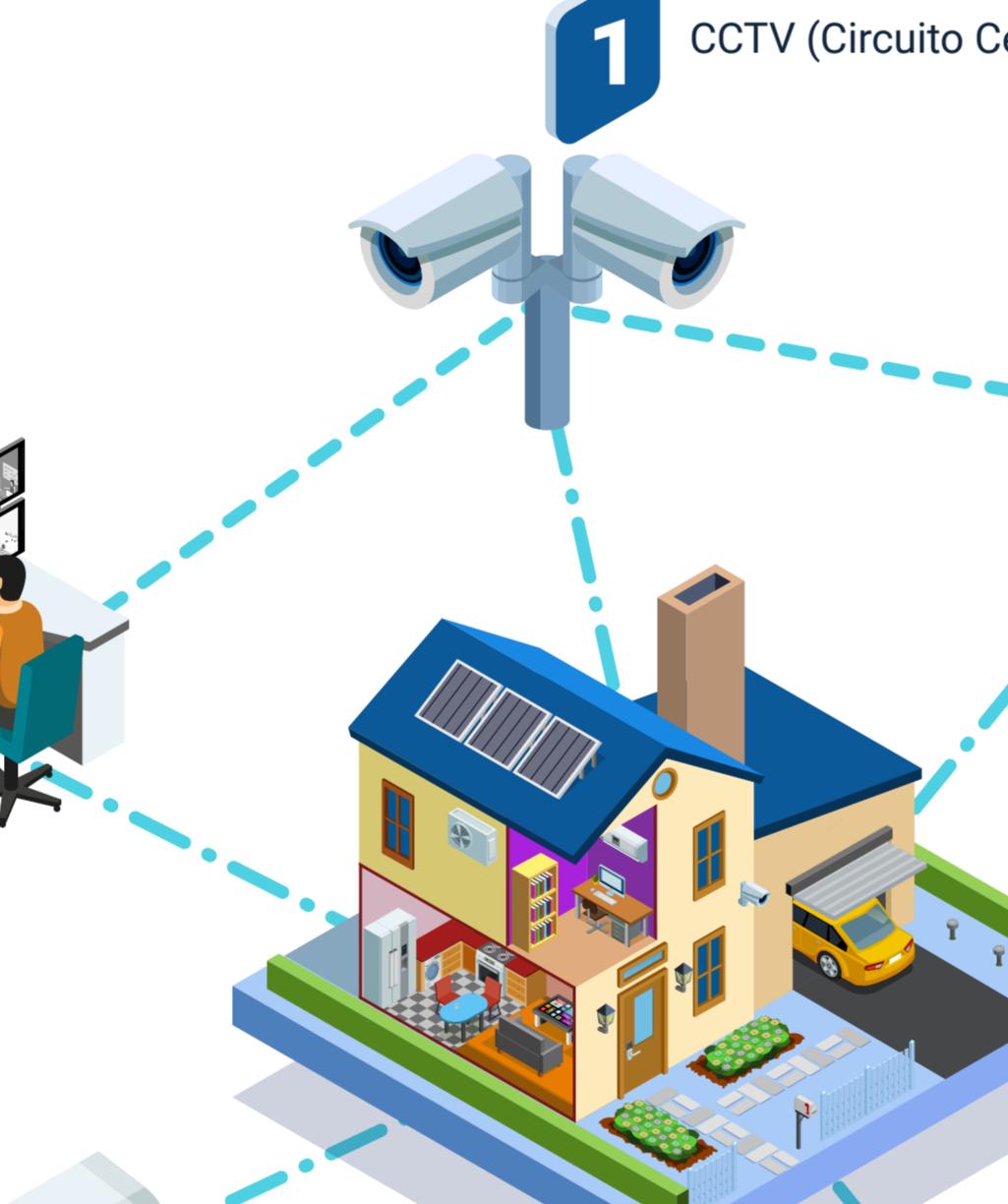


Fuente SIEMENS Publireportaje, 2020.



A continuación, se describen los niveles de operación que componen el monitoreo en el centro de datos para su correcto funcionamiento.

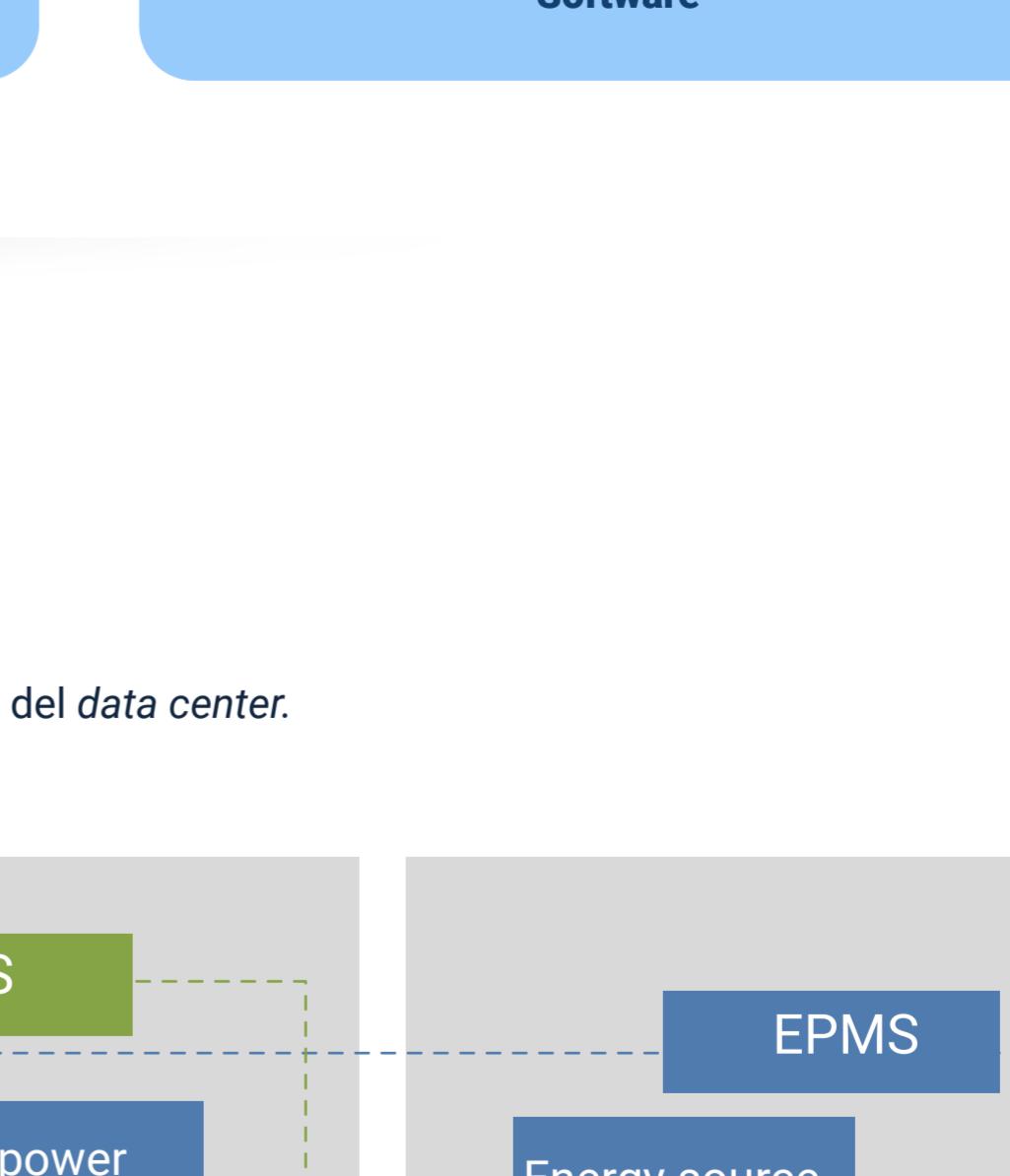
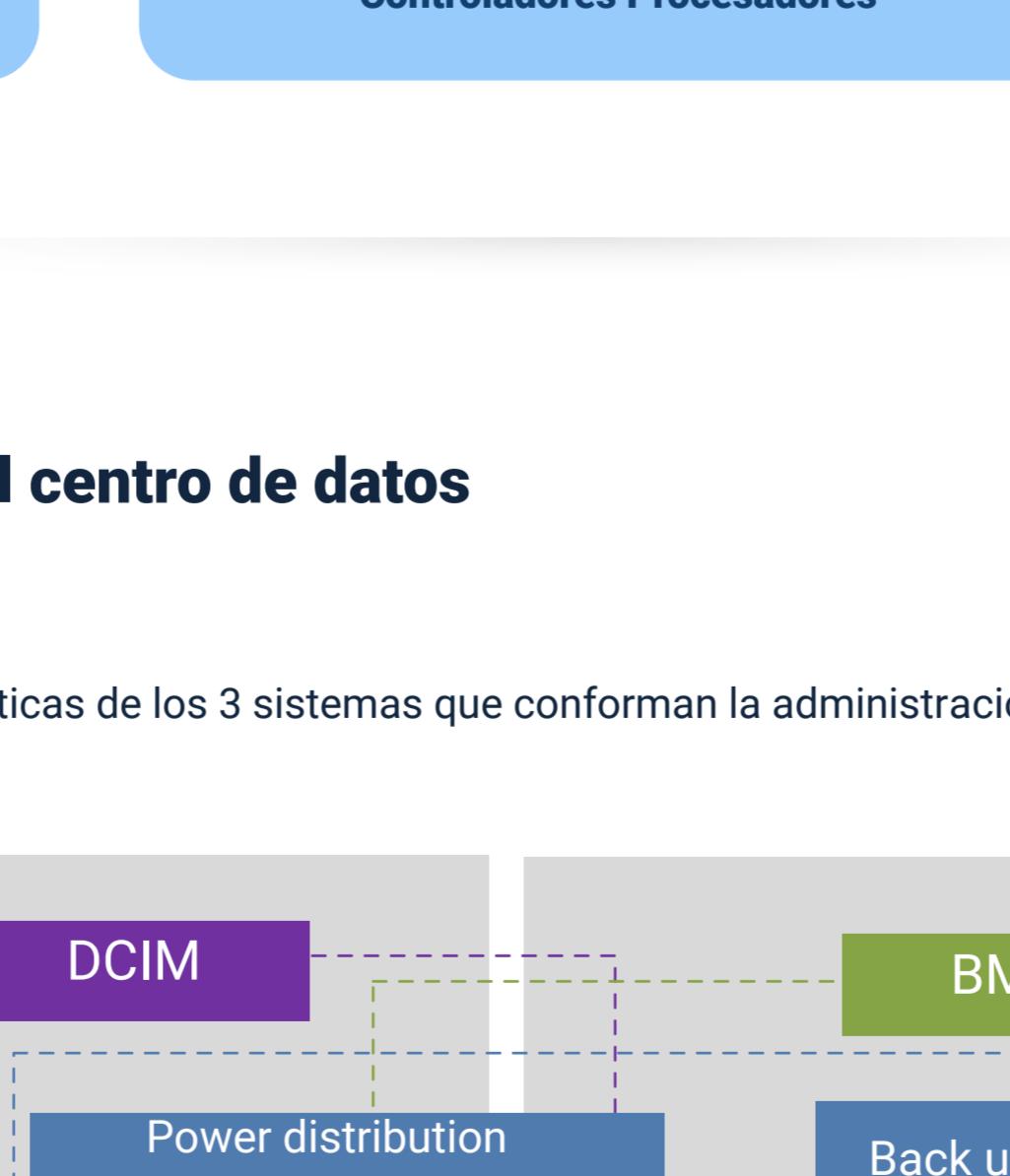
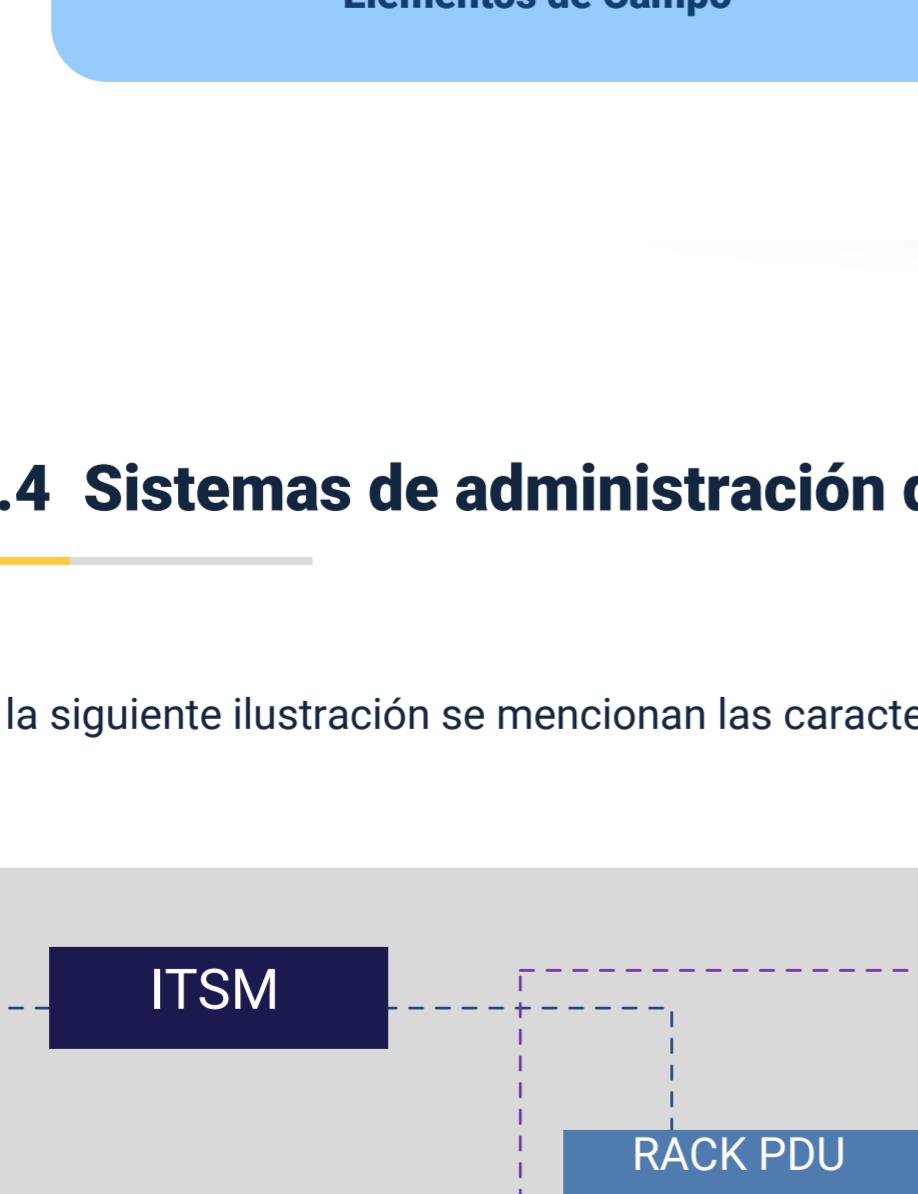
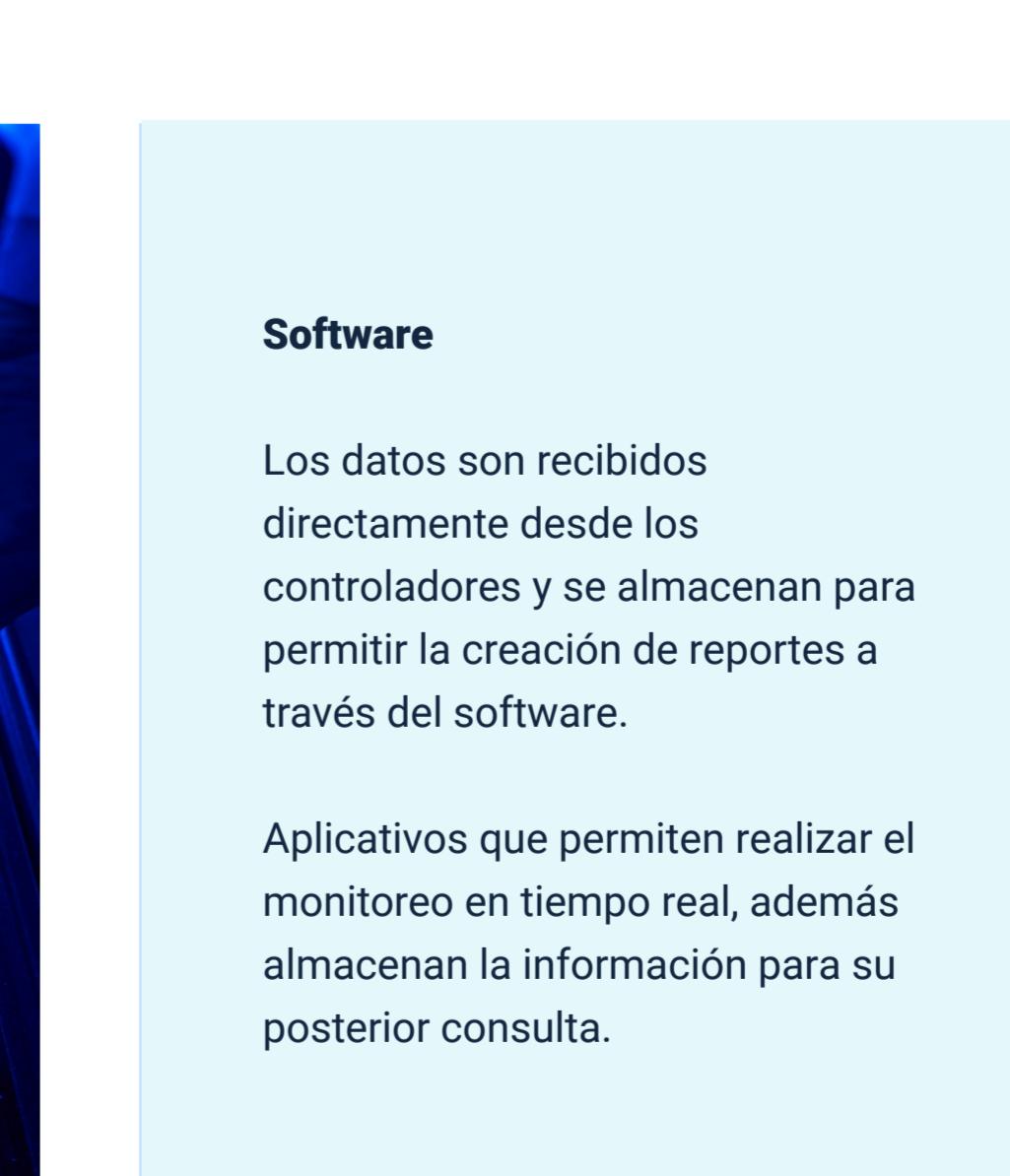
#### Niveles de operación



