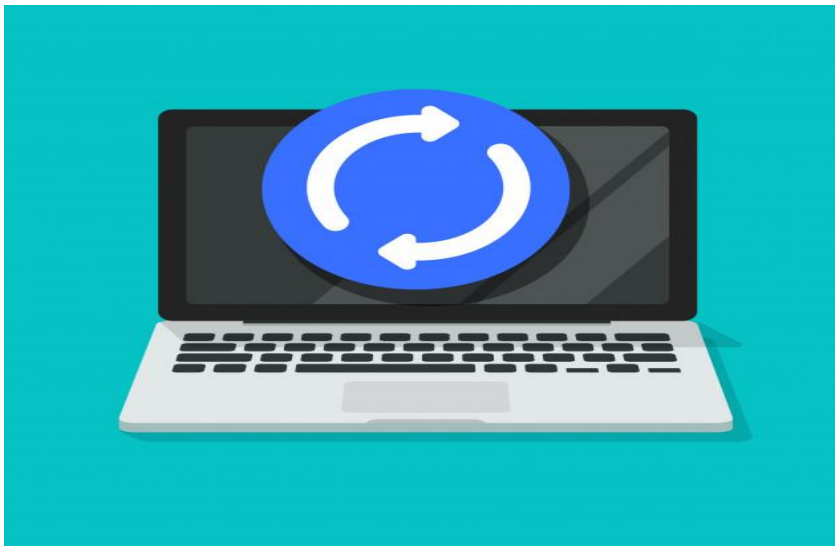
BUENAS PRÁCTICAS EN LA SEGURIDAD INFORMATICA

1. Gestión y control de sistemas antivirus.

Debemos verificar que todos los equipos se encuentren en el sistema de gestión del antivirus, 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.



Debemos revisar que las actualizaciones de la base de datos del servidor, parches de seguridad, vulnerabilidades, etc. se han realizado correctamente. Es importante valorar, que no deja de ser una revisión de que todo se realiza 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.

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.

Gestionar correctamente los incidentes de seguridad que puedan surgir 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 último debemos recuperar los sistemas afectados y documentar lo ocurrido.

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.

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.

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.

8. Gestión de la Configuración (CMDB).

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

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.

Instituto nacional de cibernautica. (2014, Diciembre 3). Buenas prácticas en la seguridad informática. Recuperado 8 de abril de 2020, de https://www.incibe.es/protege-tu-empresa/blog/decalogo-buenas-practicas-seguridad-departamento-informatica