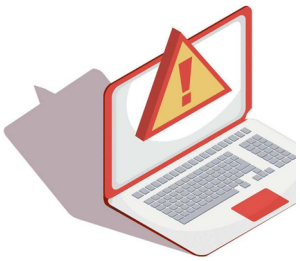


MANUAL DE BUENAS PRACTICAS

Guía completa de uso e interpretación

WWW.PEDROCONSULTING.ES

Pedro Consulting
Autónomo Pedro Jesús Acevedo Gelves

NIF: 06593924P
Teléfono: +34 627 618 838
Email: info@pedroconsulting.com | Web: www.pedroconsulting.es

Versión de documento: V1.0

Wallet:

17XTCKuxph6qdJvS9QvXA1BsCWxnzb3p9Z

Website:

www.pedroconsulting.es

INDICE:

¿QUÉ SON LAS BUENAS PRÁCTICAS? _____ PAG: 3

APLICACIÓN A LA SEGURIDAD INFORMÁTICA _____ PAG: 5

1. Gestión y control de sistemas antivirus
2. Gestión de actualizaciones automáticas
3. Gestión de copias de seguridad
4. Gestión de incidentes de seguridad
5. Gestión de la monitorización
6. Gestión de contraseñas
7. Gestión de usuarios
8. Base de datos de la gestión de la configuración (CMDB)
9. Revisión de Contratos / Mantenimientos / Licencias
10. Pruebas de planes de contingencia

REFERENCIAS CONSULTADAS _____ PAG: 21

¿QUÉ SON LAS BUENAS PRÁCTICAS?

El concepto de “buenas prácticas” se refiere a toda experiencia que se guía por principios, objetivos y procedimientos apropiados o pautas aconsejables que se adecuan a una determinada perspectiva normativa o a un parámetro consensuado, así como también toda experiencia que ha arrojado resultados positivos, demostrando su eficacia y utilidad en un contexto concreto

El concepto de buenas prácticas se utiliza en una amplia variedad de contextos para referirse a las formas óptimas de ejecutar un proceso, que pueden servir de modelo para otras organizaciones. Las buenas prácticas sistematizadas, permiten aprender de las experiencias y aprendizajes de otros, y aplicarlos de manera más amplia y/o en otros contextos. Pueden promover nuevas ideas o sugerir adaptaciones y proporcionar una orientación sobre la manera más efectiva de visibilizar los diversos impactos de una intervención en las comunidades.

La búsqueda de buenas prácticas se relaciona directamente con los actuales planteamientos sobre los criterios de calidad y eficiencia de las intervenciones sociales, que abarcan no sólo la gestión y los procedimientos, sino fundamentalmente la satisfacción de las necesidades de las personas afectadas y la superación de su problemática.

Diversas instituciones han desarrollado este concepto de identificación, selección –y en algunos casos distinción con premios- de buenas prácticas en contextos y con perspectivas muy diferentes: inclusión social, perspectiva de género, trabajo con jóvenes, urbanismo social, superación de conflictos, etc. Y cada una de estas propuestas utiliza perspectivas y criterios diferentes para la identificación y selección de las buenas prácticas. Haciendo una sistematización de los criterios comunes a todas las evaluaciones revisadas, podríamos decir que una buena práctica sería un programa, proyecto o intervención que tiene al menos algunas de las siguientes características:

- Responden a una necesidad identificada, son fruto de una evaluación cuidadosa de alguna característica en una población definida que se hace necesario modificar y mejorar y por tanto tiene objetivo definido, relevante y realista;

- Desarrollan estrategias basadas en la evidencia, y son innovadoras en su aplicación, demostrando capacidad de cuestionamiento y creatividad;
- Las estrategias y las acciones parten de unos principios y valores básicos y responden a una visión o perspectiva definida del problema que atiende;
- Los recursos humanos que implementan la iniciativa están calificados y especializados;
- Proponen un sistema riguroso de seguimiento a los procesos y los resultados de las acciones emprendidas a la vez que permiten la retroalimentación y reorientación de las acciones;
- Cuentan con una amplia base de participación, sobre todo de los beneficiarios, pero también de la comunidad, con alianzas interinstitucionales fuertes;
- Puede probar una mejora sustantiva de la situación que el dio origen;
- Incorpora estrategias de sostenibilidad de la iniciativa, propiciando su institucionalización;
- Sistematiza los procesos y resultados;
- Propicia de alguna manera la replicación de la experiencia.

APLICACIÓN A LA SEGURIDAD INFORMÁTICA

Mantener los equipos informáticos de una empresa correctamente es una actividad compleja que requiere de varias tareas que se han de ejecutar periódicamente y algunas diariamente, siempre en función de las necesidades que tengamos.

Debemos tener en cuenta que estas tareas no sólo son necesarias para asegurar un correcto funcionamiento de nuestros equipos, sino que además nos facilitarán el camino a la hora de resolver incidentes de seguridad complejos.

Por ejemplo, en caso de sufrir un ataque contra un equipo, si tenemos localizado, actualizado, y documentado todo lo referente del mismo, nos agiliza enormemente su pronta recuperación.

Este **decálogo de buenas prácticas de seguridad** tiene como objetivo recoger los aspectos fundamentales que deben considerarse en el mantenimiento de los equipos informáticos de una organización, comúnmente realizados por el Departamento Informático.

En cada tarea del decálogo se debería elaborar una guía concreta para el entorno concreto, adecuando los puntos y haciendo hincapié en las tareas a tratar para cada situación.

Cabe destacar el hecho de hacer una revisión periódica de ciertas tareas no exime del hecho de realizar una buena labor diaria, es decir, que si cada mes revisamos los parches de seguridad de un equipo, si se recibe una actualización crítica, no debemos esperar a que se cumpla el mes para su actualización.