### 1.3 Niveles de Operación de los componentes de monitoreo

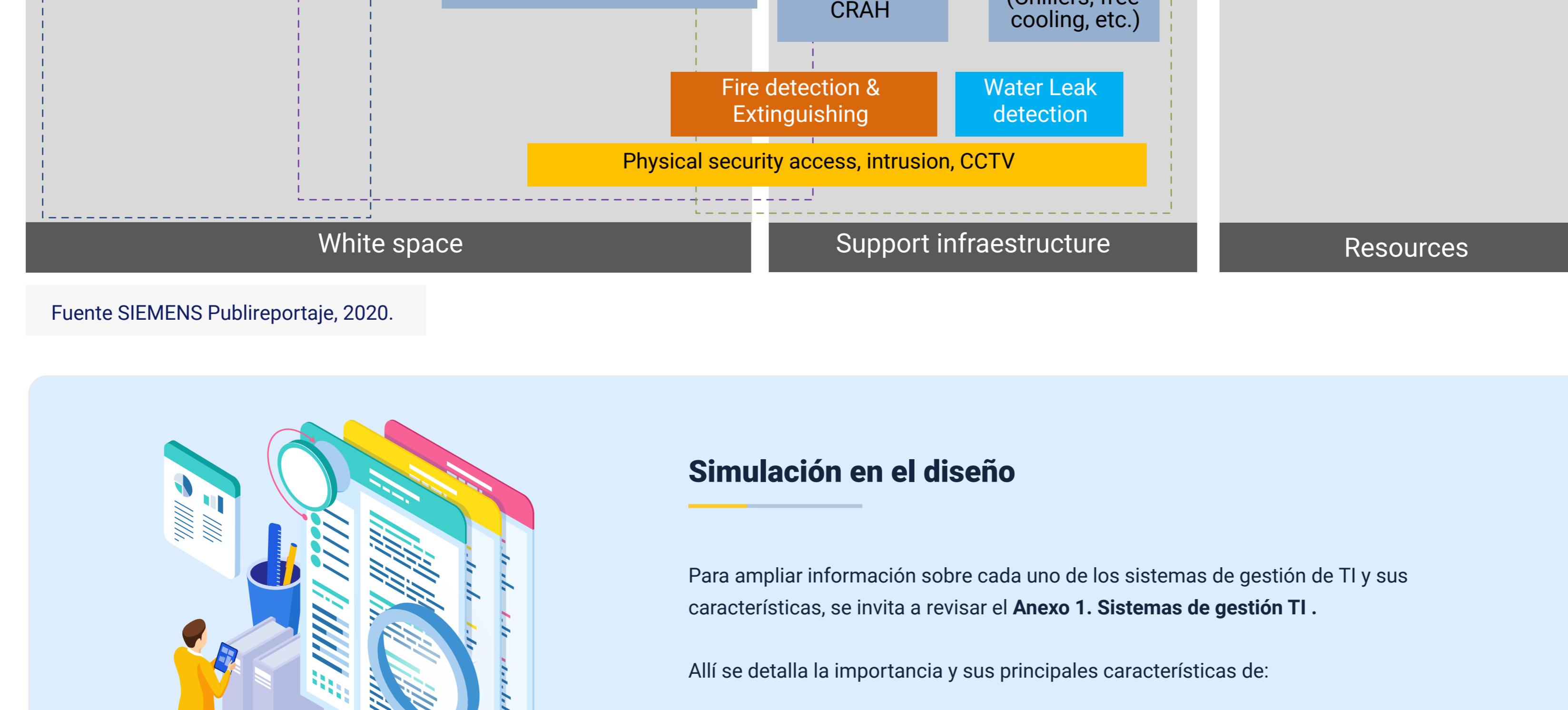
A continuación, se describen los niveles de operación que componen el monitoreo en el centro de datos para su correcto funcionamiento.

#### Niveles de operación



### 1.4 Sistemas de administración del centro de datos

En la siguiente ilustración se mencionan las características de los 3 sistemas que conforman la administración del data center.



Fuente SIEMENS Publireportaje, 2020.



#### Simulación en el diseño

Para ampliar información sobre cada uno de los sistemas de gestión de TI y sus características, se invita a revisar el Anexo 1. Sistemas de gestión TI.

Allí se detalla la importancia y sus principales características de:

✓ ITSM IT Service Management o Administración de Servicios TI.

✓ DCIM Data Center Infrastructure Management o Gestión de la Infraestructura del Centro de Datos.

✓ BMS Building Management System o sistemas de gestión de edificios.

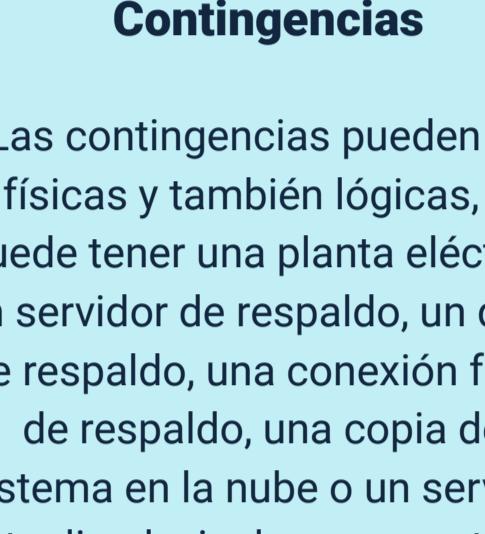
[Descargar](#)

## 2 Plan de contingencia



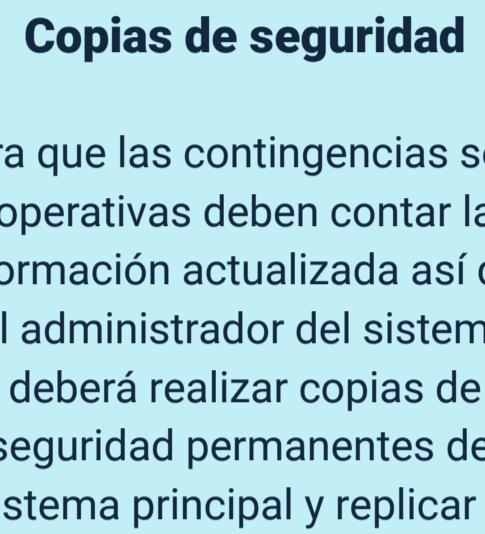
En el funcionamiento y operación del centro de datos se deben tener en cuenta todas las variables que pueden afectar su normal operación; para garantizar una disponibilidad del 100% en su funcionamiento se deberá contar con equipos "contingencia" o de respaldo que permitan suplir un requerimiento puntual en caso de ser necesario.

Al momento de presentarse una falla, el equipo de contingencia entra en funcionamiento y el sistema sigue operando sin novedad alguna para el usuario final.



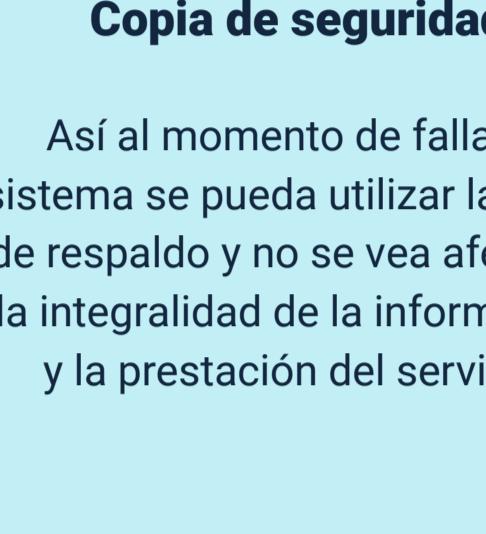
### Contingencias

Las contingencias pueden ser físicas y también lógicas, se puede tener una planta eléctrica, un servidor de respaldo, un disco de respaldo, una conexión física de respaldo, una copia del sistema en la nube o un servidor virtualizado; incluso un centro de datos de respaldo que garantece la operatividad del sistema sin importar la falla que se presente.



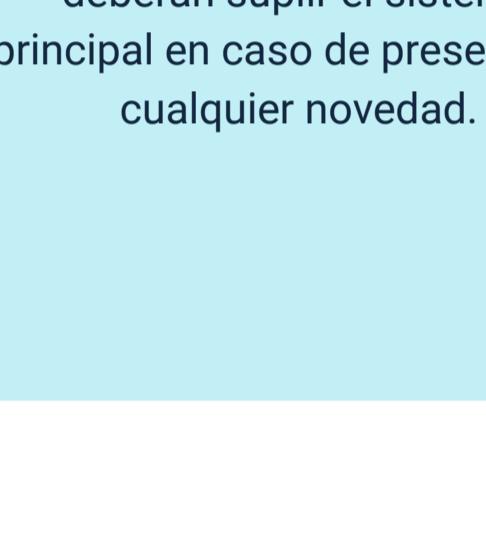
### Copias de seguridad

Para que las contingencias sean operativas deben contar la información actualizada así que el administrador del sistema deberá realizar copias de seguridad permanentes del sistema principal y replicar la información a la contingencia.



### Copia de seguridad

Así al momento de fallar el sistema se pueda utilizar la copia de respaldo y no se vea afectada la integralidad de la información y la prestación del servicio.



### Contingencias

Como se puede observar, las contingencias deberán estar pensadas de acuerdo a la infraestructura TI y como tal deberán suplir el sistema principal en caso de presentarse cualquier novedad.

### Herramientas de simulación

A continuación, se darán ejemplos de algunas herramientas de simulación que permiten tener respaldo del sistema.

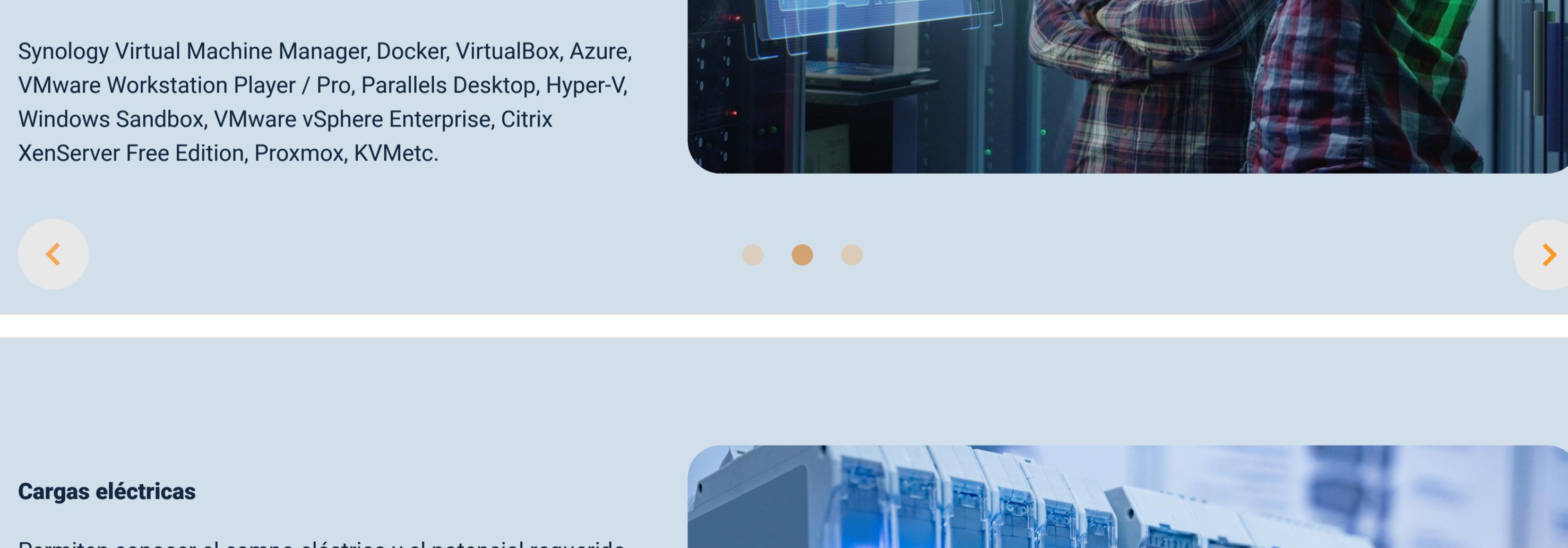
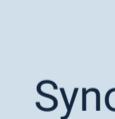
A continuación, se mencionan algunas herramientas de simulación para las redes sociales, virtualización y cargas eléctricas.