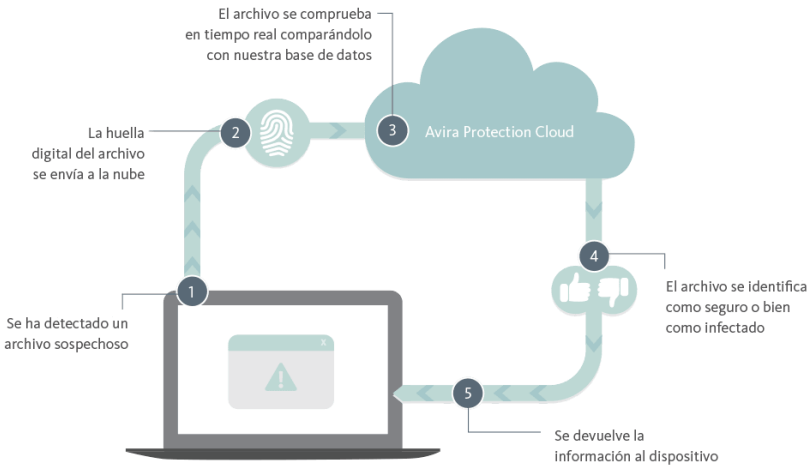
A continuación os mostramos el siguiente decálogo, con las tareas periódicas más importantes a la hora de mantener correctamente los equipos informáticos de nuestra empresa.

1. Gestión y control de sistemas antivirus

Un Antivirus informático es básicamente un conjunto de programas que protegen nuestra computadora del daño que pueda causar cualquier software o programa maligno. El nombre de Antivirus tiene su origen en el hecho de que el programa fue diseñado originalmente para combatir los virus informáticos.

El Software antivirus usa dos métodos para proteger el sistema:

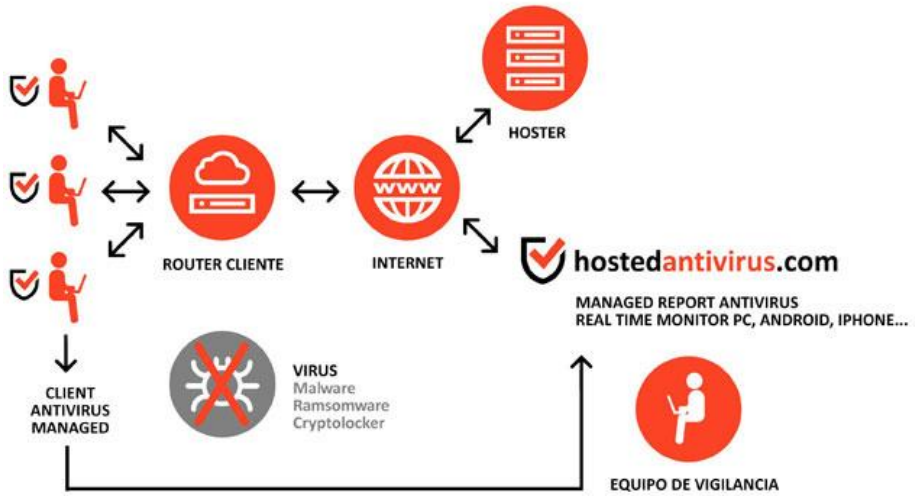
1. El primero es analizar nuestros archivos comparándolos con una base de datos de software o programas malignos
2. El segundo es la monitorización constante del comportamiento de archivos de nuestro sistema que pueden estar infectados.



Debemos verificar que todos los equipos se encuentren en el sistema de gestión del antivirus corporativo, y que los análisis periódicos de los equipos se realicen correctamente, para evitar posibles infecciones.

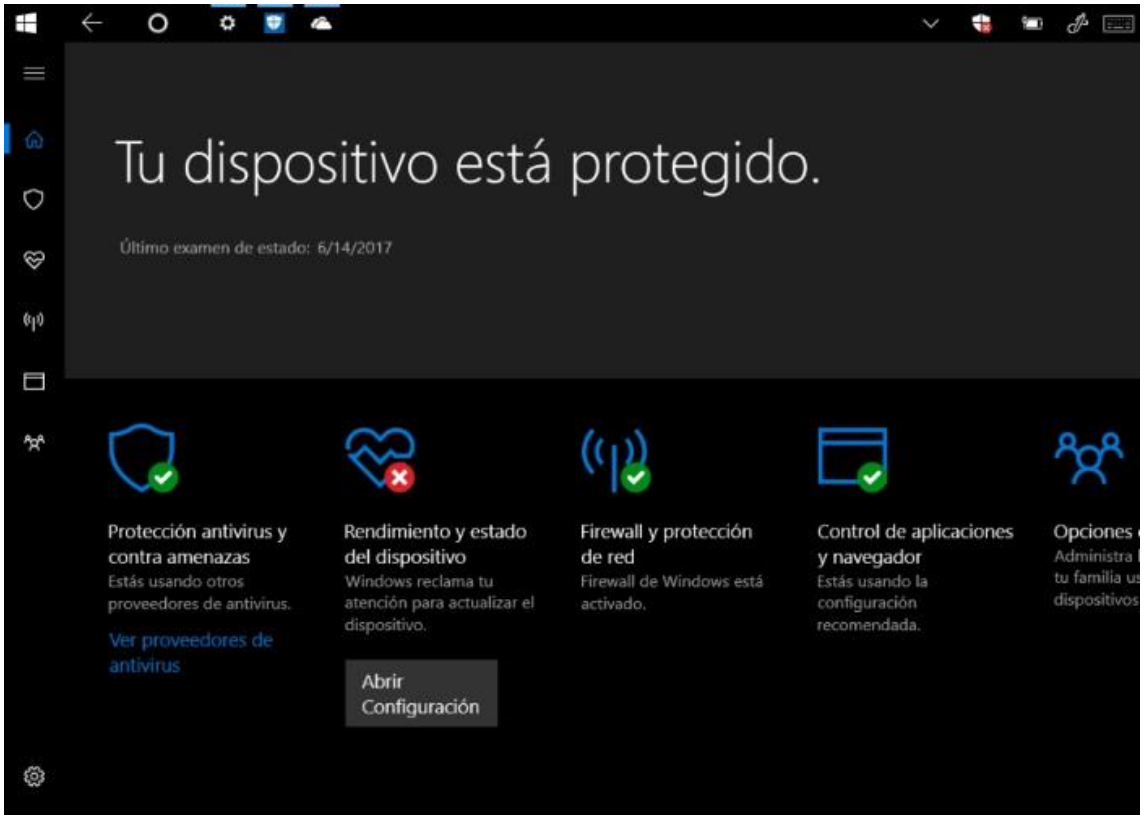
Hoy en día existen multitud de herramientas que nos facilitarán la ejecución de este trabajo, por lo que un mantenimiento adecuado, no resulta complicado.