#### Redes de datos

Aplicativos que permiten simular redes de datos con el fin de conocer su operación, equipos e infraestructura necesarias para su funcionamiento.

Ejemplos de herramientas de Simulación:

NetSim, Jimsim, KivaNS, Network Simulator, OMNET ++, Packet Tracer, OPNET Modeler, RouterSim Network Simulators, Toggit y WebNMS Simulación Toolkit, CORE, IMUNES, etc.



#### Cargas eléctricas

Permiten conocer el campo eléctrico y el potencial requerido para la implementación de un sistema. Para los ejemplos, aunque algunas herramientas no son simulaciones, sí permiten conocer las variables que hacen parte del sistema eléctrico y garantizan que al momento de diseñar la infraestructura tecnológica se puedan controlar todas las variables.

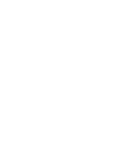
Ejemplos de herramientas de simulación:

PhET, electrical formulator, metal prices, electrical calculations lite, topmatic, two thirty volts, calculadora de costes de energía, electrotecnia (pack), ley de ohm-calc, calculadora de caída de tensión, everycircuit, icircuit, ecomatic, home electrical safety check.



#### Simulación en el diseño

Para conocer sobre la importancia de la simulación en el diseño de un centro de datos consulte:



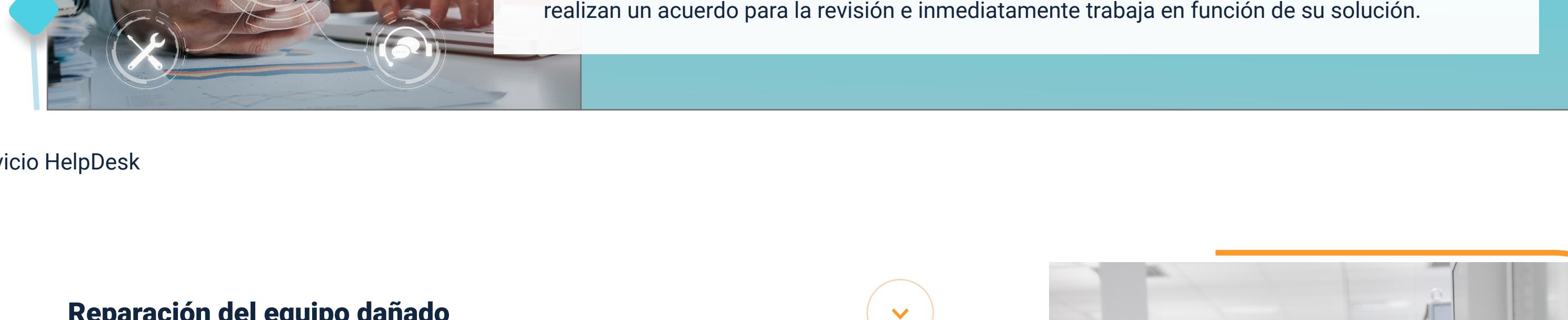
[Enlace web.](#) Khan, N. (2021) ¿Por qué simular un centro de datos? Retrieved August 29, 2022, from

Las herramientas de simulación son un recurso de gran ayuda para la gestión de los proyectos TI, también para evaluar el impacto en los cambios que se requieran realizar en la infraestructura TI, cargas, sobrecargas, comportamiento del sistema ante novedades como virus, caídas en la red, fallas eléctricas entre otros; por lo tanto, permite tener una visión amplia de la infraestructura TI y simular fallas en la misma con el fin de evitarlas.

### 3 Evaluación de causas

El buen uso de un centro de datos no está ligado solamente a su infraestructura física, ni al control de las variables, también está estrechamente ligado al seguimiento, administración y monitoreo que se realice a cada uno de sus componentes con el fin de poder realizar evaluación y seguimiento al desempeño del mismo.

Ejemplo aplicado a un caso TI



Servicio HelpDesk

#### Reparación del equipo dañado



#### Análisis de solución del requerimiento

#### Puntos a mejorar

#### Indicadores

#### Reparación del equipo dañado

El técnico requiere de insumos para reparar el equipo, así que instala la contingencia, solicita al departamento de compras el repuesto y una vez llega, resuelve el incidente en el equipo, acuerda nuevamente con el usuario la instalación del equipo principal, documenta el proceso de solución del ticket y lo finaliza; por último, el usuario hará una calificación del servicio al técnico.

#### Análisis de solución del requerimiento

Del anterior ejemplo se podrían obtener los siguientes indicadores:

- 1 Tiempo en la asignación del servicio.
- 2 Tiempo en contactar al usuario.
- 3 Tiempo en la solución del servicio.
- 4 Costo del ticket (mano de obra, repuestos, etc.).
- 5 Calificación del servicio.
- 6 Cantidad de servicios atendidos por hora, día, mes, año, etc.

#### Puntos a mejorar

Como se puede apreciar, los indicadores permiten llevar control y de su análisis se obtienen datos valiosos para el área TI como lo son:

- ✓ Acciones de mejora.
- ✓ Implementación de buenas prácticas.
- ✓ Acciones correctivas al proceso TI.
- ✓ Acciones correctivas al proceso de prestación de servicio.
- ✓ Solicitar capacitación sobre atención al usuario, tiempos de respuesta, normatividad, ITIL, etc.

#### Indicadores

En cualquier actividad se puede implementar un indicador, realizar seguimiento y aplicar las retroalimentaciones necesarias según los requerimientos garantiza que se corrijan las novedades, ofrecer un mejor servicio y mantener la infraestructura TI en condiciones óptimas de funcionamiento.

Las recomendaciones de ASHRAE permiten tener indicadores de seguimiento y control para los data center, por citar un ejemplo el desempeño del enfriamiento está regulado por la métrica PUE (Power Usage Effectiveness) que mide la eficiencia energética de la infraestructura del data center.

Indicadores de seguimiento y control



#### Ambiente físico data center

#### Estándares internacionales

#### Indicadores

#### Estadísticas data center

#### Ambiente físico data center

Como explica Alfonso. G. (2016) en su blog, este indicador tiene tres unidades como ejes centrales de operación:

- 1 Razón PUE: define la banda de operación como representación del índice de eficiencia energética
- 2 Conformidad Térmica TI: toma la operación de los equipos TI a temperaturas y condiciones normales de funcionamiento.
- 3 Resiliencia Térmica TI: operación de equipos TI ante una eventualidad o mantenimiento del sistema de aire acondicionado.

#### Estándares internacionales

Adoptar los estándares internacionales garantizan la ejecución de políticas empresariales enfocadas en buenas prácticas, también se pueden crear indicadores de acuerdo a las necesidades organizacionales mucho más sencillos y que permiten realizar seguimiento al centro de datos y al personal TI encargado de su administración.

#### Indicadores

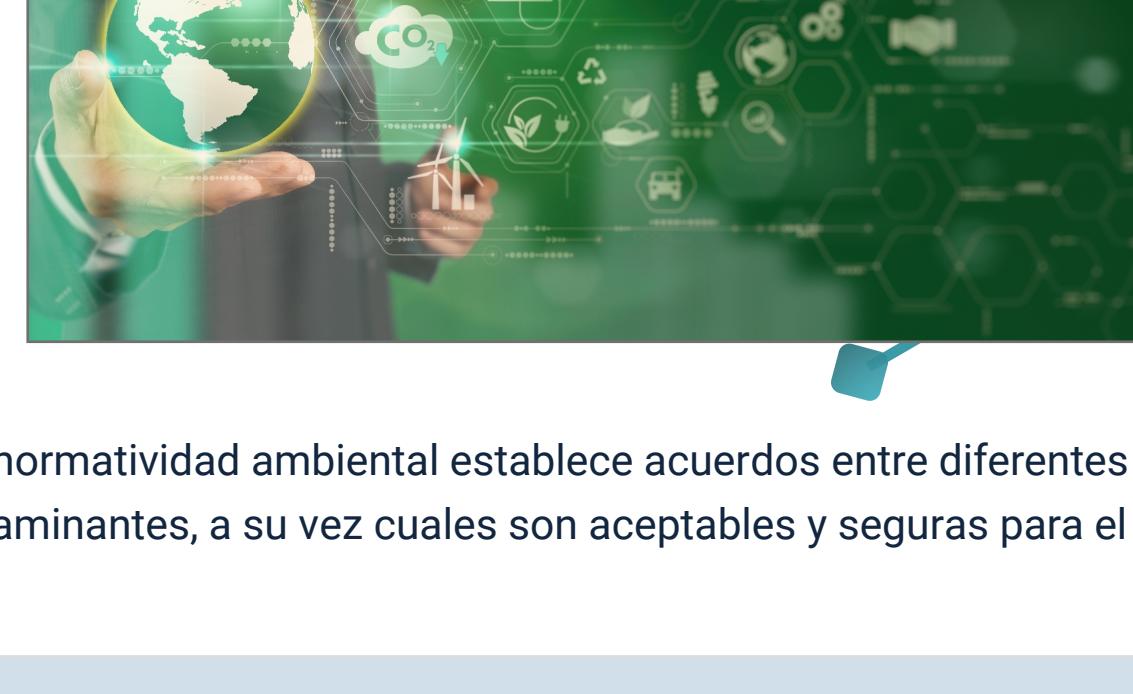
Como explica Alfonso. G. (2016) en su blog, este indicador tiene tres unidades como ejes centrales de operación:

- ✓ Tiempo de disponibilidad.
- ✓ Consumo energético.
- ✓ Cantidad de caídas al año.
- ✓ Tiempo de respuesta a las eventualidades.
- ✓ Costos de operación.
- ✓ Cantidad de alertas.
- ✓ Cantidad de correctivos aplicados en un período de tiempo determinado.
- ✓ Equipo TI encargado de realizar las actividades y la cantidad de actividades resueltas en un período de tiempo establecido.
- ✓ etc.

#### Estadísticas data center

Así, se podrán llevar datos estadísticos sobre el centro de datos y su funcionamiento, entender su dinámica y evitar fallas; también personalizar los indicadores de gestión del centro de datos de acuerdo a las dinámicas organizacionales propias de cada institución.

## 4 Uso de recursos medioambientales

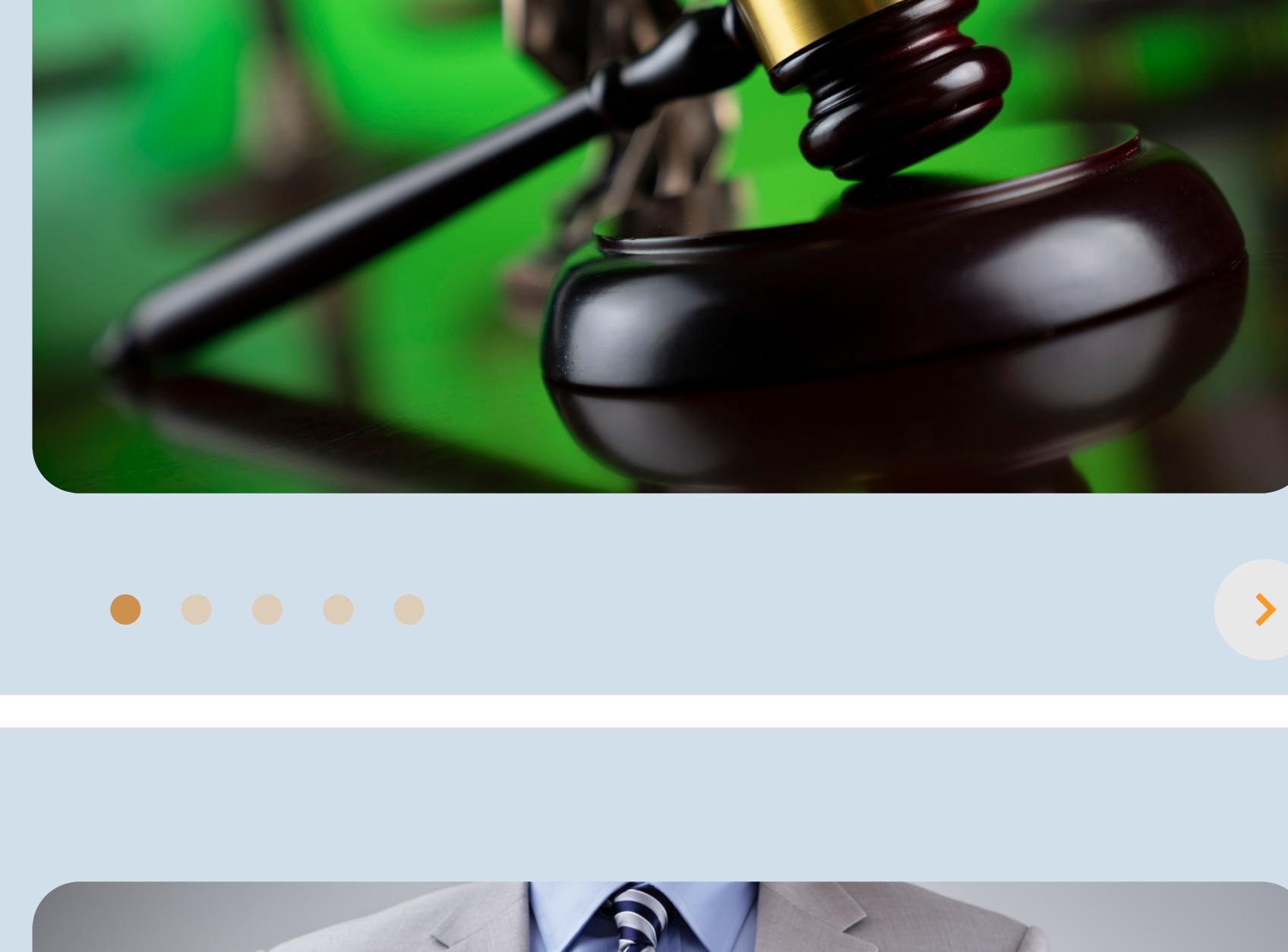


El uso indiscriminado de los recursos naturales por parte del hombre ha generado impactos negativos en el medio ambiente, las malas prácticas han contaminado ríos y recursos naturales valiosos; con el pasar de los años esas malas prácticas han llegado a un nivel que requieren intervención por entidades de control con el fin de regularlas.

Una normatividad ambiental establece acuerdos entre diferentes sectores sociales generando disposiciones legales que regulan los niveles y uso de las sustancias contaminantes, a su vez cuales son aceptables y seguras para el ser humano y el medio ambiente.

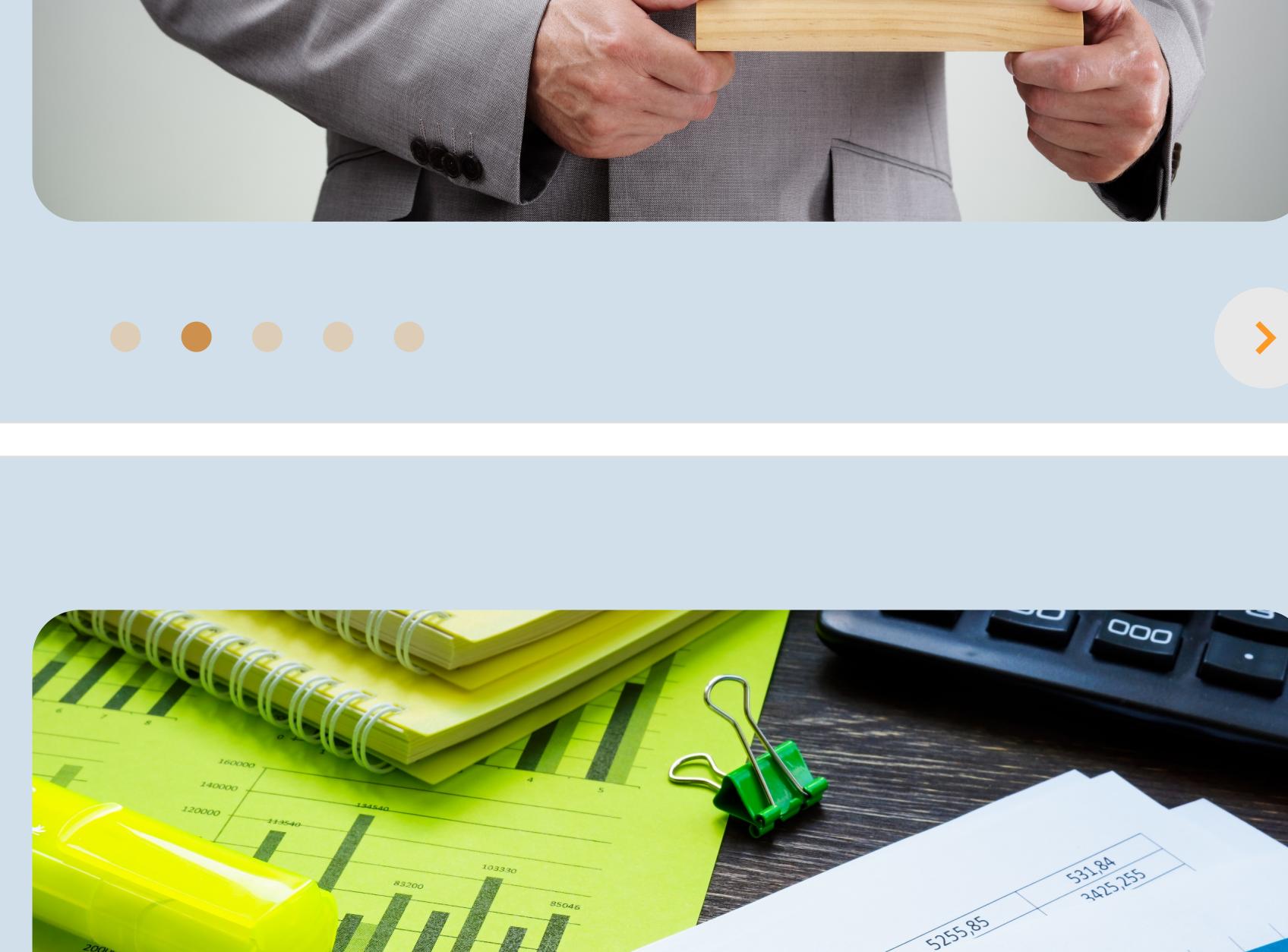
### Para Colombia la legislación ambiental vigente es:

- ✓ Ley de reserva forestal y protección de suelos y agua.
- ✓ Ley para crear el Certificado de Incentivo Forestal CIF.
- ✓ Ley para la protección de la flora colombiana.
- ✓ Ley que consagra el derecho de todas las personas residentes en el país para gozar de un ambiente sano.
- ✓ Régimen de aprovechamiento forestal y acuerdos regionales con este fin.



### Normatividad ambiental

Por tanto, la normatividad ambiental regula las buenas prácticas que permiten garantizar la conservación del medio ambiente y la protección del ser humano.



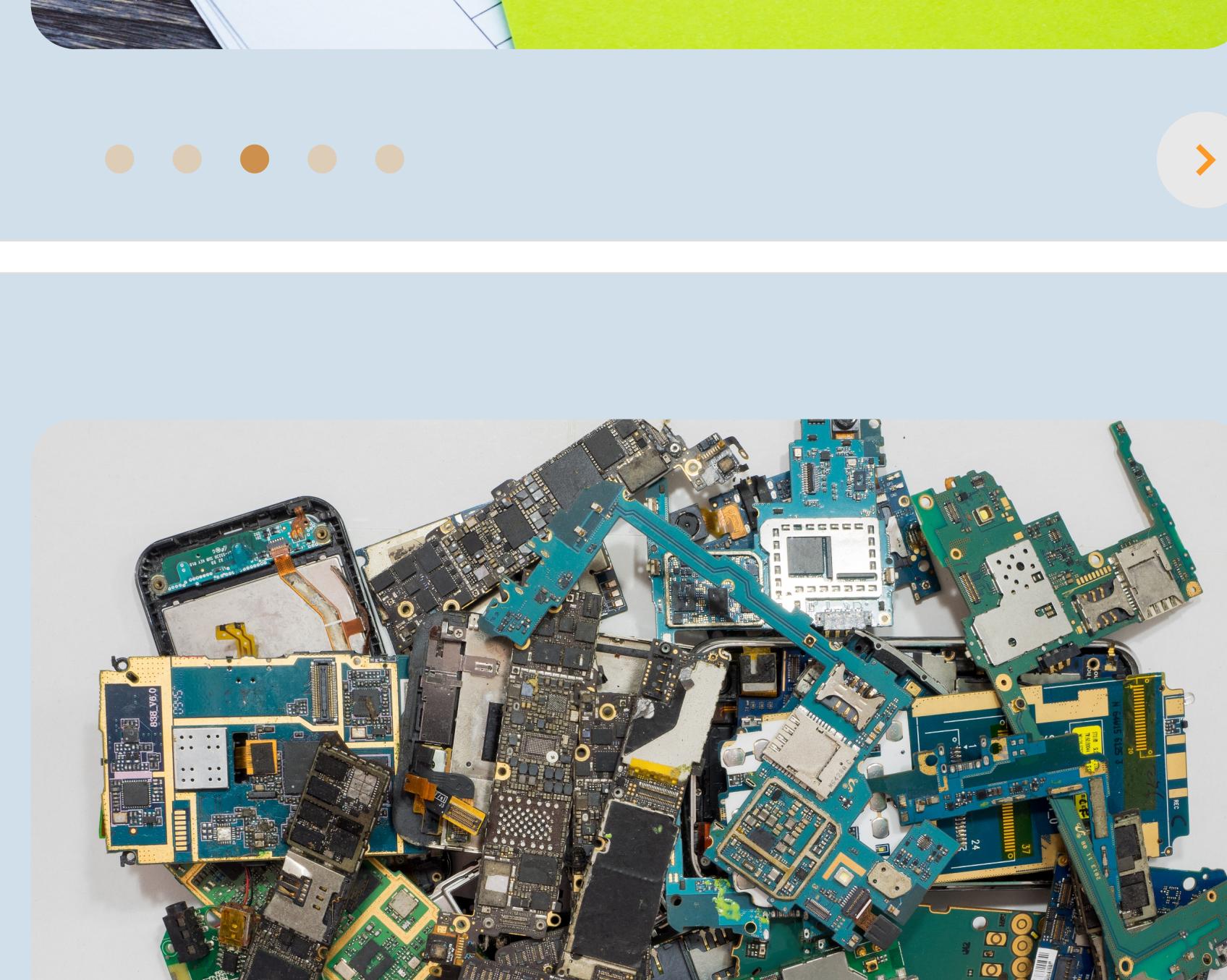
### Normatividad

Para la disposición de los componentes electrónicos en Colombia se cuentan con las siguientes normativas:

Normativa para la disposición de componentes electrónicos en Colombia.

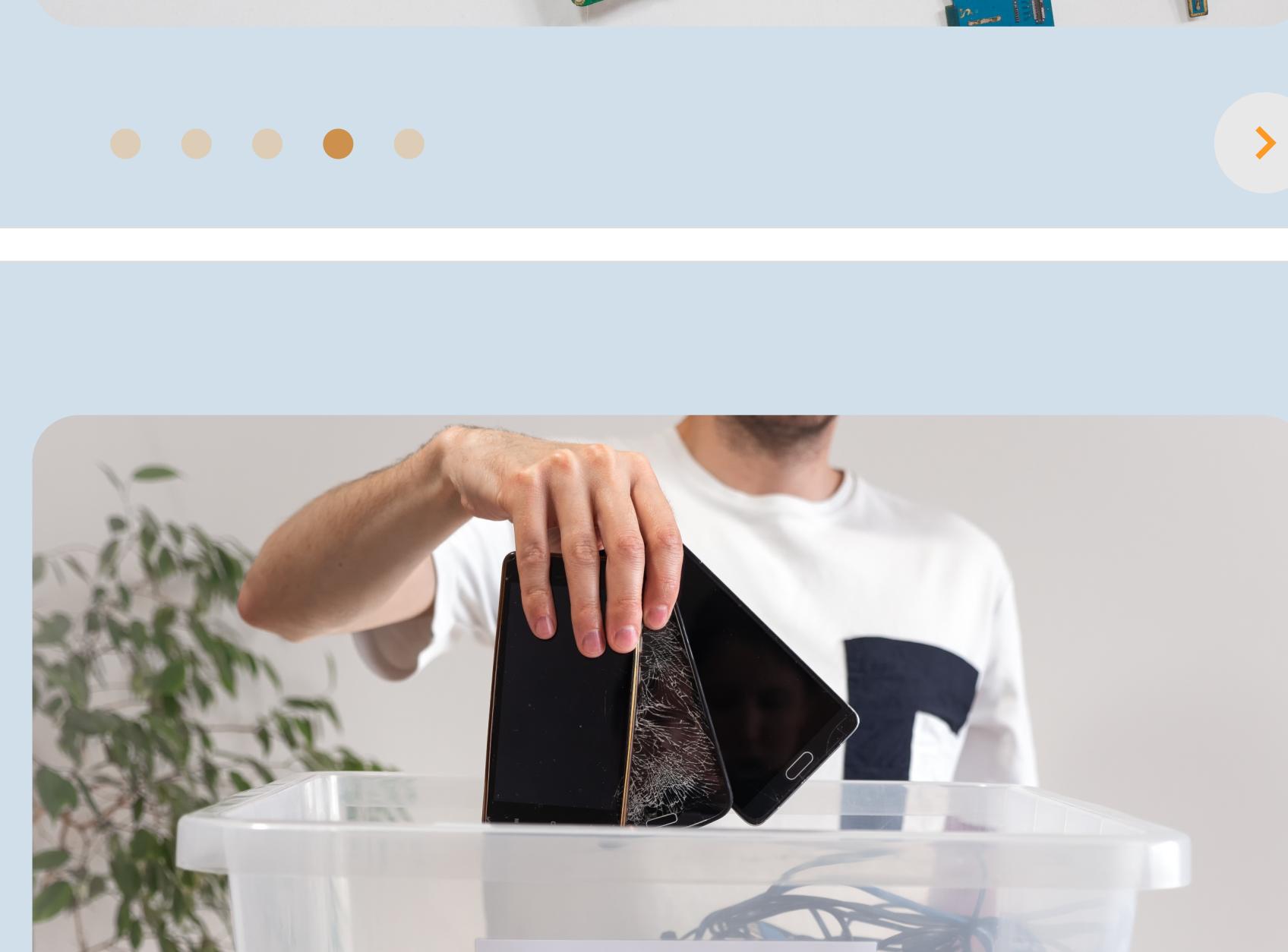
Decreto 284 de 2018: reglamenta la gestión integral que se debe dar a los residuos y aparatos eléctricos y electrónicos más conocidos como RAEE, para prevenir y minimizar los impactos adversos al ambiente.

Ley 1672 de 2013: expide los lineamientos para adoptar la política de gestión integral de residuos y aparatos eléctricos y electrónicos RAEE en Colombia.



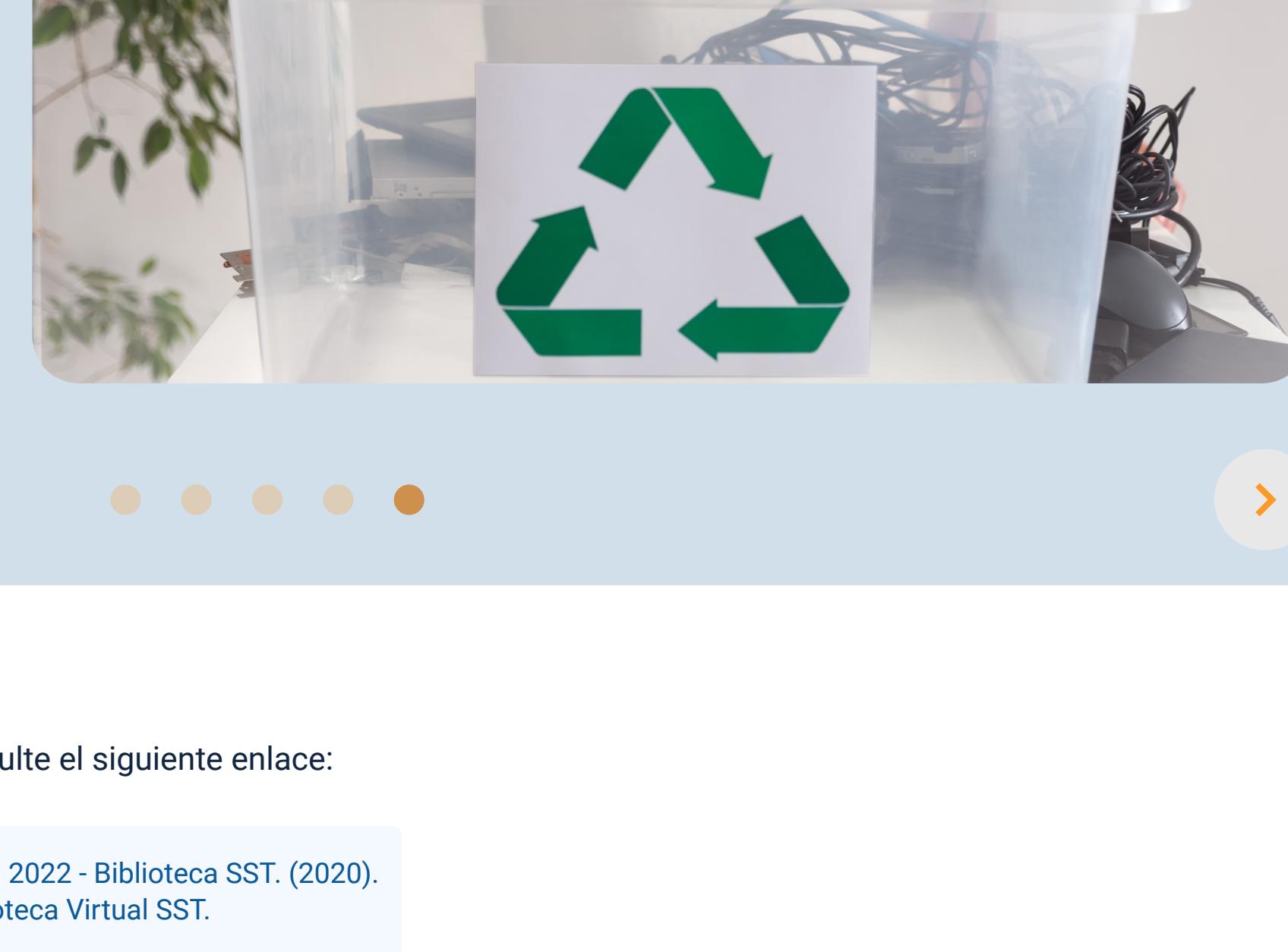
### Residuos electrónicos

Tanto el decreto 248 como la ley 1672, regulan el manejo de residuos electrónicos y su clasificación según su disposición en elementos aprovechables y no aprovechables, es decir, para la disposición final de los residuos eléctricos y electrónicos, estos se deben clasificar y disponer en lugares especialmente seleccionados y diseñados para evitar la contaminación, daños y riesgos a la salud humana y al medio ambiente, la ley 1672 también advierte: "En todo caso, quedará prohibida la disposición de Residuos de Aparatos Eléctricos y Electrónicos RAEE en rellenos sanitarios".