Debemos tener una buena gestión acompañado de una programación de revisiones periódicas para corroborar que todo se realiza correctamente.



2. Gestión de actualizaciones automáticas

Las actualizaciones son añadidos o modificaciones realizadas sobre los sistemas operativos o aplicaciones que tenemos instalados en nuestros dispositivos y cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad.

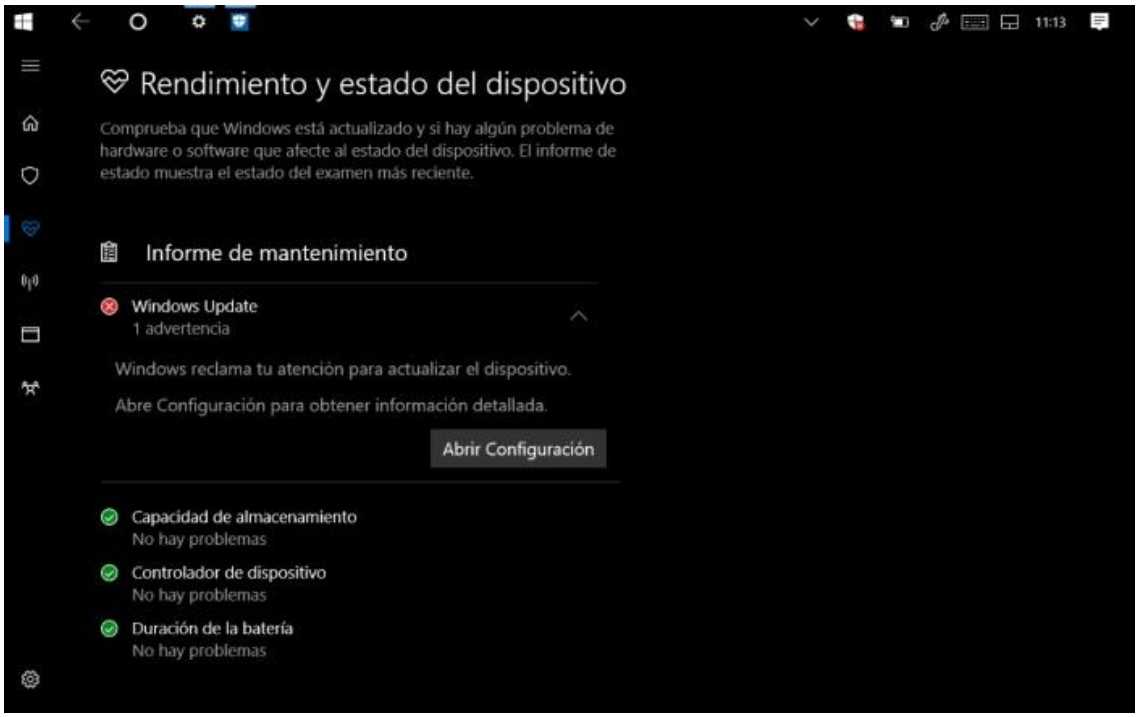


Si no mantenemos nuestros equipos al día nos exponemos a todo tipo de riesgos: robo de información, pérdida de privacidad, perjuicio económico, suplantación de identidad, etc.

Es importante SIEMPRE cumplir con estos parámetros en las actualizaciones:

- Vigilar el estado de actualización de todos nuestros dispositivos y aplicaciones.
- Elegir la opción de actualizaciones automáticas siempre que esté disponible.
- Instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus.
- Ser cuidadosos con las aplicaciones que instalamos, huyendo de fuentes no confiables y vigilando los privilegios que les concedemos.
- Evitar hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad.

Debemos revisar que las actualizaciones de la base de datos del servidor, parches de seguridad, vulnerabilidades, etc. se han realizado correctamente. Hoy en día, un mes es demasiado tiempo para realizar ciertas tareas, y automatizar las funciones más básicas te permite evitar multitud de incomodas situaciones.



Por ello, con una buena organización y configuración, facilitamos enormemente la gestión. Pero siempre hemos de revisar que todo se realiza correctamente.

3. Gestión de copias de seguridad

Una **copia de seguridad**, **respaldo, copy backup, copia de respaldo**, **copia de reserva** (del inglés ***backup***) en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Las copias de seguridad son útiles ante distintos eventos y usos:

1. recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque de hacking.
2. Restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas.

3. guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales, etc

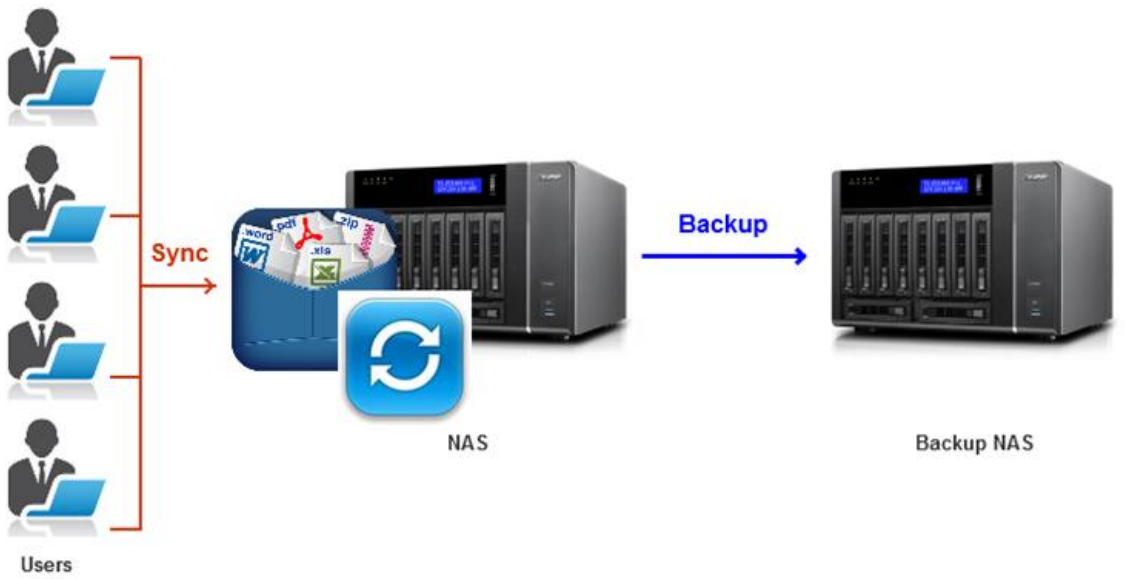
El proceso de copia de seguridad se complementa con otro conocido como **restauración de los datos,** que es la acción de leer y grabar en la ubicación original u otra alternativa los datos requeridos.

Ya que los sistemas de respaldo contienen por lo menos una copia de todos los datos que vale la pena salvar, deben de tenerse en cuenta los requerimientos de almacenamiento.

La organización del espacio de almacenamiento y la administración del proceso de efectuar la copia de seguridad son tareas complicadas.

Para brindar una estructura de almacenamiento es conveniente utilizar un modelo de almacenaje de datos.

Ejemplo:



Plantear una buena estrategia de copias de seguridad es básico hoy en día. Hay que ser conscientes que los equipos informáticos pueden sufrir fallos, borrados o perdidas de información accidental o deliberada.

Por ello, se debe establecer una política de copias de seguridad de toda la información que consideremos vital para la empresa.

4. Gestión de incidentes de seguridad

Un incidente de seguridad informática es la violación o amenaza inminente que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad).

Gestionar correctamente los incidentes de seguridad que puedan surgir en nuestra empresa es de vital importancia.

Para ello debemos:

- **en primer lugar identificar el incidente,** que puede recepcionarse por la notificación de un usuario o por su identificación desde el departamento de TI mediante el análisis de logs, o anomalías en los sistemas.
- **Después debemos clasificarlo en base a su criticidad, tipología, equipos afectados, etc. para posteriormente poder mitigarlo y contenerlo.** Esto puede pasar por aislar el equipo que ha sufrido el incidente, o detener algún servicio o aplicación hasta que se resuelva, o su escalado para obtener una ayuda o soporte especializado.

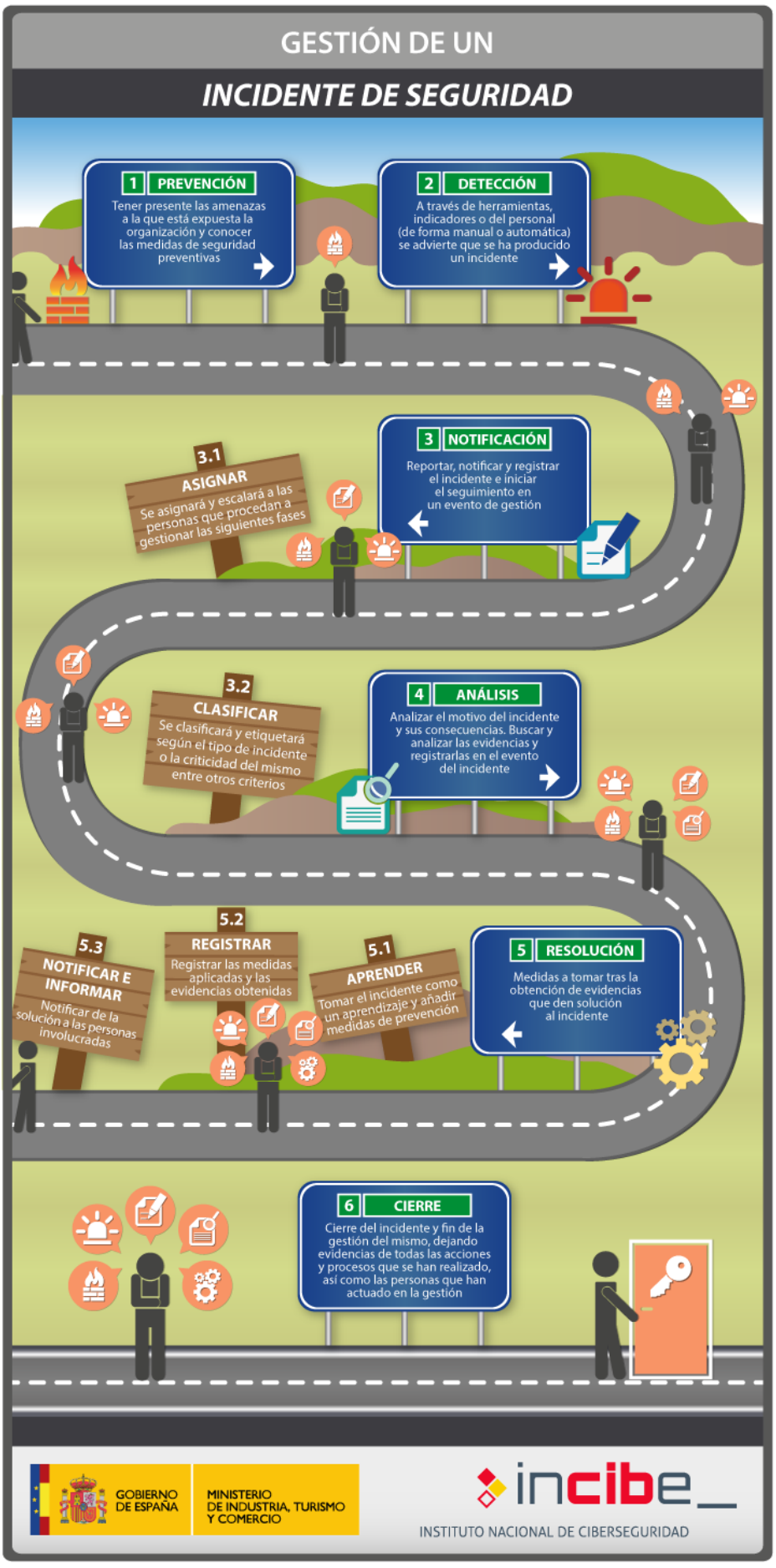
Por este motivo es importante tener la capacidad, en primer lugar, de prevenirlos, y en segundo, de detectarlos y de responder adecuadamente a ellos.