### Manejo de residuos

Es importante reconocer que no solo las empresas tienen obligación con la disposición de los RAEE, "los usuarios y consumidores también deberán entregar dichos elementos en sitios dispuestos para tal fin, además de asumir la corresponsabilidad social con la gestión integral de RAEE, reconocer y respetar el derecho de todos los ciudadanos a un medio ambiente saludable" (Ley 1672 de 2013). Por ello en lugares públicos como centros comerciales se han creado espacios para la correcta disposición final de los residuos tecnológicos, lámparas, baterías, celulares, portátiles, entre otros.

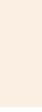


### Normatividad ambiental en Colombia

Para conocer la evolución de la normatividad ambiental en Colombia consulte el siguiente enlace:



[Enlace web. Normatividad Ambiental Vigente en Colombia 2022 - Biblioteca SST. \(2020\).](#)



Las herramientas de simulación son un recurso de gran ayuda para la gestión de los proyectos TI, también para evaluar el impacto en los cambios que se requieran realizar en la infraestructura TI, cargas, sobrecargas, comportamiento del sistema ante novedades como virus, caídas en la red, fallas eléctricas entre otros; por lo tanto, permite tener una visión amplia de la infraestructura TI y simular fallas en la misma con el fin de evitarlas.

## 5 Manejo de posturas

La Seguridad y Salud en el Trabajo o SST garantizan el monitoreo y control de las variables que puedan afectar al individuo dentro de las instalaciones de la organización; por tanto, llevar control de los riesgos y evitar los accidentes se vuelven en los motores primarios de este sistema organizacional.



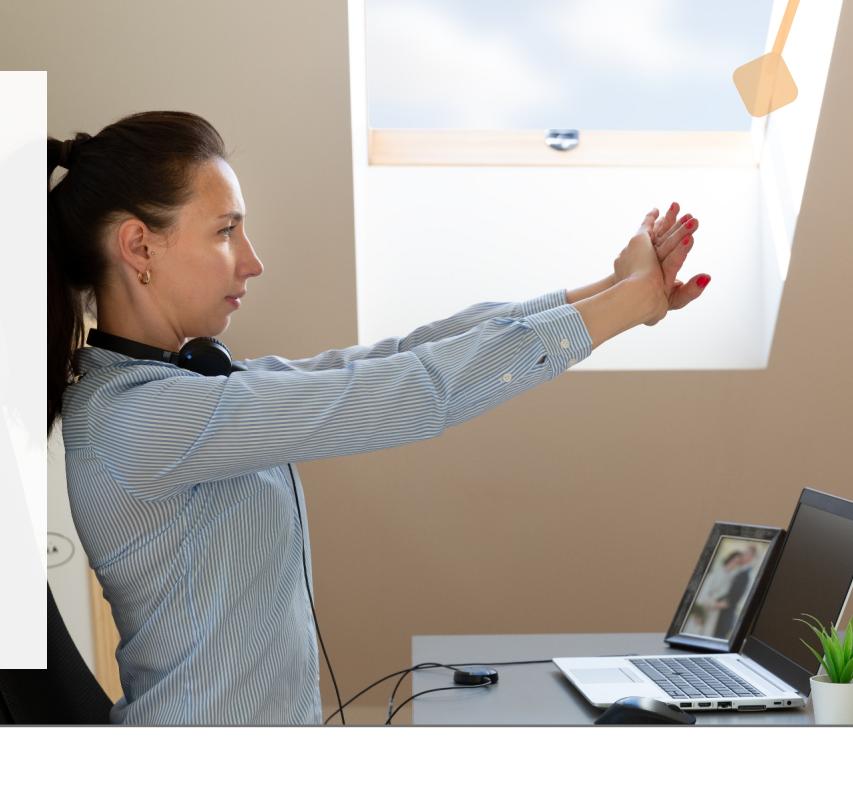
**Normatividad ambiental en Colombia**

Para conocer la evolución de la normatividad ambiental en Colombia consulte el siguiente enlace:

Normatividad Ambiental Vigente en Colombia 2022 - Biblioteca SST. (2020). Biblioteca Virtual de Seguridad y Salud en el Trabajo; Biblioteca Virtual SST.

[Enlace web](#) 

Hablando específicamente de la Seguridad y Salud en el Trabajo enfocado en TI, podría decirse que el nivel de riesgo no sea alto o peor aún, que no existan riesgos que deban ser mitigados debido a la naturaleza misma de la actividad que se realiza, monitoreo de cámaras o del centro de datos, analizar la red, desarrollar aplicativos, utilizar el sistema de información para hacer consultas, entre otros; son algunas de las actividades del día a día, completamente diferentes a los que por ejemplo en la construcción se encuentran de manera mucho más evidentes y hacen que se consideren actividades de riesgo; sin embargo; algunas de los riesgos más relevantes dentro de TI son:



Seguridad y Salud en el Trabajo



- Fatiga visual o muscular 
- Golpes o caídas 
- Contacto eléctrico 
- Carga mental 

**Fatiga visual o muscular:**

La realización de actividades en donde se deba adoptar la misma postura y fijar la vista sobre una pantalla por tiempo prolongado generan cansancio y fatiga, se deben realizar pausas activas que activen al individuo. Si se cuenta con una ventana se pueden hacer pausas y mirar objetos a diferentes distancias, así el ojo podrá ejercitarse, también si con frecuencia se levanta de su silla y realiza movimientos que activen el cuerpo, podrá garantizar que el cansancio y la fatiga no lleguen. Adicionalmente, implementar buenas posturas, garantizar el cumplimiento ergonómico en el puesto de trabajo pueden ser buenas prácticas que reducen daños físicos en el cuerpo humano, así la cabeza levantada, columna erguida, pies apoyados, rodillas en ángulo recto y brazos apoyados, son algunas de las prácticas que se deben aplicar a la hora de desarrollar las labores en oficinas.



**Golpes o caídas:**

En el centro de datos existen elementos en el suelo, piso y espacio en general que pueden ocasionar golpes o generar caídas, se deben identificar estos factores de riesgo, marcarlos y en caso de ser posible eliminarlos, así los riesgos se reducen. También es importante resaltar que por ejemplo al caerse por un cable en el suelo, no solamente existe el riesgo del daño físico al individuo, también se pone en riesgo el sistema y su operación. ITIL, COBIT, RETIE, entre otros, dan parámetros, normas y estándares nacionales e internacionales para el manejo de cableado y garantizar su correcta ubicación según el cuarto de datos.



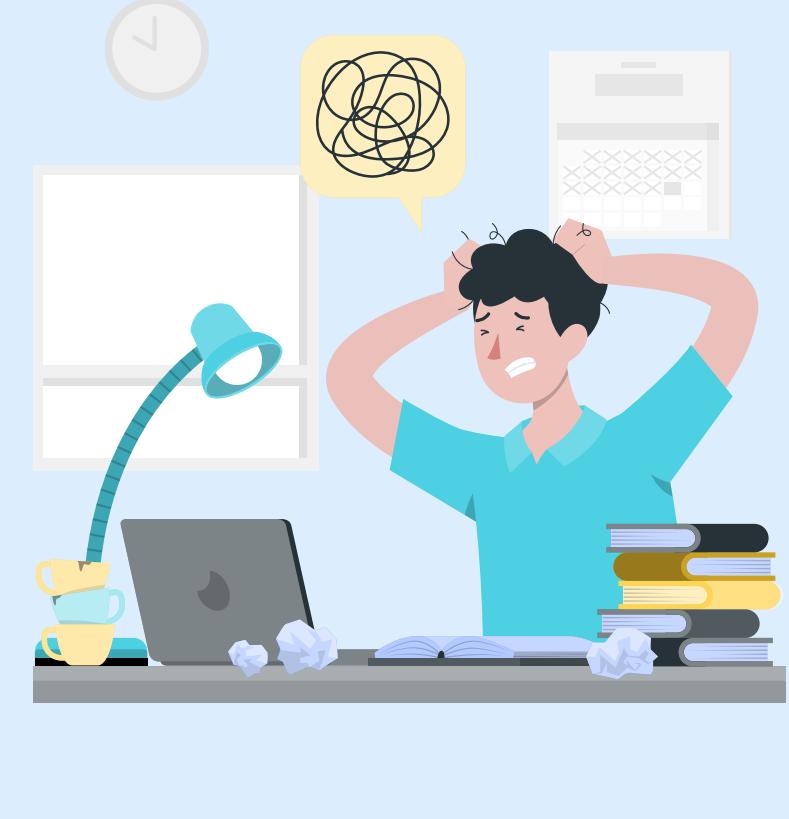
**Contacto eléctrico:**

Es inevitable que al trabajar con equipos electrónicos se sufra un riesgo eléctrico. La electricidad puede ocasionar daños en cuatro maneras diferentes: Choque eléctrico o electrocución, ignición de vapores inflamables, incendios por sobrecargas, caídas por electrocución, para evitar estos riesgos y sus perjudiciales consecuencias, se debe contar con las instalaciones adecuadas, además de realizar mantenimientos periódicos que garanticen su operabilidad. Respecto a los equipos eléctricos, se debe conocer y comprender su uso, mismo que deberá ser realizado por un experto y jamás permitir el acceso a zonas con peligro de descargas eléctricas como plantas o subestaciones a personal no autorizado. Puede consultar la guía RETIE colombiana para conocer más sobre este tema.



**Carga mental:**

Factor presente en todas las actividades, se debe tener presente que la carga mental para una actividad que requiera fuerza o destrezas físicas será la misma a una actividad que requiere de la lógica, el pensamiento y la toma de decisiones permanentes; por tanto se puede determinar que el nivel de carga mental está directamente relacionado con la exigencia del trabajo que se desarrolle y las condiciones en las que se realice en conjunto con las características de cada individuo. Algunos de los factores que determinan la carga mental son: contenido del trabajo, las condiciones ambientales, los aspectos psicosociales y organizativos, el puesto de trabajo, las exigencias del cargo, capacidad de respuesta del individuo, además de los factores personales y las condiciones extralaborales.



Cumplir con lo establecido en el Sistema de Seguridad y Salud en el Trabajo, permiten tener condiciones favorables para la ejecución de las actividades cotidianas, además; garantizan que el individuo desarrolle sus funciones en espacios propicios para tal fin.

### Riesgos laborales

Para ampliar los conceptos sobre los riesgos laborales del trabajo informático consulte el siguiente enlace:



[Enlace web. UNIR Revista. \(2020\). ¿Cuáles son los riesgos laborales del trabajo informático? UNIR.](#)

## 6 Manejo de posturas

Según informes internacionales, "los ataques a los sistemas de información utilizando malware aumentaron en un 150%, garantizar la seguridad informática en la plataforma tecnológica de la empresa es vital para el funcionamiento de la organización.

Para ilustrar mejor la información anterior, puede consultar el siguiente enlace:

### Ataques de sistemas de información

Para ampliar los conceptos sobre los riesgos laborales del trabajo informático consulte el siguiente enlace:



[Enlace web. El mundo registra un alarmante aumento de los ataques ciberneticos con sistemas de ransomware. \(2021\). TRT](#)

Así como en COBIT e ITIL se aplican buenas prácticas en el uso de los sistemas de información para evitar los "riesgos" en los que puede caer la infraestructura Tecnológica de la organización, se darán a continuación algunos criterios de seguridad para el software y la red de datos que permiten mejorar e incrementar la protección del sistema.

Algunos de los criterios de seguridad del software son:

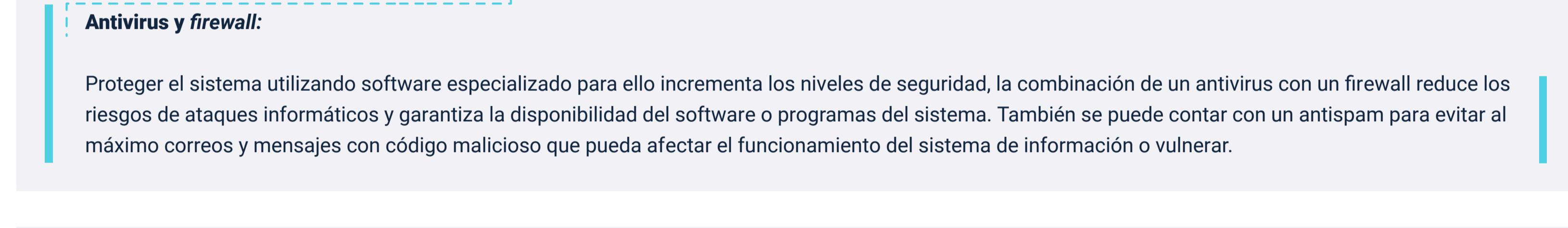


#### Criterios de seguridad del software



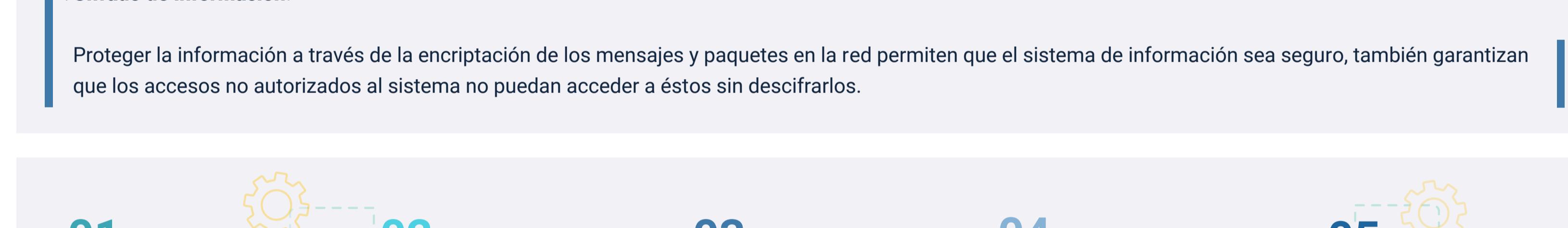
#### Servidor Propio:

Utilizar los servicios directamente en un servidor local permiten reducir los riesgos de los incidentes en el sistema de información, dará estabilidad a la red y reduce los tiempos de consulta agilizando las respuestas a los usuarios, también garantiza la ejecución de los aplicativos en un ambiente controlado y seguro.



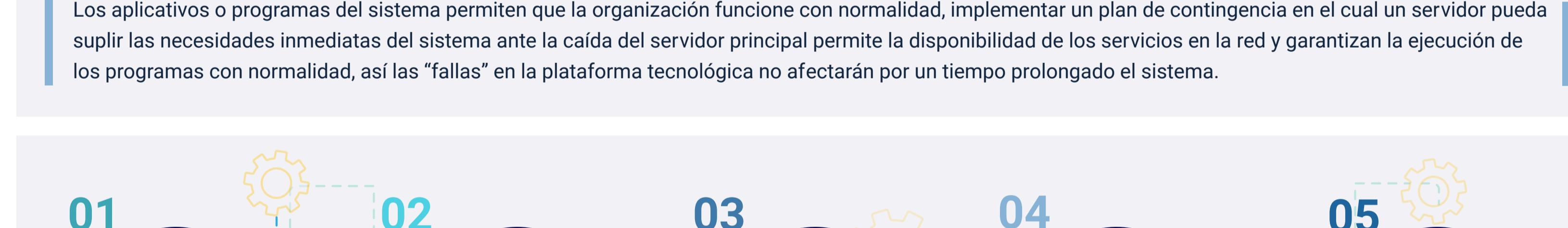
#### Antivirus y firewall:

Proteger el sistema utilizando software especializado para ello incrementa los niveles de seguridad, la combinación de un antivirus con un firewall reduce los riesgos de ataques informáticos y garantiza la disponibilidad del software o programas del sistema. También se puede contar con un antispm para evitar al máximo correos y mensajes con código malicioso que pueda afectar el funcionamiento del sistema de información o vulnerar.



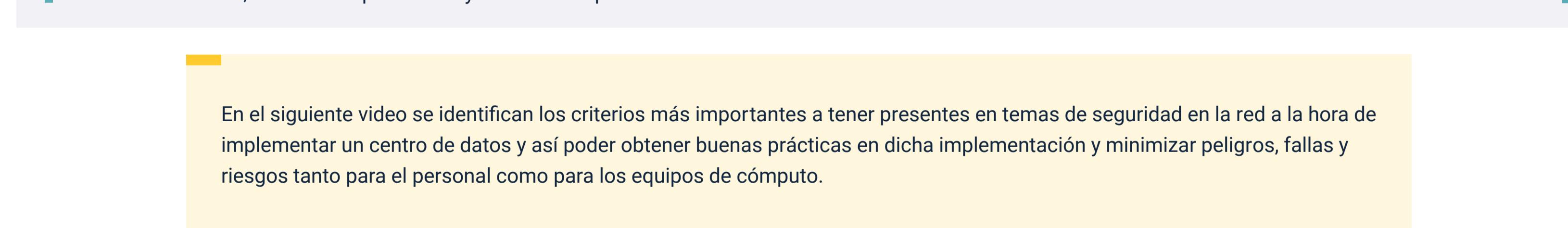
#### Cifrado de información:

Proteger la información a través de la encriptación de los mensajes y paquetes en la red permiten que el sistema de información sea seguro, también garantizan que los accesos no autorizados al sistema no puedan acceder a éstos sin descifrarlos.



#### Plan de contingencia:

Los aplicativos o programas del sistema permiten que la organización funcione con normalidad, implementar un plan de contingencia en el cual un servidor pueda suplir las necesidades inmediatas del sistema ante la caída del servidor principal permite la disponibilidad de los servicios en la red y garantizan la ejecución de los programas con normalidad, así las "fallas" en la plataforma tecnológica no afectarán por un tiempo prolongado el sistema.



#### Proteger el sistema:

Incrementar los niveles de protección, encriptar la información, crear niveles de acceso, implementar software antivirus, proteger el sistema a través de monitoreo, entre otros; permiten incrementar los niveles de seguridad, pero si el software como tal no es seguro, no vendrá bien todo el esfuerzo hecho con los demás elementos que integran al sistema; por lo tanto, el mismo software deberá contar con niveles de seguridad suficientes para protegerse ante anomalías como caídas del sistema, accesos no permitidos y fallas en la operación.

En el siguiente video se identifican los criterios más importantes a tener presentes en temas de seguridad en la red a la hora de implementar un centro de datos y así poder obtener buenas prácticas en dicha implementación y minimizar peligros, fallas y riesgos tanto para el personal como para los equipos de cómputo.



### Seguridad informática

Para conocer más información sobre medidas de seguridad informática consulte:



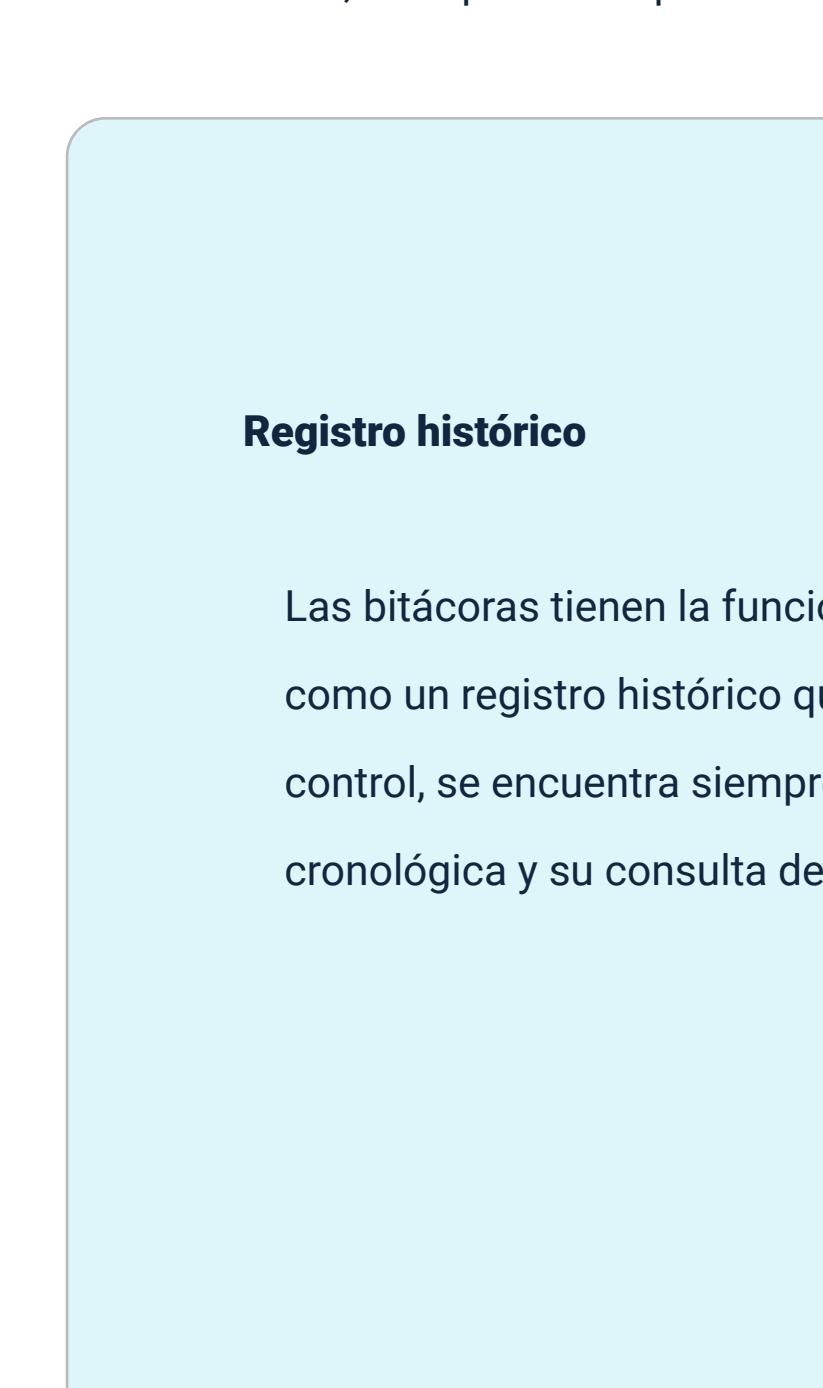
[Enlace web. Palacio, A. \(2017\). Las mejores medidas de Seguridad Informática. Com.mx.](#)



[Enlace web. Las 9 medidas de seguridad informática. \(2019\). Datos 101.](#)



## 7 Bitácoras e inventarios

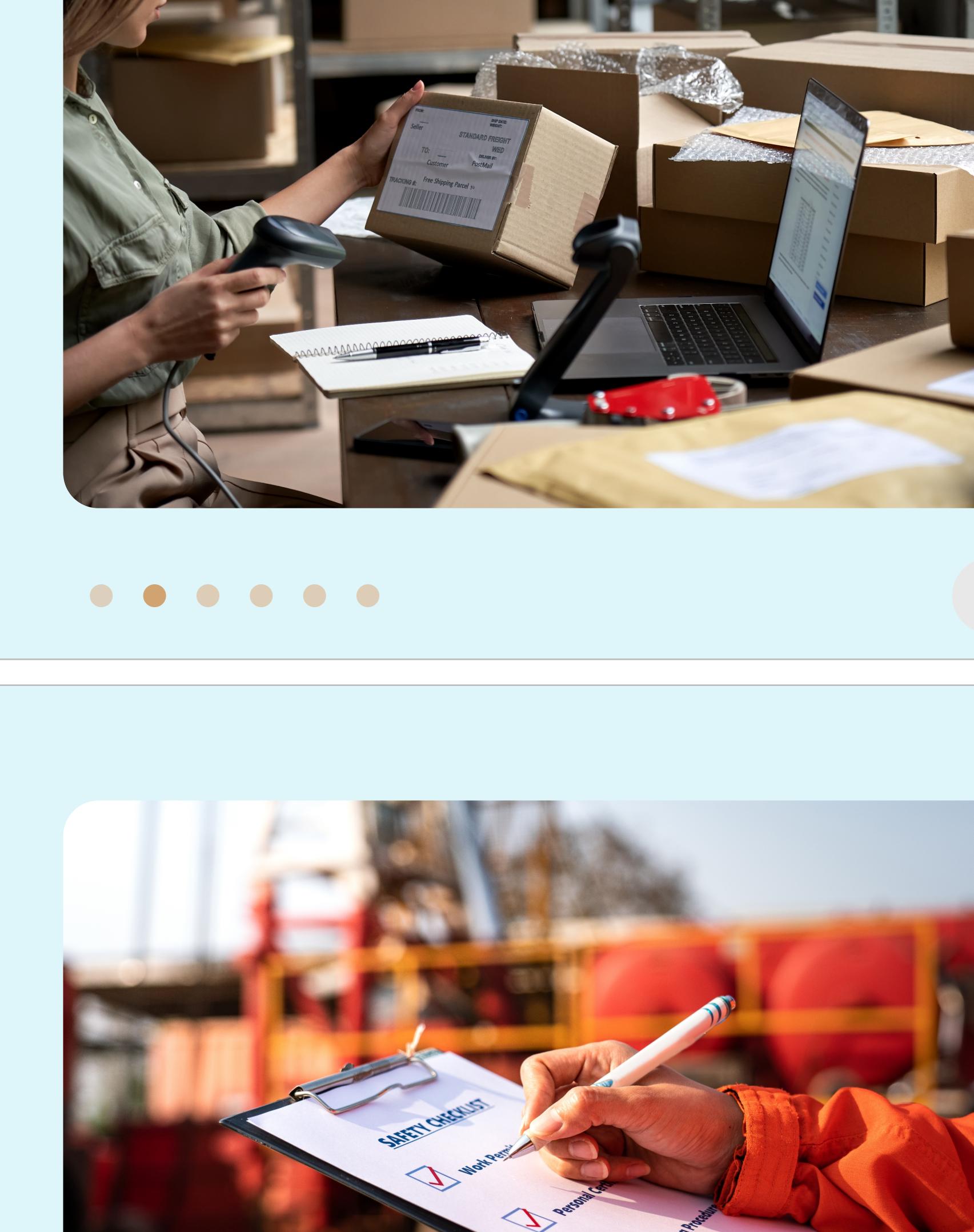


La palabra Bitácora proviene del francés *Bitacle* y su principal uso fue en la vida marítima. Corresponde a un instrumento que se fijaba a la cubierta, cerca del timón y de la aguja náutica que facilitaba la navegación en océanos desconocidos, era un cuaderno donde se narraban todos los acontecimientos que se presentaban, así quedaba constancia de cada uno de ellos. En la actualidad obtuvieron gran apogeo gracias a los weblogs o blogs que son bitácoras virtuales publicadas en Internet.

A continuación, se explica la importancia de tener registro de todos los eventos en las bitácoras donde se hace un seguimiento y control en el campo de IT.

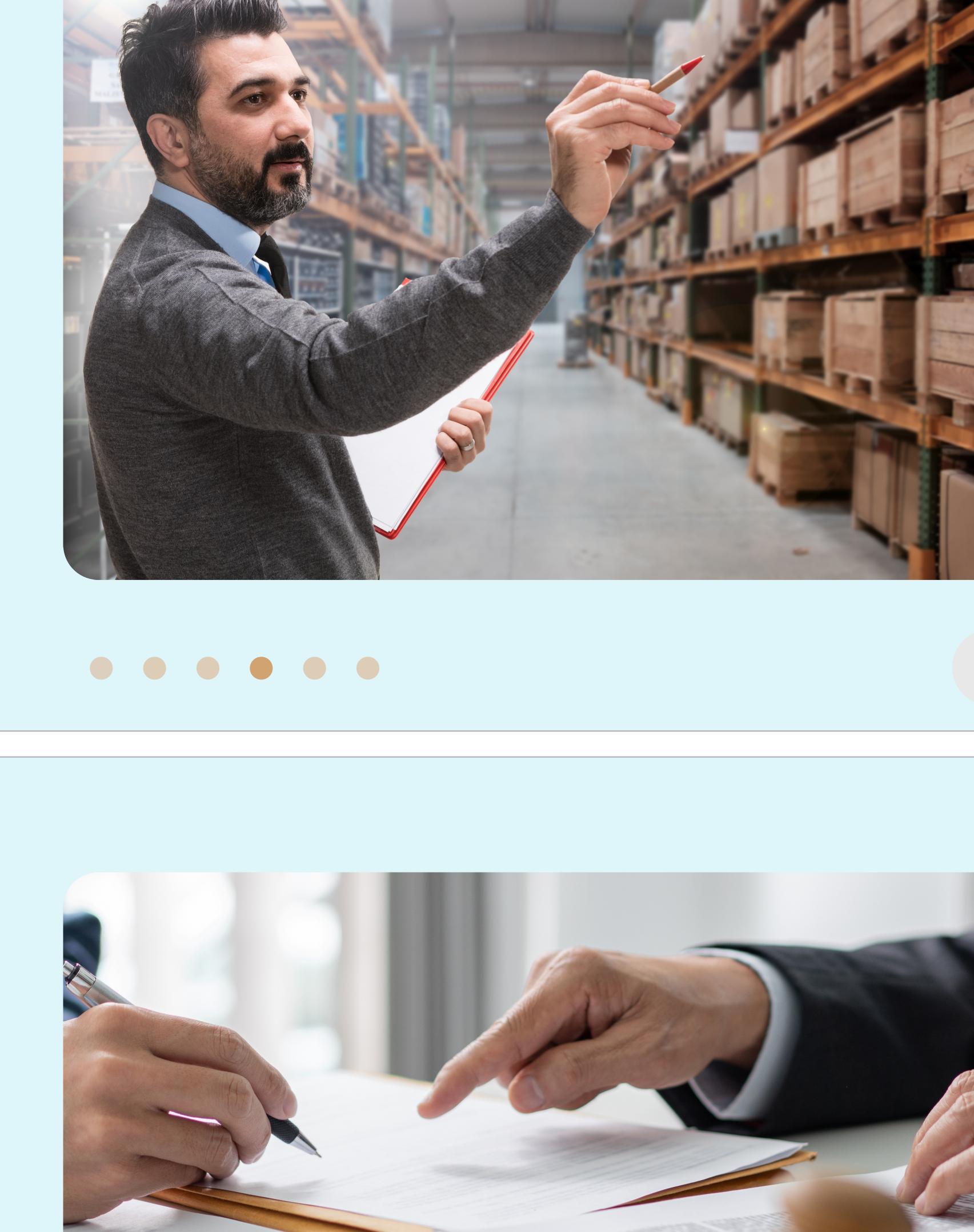
### Registro histórico

Las bitácoras tienen la función de guardar el día a día como un registro histórico que garantiza el seguimiento y control, se encuentra siempre organizado de manera cronológica y su consulta debe ser de fácil acceso.