La detección se basa obligatoriamente en el despliegue de sistemas de vigilancia y en el uso adecuado de los mismos, mientras que la respuesta adecuada a los incidentes de seguridad pasa en primer lugar por la identificación clara de cualquier incidente, su escalado hacia los grupos gestores del mismo correctos en cada caso y su contención, erradicación y recuperación.

Y por supuesto, en todos los casos, por unas lecciones aprendidas: es imposible predecir un incidente, y el daño, por definición, será alto, con lo que un aspecto crítico es aprender de cada incidente de seguridad que suframos y mejorar nuestra protección para que, en un futuro, no nos pase algo similar y si nos pasa el daño sea mínimo.

- **Por último debemos recuperar los sistemas afectados y documentar lo ocurrido.**

En la siguiente página, el **INCIBE *(Instituto Nacional de Ciberseguridad)*** nos muestra una infografía muy útil y bien explicada de cómo gestionar este tipo de incidentes.

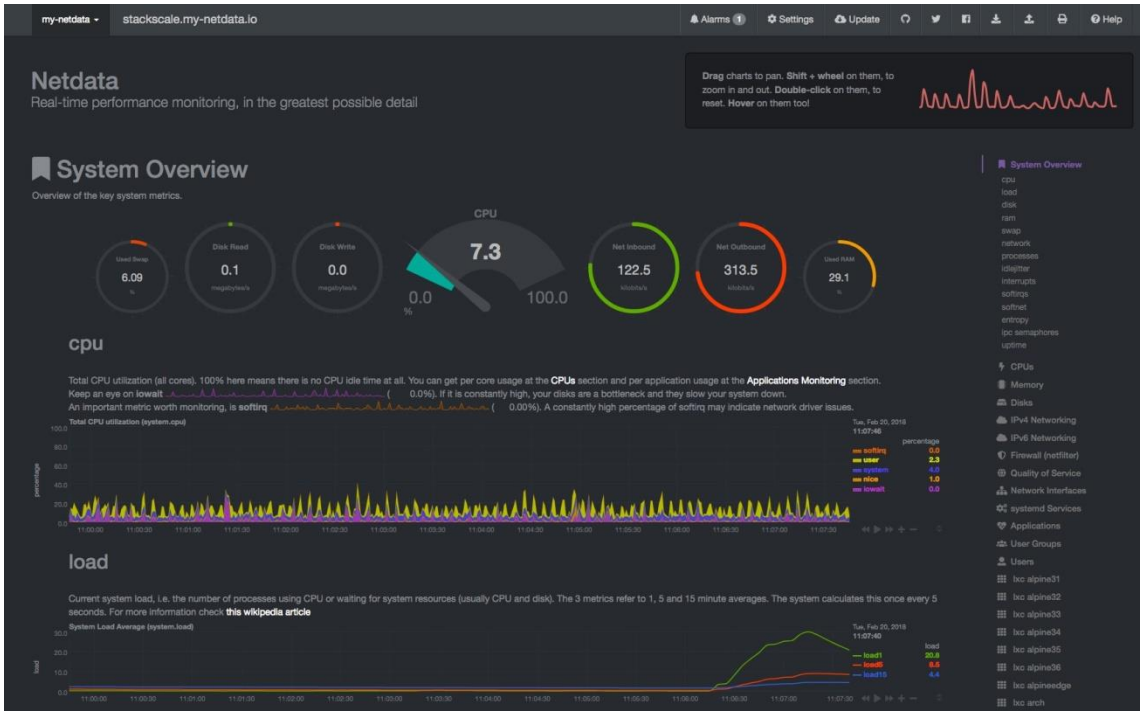

GESTIÓN DE UN
INCIDENTE DE SEGURIDAD
1 PREVENCIÓN
Tener presente las amenazas a la que está expuesta la organización y conocer las medidas de seguridad preventivas
2 DETECCIÓN
A través de herramientas, indicadores o del personal (de forma manual o automática) se advierte que se ha producido un incidente
3 NOTIFICACIÓN
Reportar, notificar y registrar el incidente e iniciar el seguimiento en un evento de gestión
3.1 ASIGNAR
Se asignará y escalará a las personas que procedan a gestionar las siguientes fases
4 ANÁLISIS
Analizar el motivo del incidente y sus consecuencias. Buscar y analizar las evidencias y registrarlas en el evento del incidente
3.2 CLASIFICAR
Se clasificará y etiquetará según el tipo de incidente o la criticidad del mismo entre otros criterios
5 RESOLUCIÓN
Medidas a tomar tras la obtención de evidencias que den solución al incidente
5.1 APRENDER
Tomar el incidente como un aprendizaje y añadir medidas de prevención
5.2 REGISTRAR
Registrar las medidas aplicadas y las evidencias obtenidas
5.3 NOTIFICAR E INFORMAR
Notificar de la solución a las personas involucradas
6 CIERRE
Cierre del incidente y fin de la gestión del mismo, dejando evidencias de todas las acciones y procesos que se han realizado, así como las personas que han actuado en la gestión
GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

5. Gestión de la monitorización

Es imprescindible en cualquier empresa tener un sistema que controle diferentes características de los sistemas tecnológicos. Desde la monitorización de la carga de un SAI, hasta la temperatura de los CPD, los registros de los sistemas antivirus, los elementos de seguridad de la red, el volumen de tráfico de la salida a Internet o la propia carga de CPU o Disco Duro de cualquier servidor.

Este tipo de aplicativos deber de tener un sistema de aviso ante cortes, pérdidas de servicio o fallas puntuales, pero además permitir la obtención de informes periódicos de cada elemento para tener un registro y prever de manera proactiva cambios o sustituciones que pueden evitar fallos posteriores que resultasen insalvables.

Herramientas tan poderosas como ***NAGIOS o NETDATA*** nos ayudan a conseguir que todo en nuestro Data Center este bajo nuestro control:

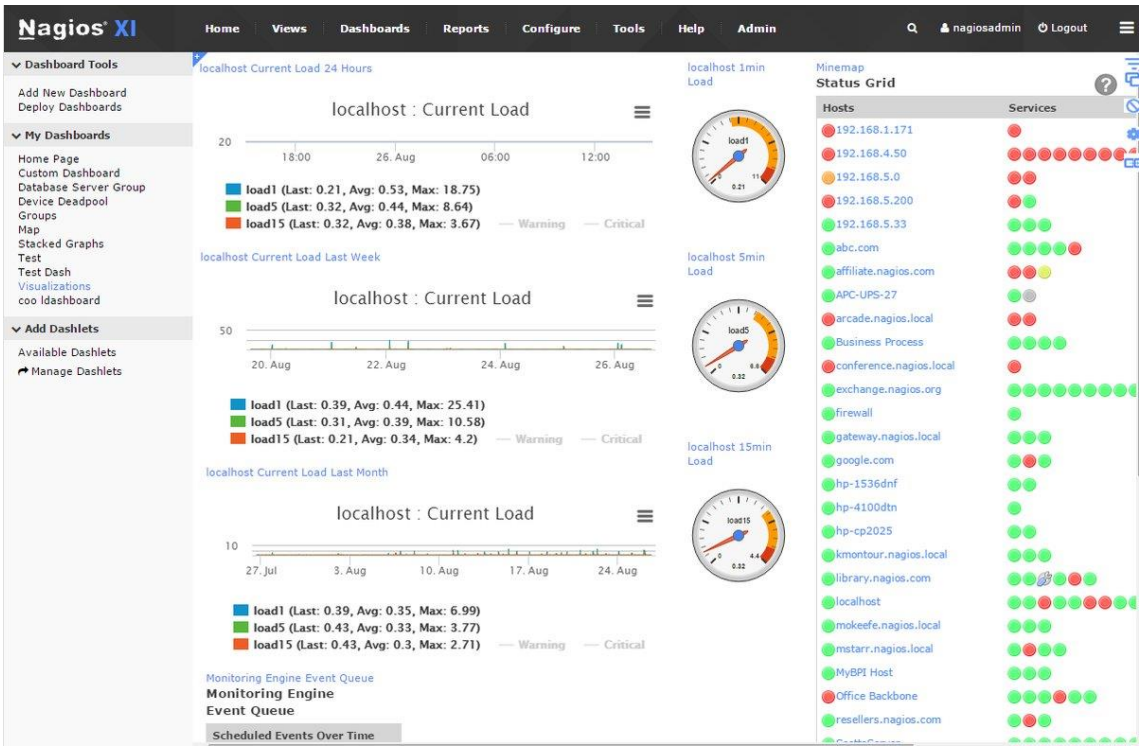


Generalmente los sistemas informáticos, actualmente complejos y difíciles de configurar, no fallan sin previo aviso. Tanto los **sistemas físicos** (ordenadores de la empresa, impresoras, routers, servidores, firewalls) así como los **sistemas lógicos** (conexión a Internet, línea telefónica, bases de datos, software…) suelen presentar pequeños fallos y problemas, que con el tiempo, producen la pérdida de servicio o inducen a errores graves.

Con un sistema de monitorización, en nuestra empresa seremos capaces de **obtener información de los sistemas**, antes y después de una adversidad, para realizar un **análisis** y mejorar el servicio, además de responder rápidamente ante un problema.

Manteniendo los sistemas informáticos monitorizados, conseguiremos más fácilmente **prever, solucionar y mejorar los servicios de la empresa**. Si contamos con un sistema de monitorización moderno y eficiente conseguiremos:

- Reducción de costes e incidencias
- Notificación de problemas leves y graves en nuestros sistemas
- Prevención de interrupciones de servicio o vulnerabilidades
- Análisis del rendimiento y seguridad de la empresa
- Análisis, detallado y en tiempo real, del acceso a nuestros sistemas
- Mejor aprovechamiento de los recursos

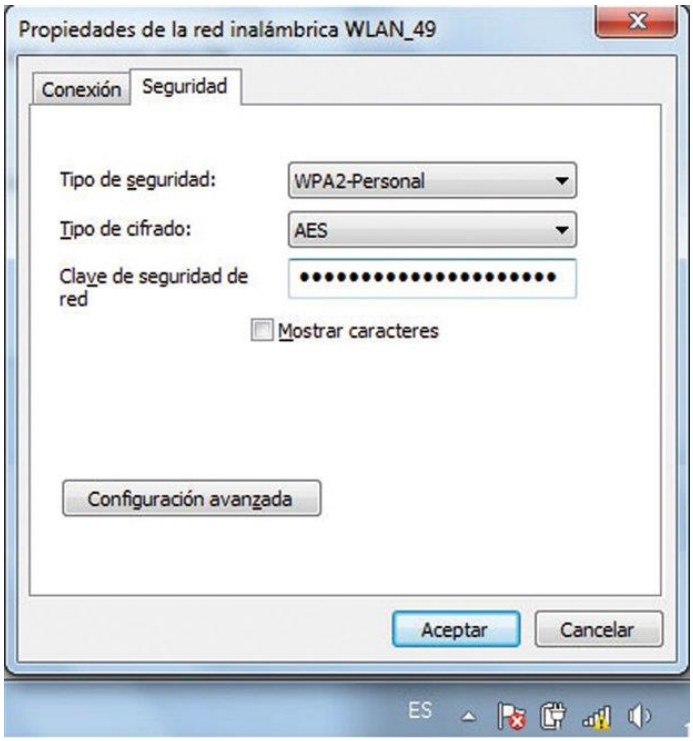


Dado que en una empresa existen muchos sistemas informáticos, a menudo se suelen desaprovechar o gestionar de manera incorrecta, lo cual tiene un coste económico mayor. Manteniendo el sistema monitorizado, seremos capaces de obtener métricas de uso real de cada equipo y **organizar de manera eficiente los recursos**, además de mantener a raya la seguridad integral de todos los equipos de la empresa.