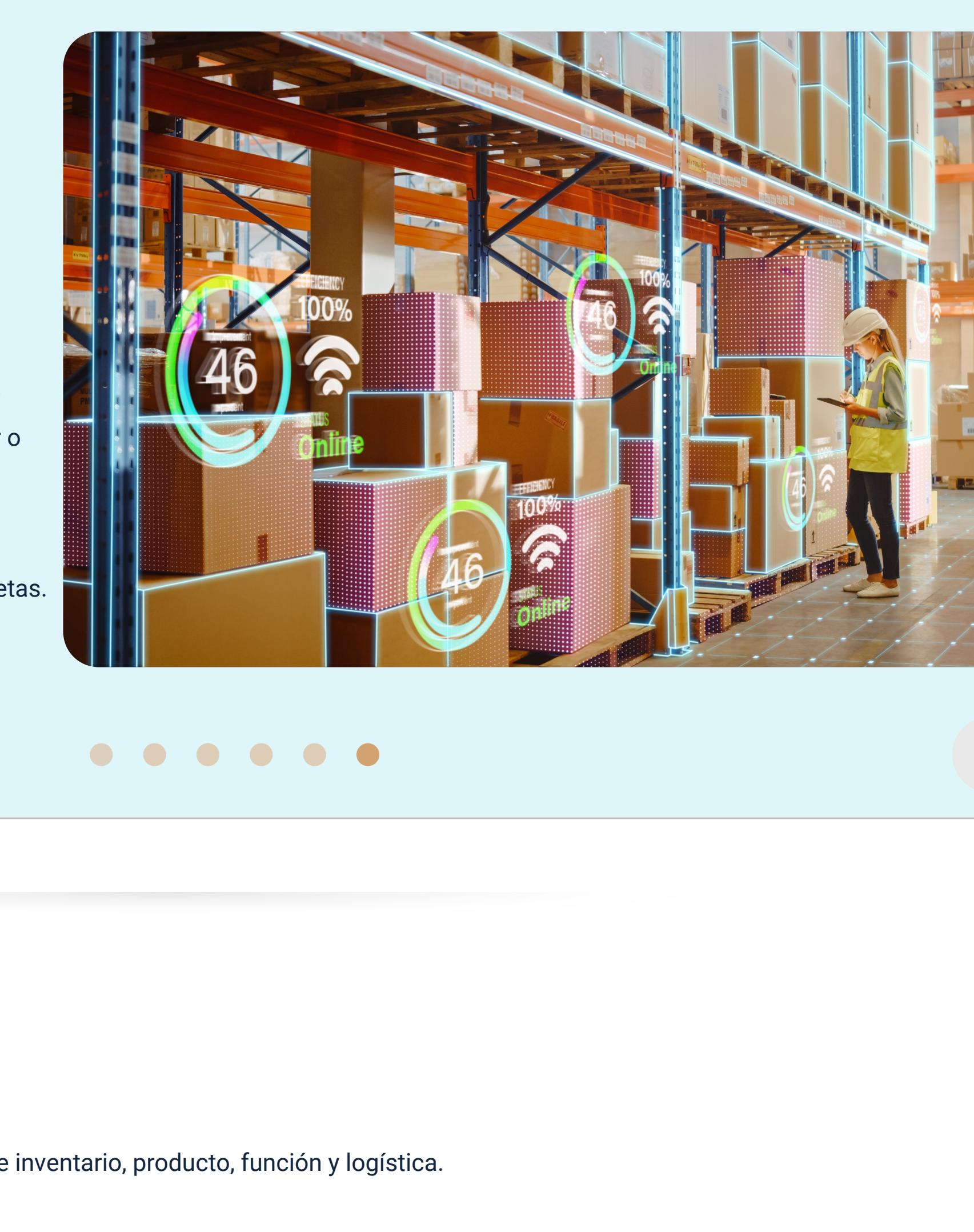
### Recopilar datos

En el campo de Infraestructuras TI, las bitácoras son de gran ayuda, permiten recopilar los históricos de cada dispositivo y así administrarlo para prevenir y/o corregir fallas que puedan afectar al sistema.



### Hoja de mantenimiento

Para dar un ejemplo de uso, si en la infraestructura TI ocurre un siniestro y es necesario acudir a la aseguradora para recuperar los activos que se vieron afectados, ésta solicitará al administrador TI la bitácora o hoja de mantenimiento de los mismos para garantizar su correcto uso, actividades de mantenimiento y reparaciones hechas; así podrá calcular el valor actual de cada dispositivo y proyectarlo de acuerdo a los criterios de la póliza, ofreciendo una compensación monetaria que permita recuperarlos nuevamente.



### Inventarios

Con respecto a los inventarios no solo permiten conocer la cantidad de dispositivos tiene una organización, su ubicación, valor de compra y depreciación; también una correcta gestión de inventarios garantiza la correcta administración de la infraestructura física de la organización y su futuro éxito.

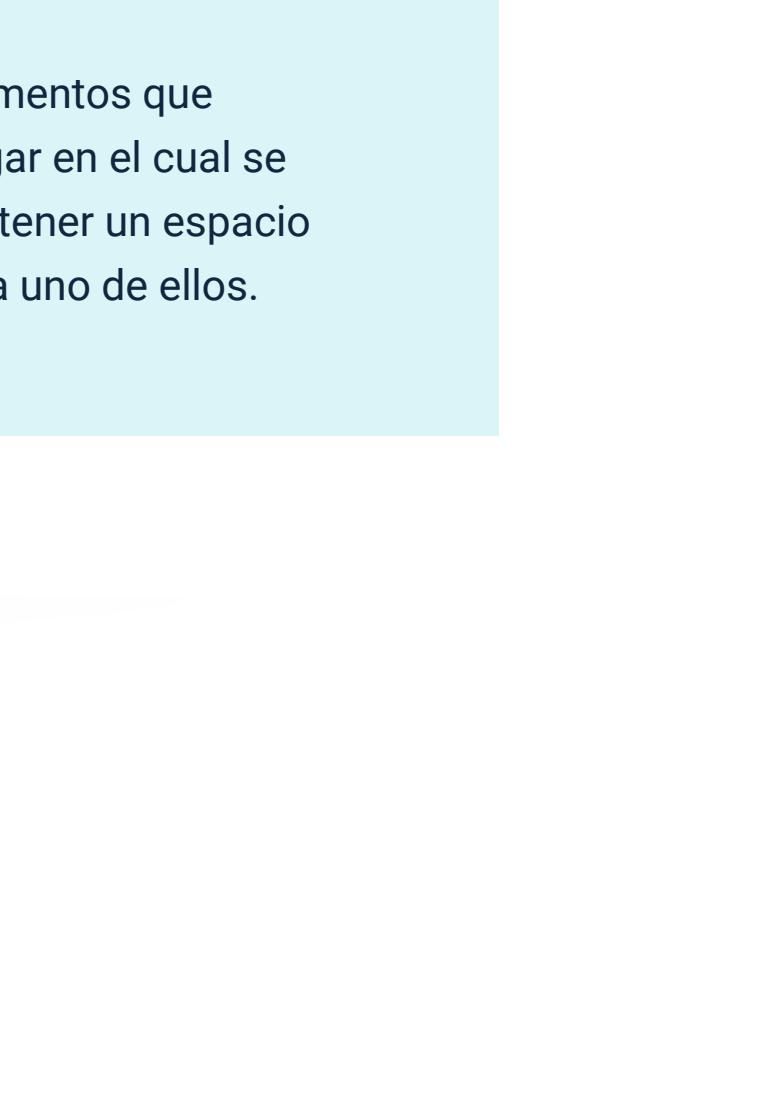
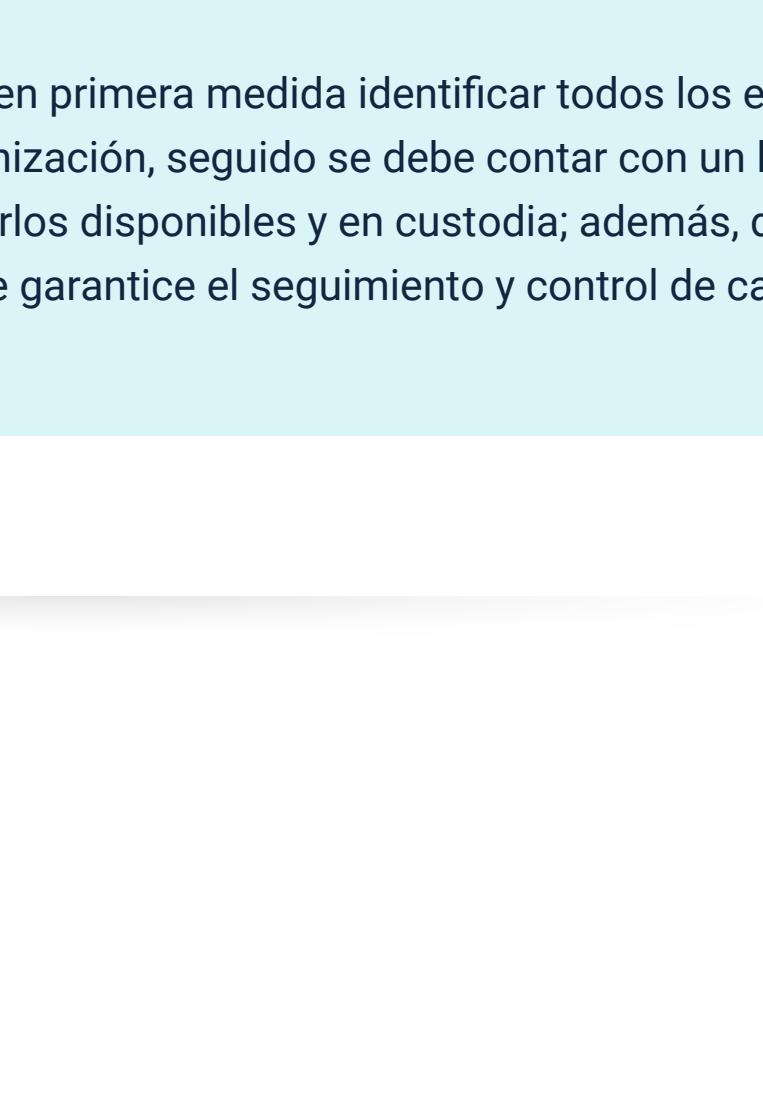
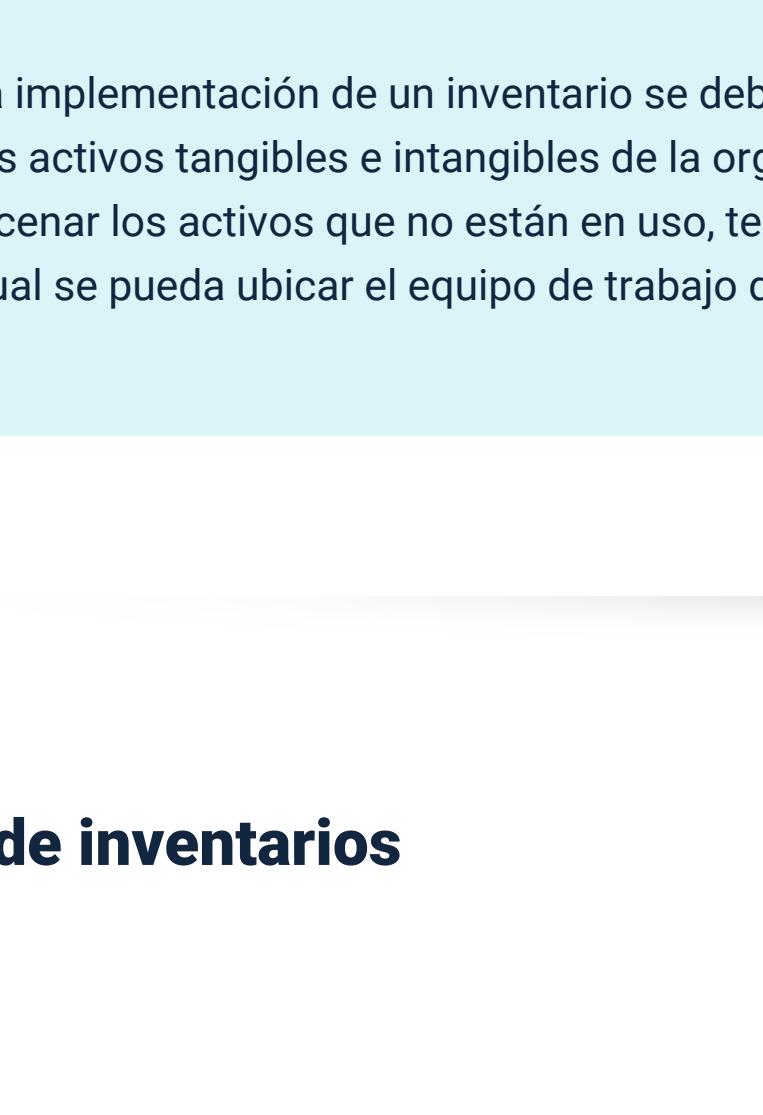


### 7.1 Clasificación de los Inventarios

A continuación, se muestra la clasificación de inventarios según tipo de inventario, producto, función y logística.

#### Tipo de Inventario

Según su ubicación: físicos, intangibles.