6. Gestión de contraseñas

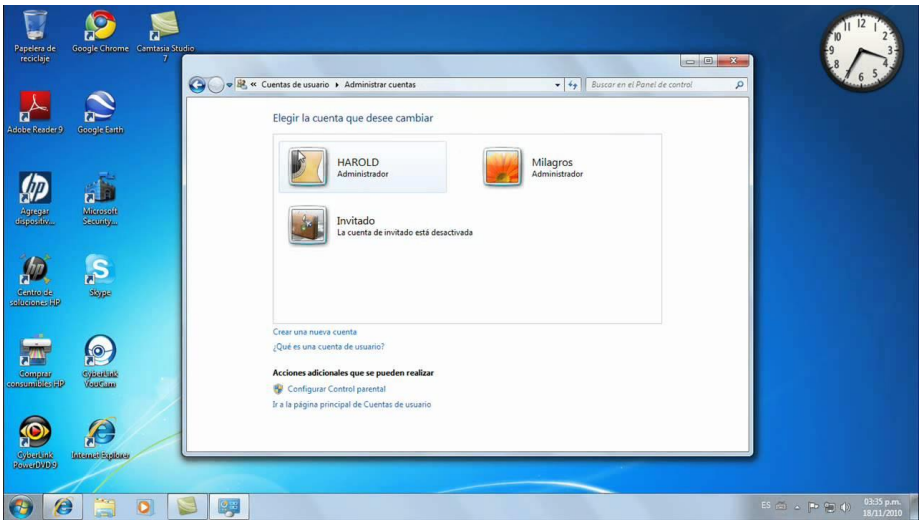
Es recomendable tener un protocolo de cambio de contraseñas críticas en un entorno corporativo. Hay que tener en cuenta que con el tiempo, muchas contraseñas pasan por demasiadas manos, lo que puede suponer un problema de seguridad.

Cambiar periódicamente la contraseña de la wifi pública, activar la caducidad de las contraseñas de los usuarios del directorio activo o modificar las claves de los equipos en producción de vez en cuando, ayuda a asegurarnos que nuestros trabajadores tienen acceso únicamente a los recursos necesarios para su desempeño.



7. Gestión de usuarios

En un SO multiusuario se utiliza el concepto de **usuario** para controlar el acceso al sistema. Se pueden declarar diferentes **usuarios** y asignar un nivel de acceso diferente, o unos privilegios, para cada uno de ellos.



Muchas veces no se cursa correctamente la baja de un usuario en los sistemas o queda algún usuario que no se tenía en cuenta en algún momento. No está de más programar informes que nos adviertan de usuarios inactivos en el sistema y poder así eliminar o deshabilitar aquellas cuentas de acceso al servidor que no sean necesarias.

Por ejemplo, podemos generar avisos mensuales de usuarios inactivos durante más de un mes. Así, con ésta información, podemos valorar la necesidad de cursar la baja de los mismos, evitando tener cuentas en el sistema de usuarios inactivos de cualquier tipo, ya sean cuentas de usuario, de VPN o de algún aplicativo concreto.

Si se van a definir diferentes usuarios/grupos para controlar el acceso al sistema, es necesario aplicar algunas medidas elementales:

- Se debe explicar a los usuarios que las cuentas son **estrictamente personales.** Cualquiera que acceda a su cuenta, porque la dejan abierta, o porque le dicen el usuario/contraseña a otra persona, puede realizar las mismas acciones que ellos.
- **No se deben escribir las contraseñas en papel, ni en el teclado, ni en la mesa debajo del teclado, ni en una nota junto al monitor, etc...**
- Las contraseñas **no deben ser fáciles de adivinar.** Una persona que conozca al usuario puede adivinar una contraseña con datos personales. Una máquina puede probar de manera automática muchas contraseñas hasta dar con la

correcta (ataques basados en diccionarios). Una buena contraseña debe incluir mayúsculas, minúsculas, números y signos, además de contar con una longitud suficiente. El administrador puede establecer criterios como: longitud mínima, tiempo máximo de uso de la contraseña, etc.

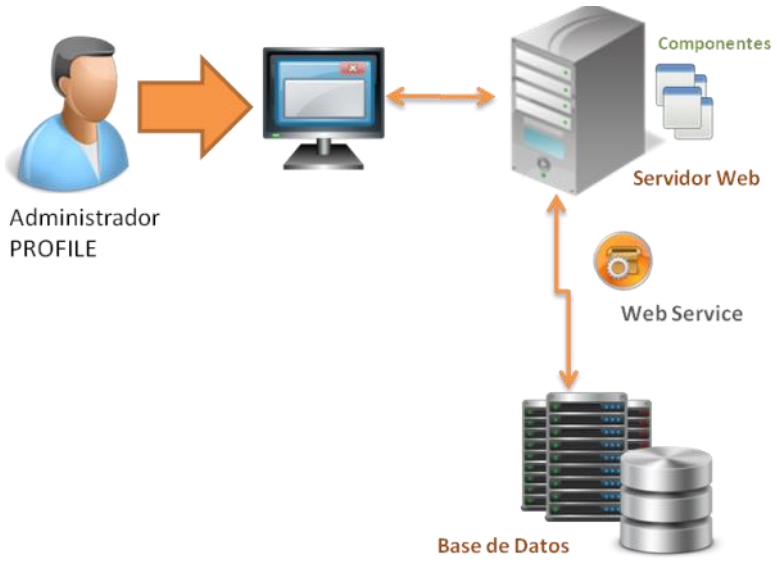
- Se debe configurar el sistema para que permita al usuario realizar su labor, pero no entorpecer la de los otros usuarios, ni robarles información.
- Se debe configurar el sistema para que un usuario no pueda acaparar tantos recursos que provoque una denegación de servicio.

La seguridad no es algo que se pueda alcanzar de manera automática con un producto o una acción. Es un objetivo que se debe tener en mente cuando se realiza cualquier acción.

8. Base de datos de la gestión de la configuración (CMDB)

Una **base de datos de la gestión de configuración** (**CMDB**, por sus siglas en inglés) es una base de datos que contiene detalles relevantes de cada CI (ítem/elemento de configuración) y de la relación entre ellos, incluyendo el equipo físico, software y la relación entre incidencias, problemas, cambios y otros datos del servicio de TI.

La CMDB es un repositorio de información donde se relacionan todos los componentes de un sistema de información, ya sean hardware, software, documentación, etc.



Mantener una Base de Datos de Gestión de Configuración (CMDB) de los activos de nuestra empresa es una tarea tremendamente útil e importante aunque sea algo tediosa y compleja.

Además es necesario realizar tareas periódicas para mantenerla actualizada, realizar auditorías, revisar los cambios, entradas y salidas de material, accesos etc. Existen herramientas específicas que nos ayudarán a llevar un buen mantenimiento de nuestra CMDB.