#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función

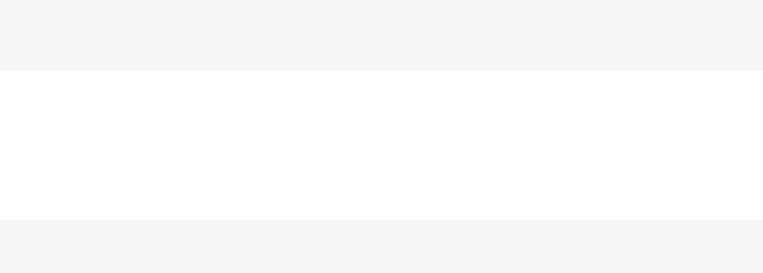


#### Tipo de Inventario

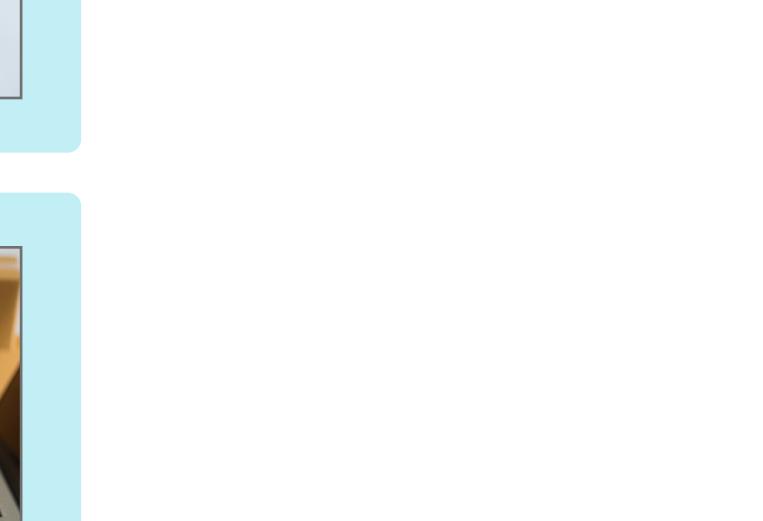
#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

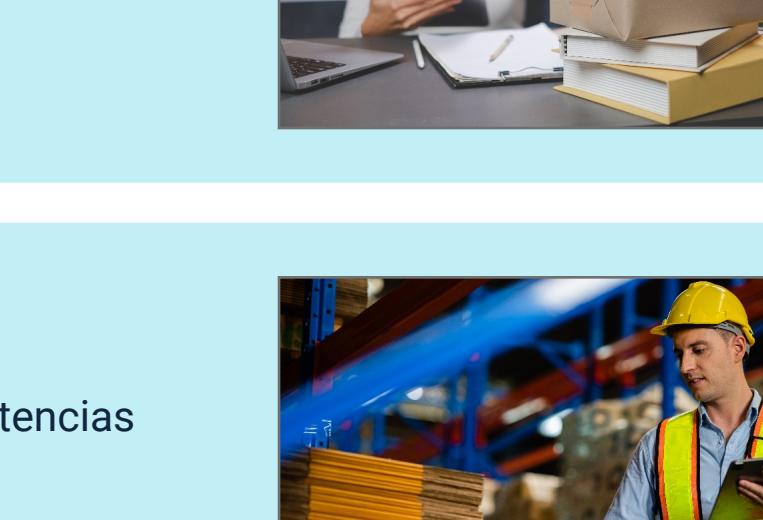
#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

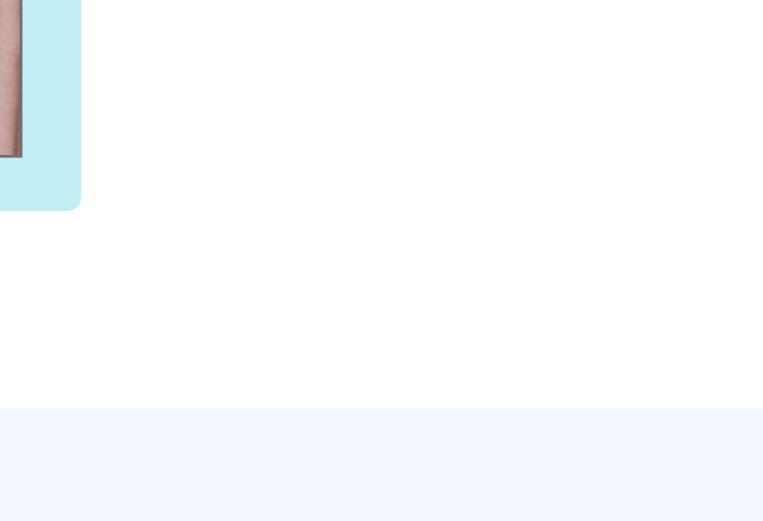
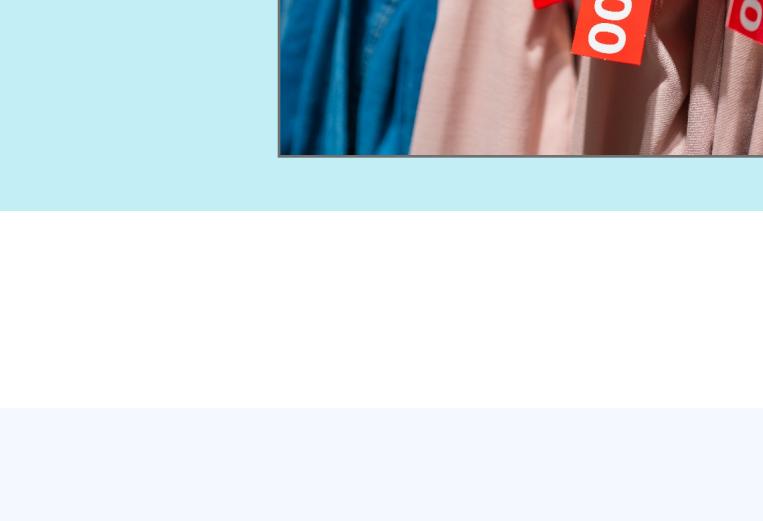
#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función

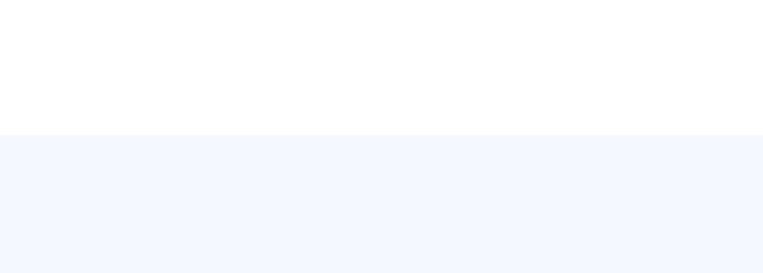
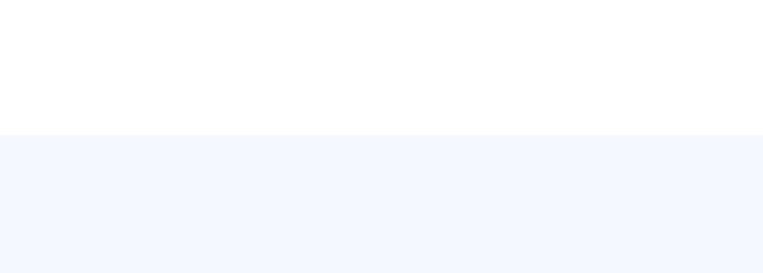


#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

#### Tipo de Producto

#### Tipo de Producto

Materias primas, productos en proceso de fabricación, productos terminados, suministros de fábrica.



#### De acuerdo a su función



#### Tipo de Inventario

#### Tipo de Producto

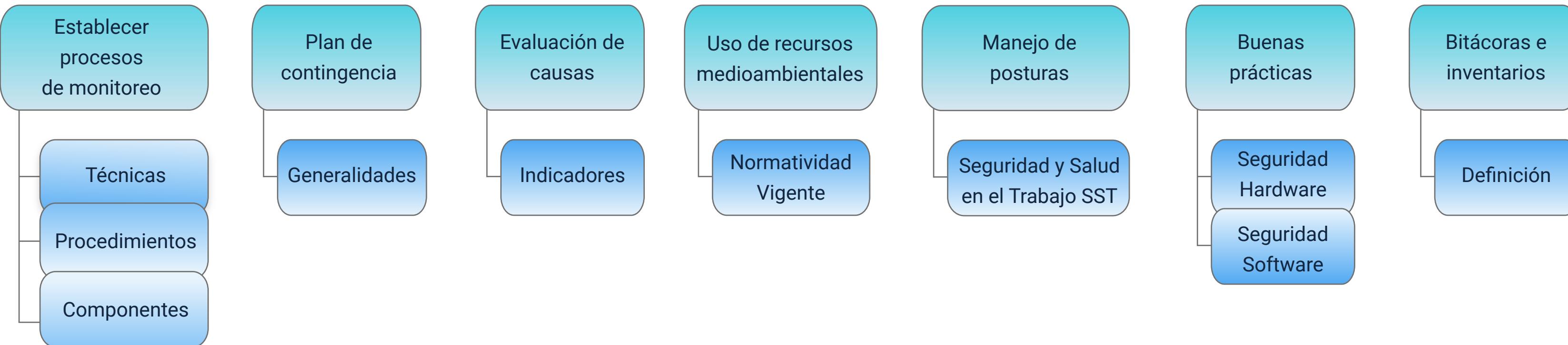
#### Tipo de Producto

## Implementación de infraestructura de tecnologías de la información y las comunicaciones.

Síntesis: Monitoreo a la infraestructura T.I según normativa vigente.



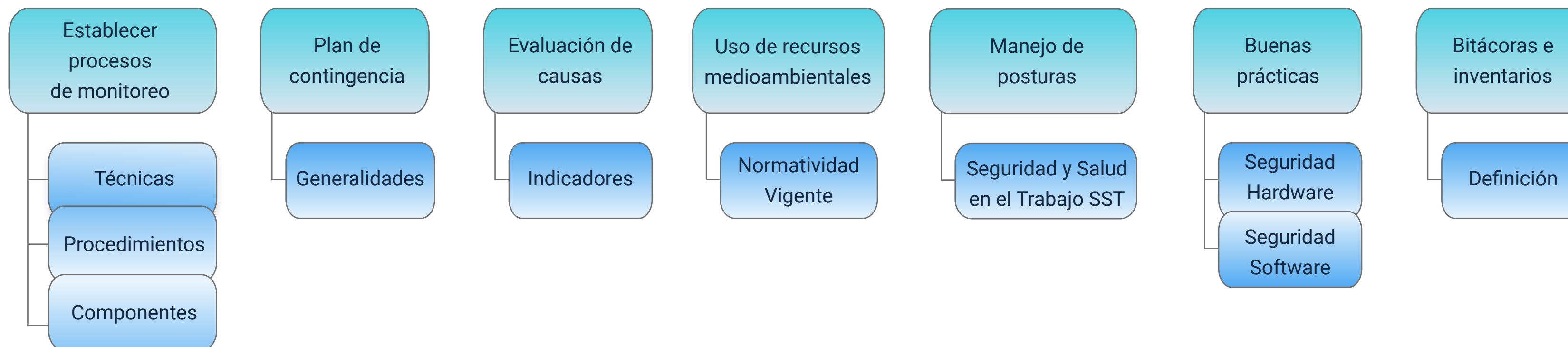
A través del componente formativo se conocerá la importancia del monitoreo al centro de datos, a través de la implementación de buenas prácticas basados en estándares nacionales e internacionales; adicionalmente, se abordarán los conceptos de seguridad y salud en el trabajo, factor clave para evitar riesgos y accidentes, también se conocerá la normatividad vigente en Colombia para la disposición de residuos tecnológicos.

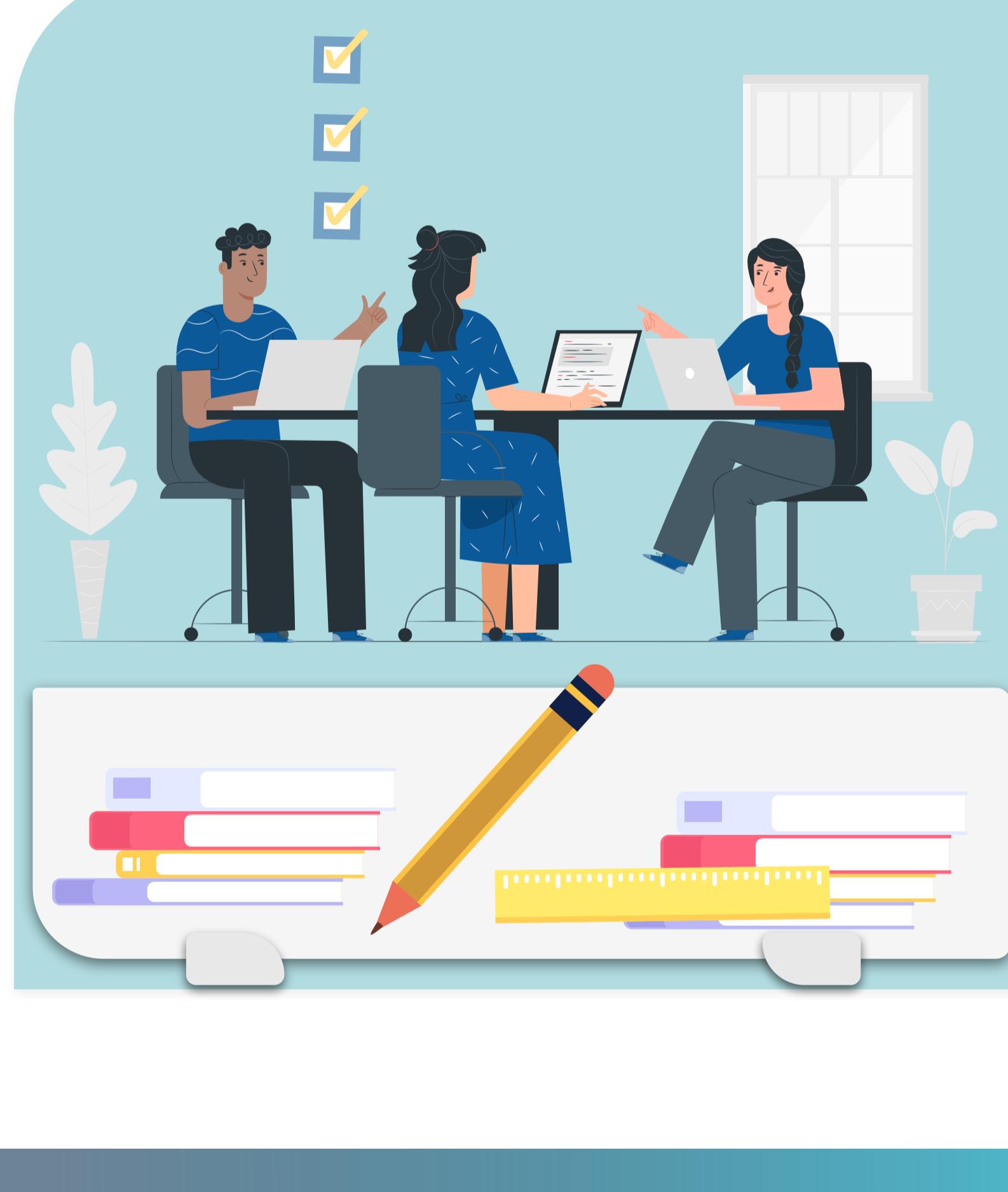


## Implementación de infraestructura de tecnologías de la información y las comunicaciones.

Síntesis: Monitoreo a la infraestructura T.I según normativa vigente.

A través del componente formativo se conocerá la importancia del monitoreo al centro de datos, a través de la implementación de buenas prácticas basados en estándares nacionales e internacionales; adicionalmente, se abordarán los conceptos de seguridad y salud en el trabajo, factor clave para evitar riesgos y accidentes, también se conocerá la normatividad vigente en Colombia para la disposición de residuos tecnológicos.



**Portada actividad****800 x 800****Portada actividad****800 x 800****Imagen acompañamiento Actividad****600\*600****Imagen Resultado****900\*600**

**i**

## Actividad didáctica



### Relación de Conceptos

Relacione la descripción con el concepto según el material y el conocimiento adquirido.

Relación de Conceptos

Realizar 