Es vital mantener una base de datos actualizada y bien gestionada para afrontar cualquier situación tales como valorar accesos al entorno corporativo, encontrar rápidamente un equipo infectado o saber quién tiene acceso a cada recurso en la empresa.

9. Revisión de Contratos / Mantenimientos / Licencias

Contrato es un acuerdo legal manifestado en común entre dos o más personas con capacidad (partes del contrato), que se obligan en virtud del mismo, regulando sus relaciones a una determinada finalidad o cosa, y a cuyo cumplimiento pueden compelerse de manera recíproca, si el contrato es bilateral, o compelerse una parte a la otra, si el contrato es unilateral.

La mayoría de empresas ha de tener contratadas licencias o mantenimientos de sus dispositivos para apoyo técnico o funcionalidades concretas. Es vital revisar periódicamente la fecha de caducidad de los mismos, evitando así quedarnos sin soporte ante un fallo o perdiendo acceso a algún aplicativo concreto por falta de licencia.

No realizar esta revisión puede suponer una perdida en la producción, lo que puede acarrear en una pérdida económica innecesaria.

10. Pruebas de planes de contingencia

Aunque este punto no sea una tarea del todo diaria sí que es un punto que muchas veces pasa desapercibido y, aunque suene lógico y obvio, no siempre se realiza. Hay que realizar “simulacros” en caso de desastre.

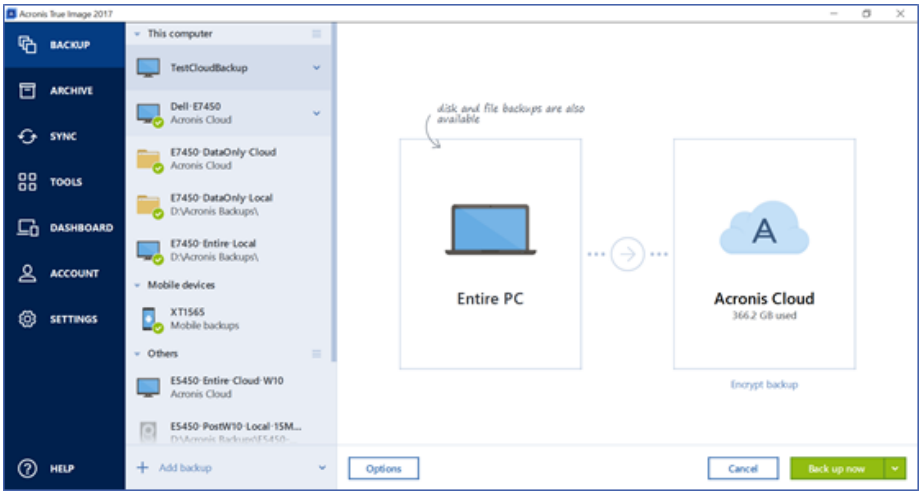
Debemos entre otras cosas, probar a recuperar copias de seguridad, probar los equipos que se encuentren como respaldo, líneas secundarias para contingencia etc.

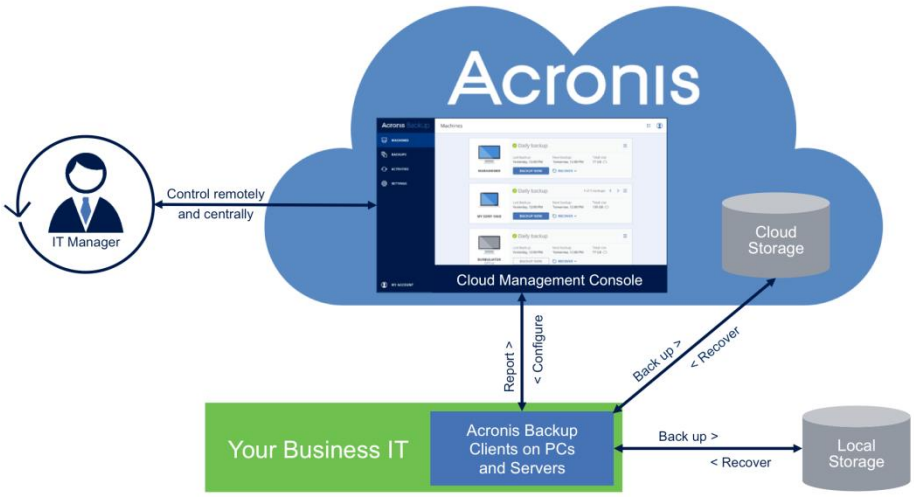
Imaginémonos que llevamos meses haciendo una copia de seguridad de una base de datos y llega un día que se corrompe y la tenemos que recuperar de la última copia de

seguridad. Pero ésta no se ha programado correctamente y no está copiando lo que queríamos.

Con el fin de asegurar el éxito de los planes de contingencia, para ganar experiencia frente a estas situaciones o para medir tiempos de respuesta, es importante realizar pruebas para comprobar que en caso de un incidente grave, vamos a poder volver a la normalidad lo antes posible.

Es importante también poder salvar los datos desde cualquier dispositivo o medio, pudiéndose recuperar desde una nube privada, Storage Local, NAS, etc. Acronis Backup, nos ofrece por ejemplo, soluciones altamente recomendadas para guardar nuestros datos en cualquier entorno, ya sea local, en Nube pública o privada.





11 Referencias consultadas

Para el siguiente manual se han consultado las referencias expuestas a continuación a las cuales agradecemos sus fuentes de contenidos:

WIKIPEDIA: https://es.wikipedia.org

INCIBE (Instituto Nacional de Seguridad) https://www.incibe.es

OSI (Oficina de Seguridad del Internauta) https://www.osi.es/

ACRONIS (Soluciones de Software de Backup) https://www.acronis.com/

AVIRA (Solución antivirus) https://www.avira.com/

HOSTED ANTIVIRUS (Solución Antivirus empresarial) http://www.hostedantivirus.com/

NAGIOS (Software de Monitorización de sistemas) https://www.nagios.org/

NETDATA (Software de Monitorización de Data Center) https://my-netdata.io/

MICROSOFT (Software de Sistema Operativo) https://www.microsoft.com/es-es