Backup365
online

ANÁLISIS Y GESTIÓN DE RIESGOS

¿Es necesario realizar un Análisis de Riesgos, en sentido estricto? ¿No bastaría con usar la **experiencia de los técnicos de la empresa** para determinar qué medidas son las más oportunas en cada caso?

"La excesiva confianza en las capacidades personales y en la experiencia es, en sí misma, un riesgo.

… evitar que un exceso de confianza nos conduzca a errores, imprecisiones, olvidos, etc., que podrían tener consecuencias desastrosas para nuestros sistemas o servicios."

Fuente: Esquema Nac. De Seguridad – Preguntas frecuentes 8.1

EN UN DÍA NORMAL

EN UN ENTORNO EMPRESARIAL

CADA 24 SEGUNDOS

un equipo accede a un web infectado

CADA 34 SEGUNDOS

se descarga un malware desconocido

CADA 60 SEGUNDOS

un bot se comunica con su centro de control y gestión

CADA 5 MINUTOS

se utiliza una aplicación de alto riesgo

CADA 6 MINUTOS

se descarga un malware conocido

CADA 36 MINUTOS

se envían datos sensibles fuera de la organización

Fuente: CheckPoint

¿ Cómo establecer un Plan de Seguridad ?

Evitar la Fuga de Datos y Asegurar la Continuidad

Backup365 es consciente del actual contexto de crecientes amenazas y por ello nos hemos especializado en proteger la información de nuestros clientes más allá de las soluciones básicas habitualmente empleadas.

Servicios **DLP** (Data Loss Prevention) para evitar la fuga de información sensible. Monitorizar los archivos y flujos de información, para *–entre otras–* verificar si pueden salir del equipo, ser capturados, impresos o almacenados en un dispositivo USB autorizado y cómo.

BACKUP EXTERNALIZADO como servicio *–Archivos, BBDD, Clonación de Sistemas, etc–*. Para cuando todas las medidas preventivas han fallado, garantizar la disponibilidad de una copia de seguridad que permita la continuidad.

Porque invertir en prevención, nunca es un gasto. Y siempre retorna más.

Auto-evaluación básica

Hacemos copias de seguridad cada,

Día: ☐ Semana: ☐ Mes: ☐ Nunca: ☐

En caso de siniestro grave (incendio, borrado, virus…) podemos perder:

Todo: ☐ Mucho: ☐ Poco: ☐ Nada: ☐

En caso de siniestro grave, ¿podemos seguir trabajando con normalidad?:

Sin problema: ☐ A medias: ☐ Sería difícil: ☐ Sería muy difícil: ☐

En caso de siniestro grave, recuperaríamos la operativa en un plazo de:

Inmediato: ☐ Pocos días: ☐ 2 Semanas: ☐ 1 Mes: ☐ Varios meses: ☐

¿Disponemos de equipamiento para hacer las copias de seguridad?:

Sí, automatizado: ☐ Sí, manual: ☐ No: ☐

¿Disponemos de personal y conocimientos para hacer las copias?:

Sí: ☐ No: ☐

¿Revisamos las copias de seguridad con regularidad?:

Siempre: ☐ Ocasionalmente: ☐ Nunca: ☐

¿Trasladamos las copias cifradas y encriptadas a otro edificio?:

Siempre: ☐ Ocasionalmente: ☐ Nunca: ☐

¿Cumplimos con las Normativas?:

LOPD: ☐ LSSI: ☐ Ninguna: ☐

¿Cuánto ocupan los datos importantes en nuestros ordenadores?:

Más de, 1GB: ☐ 10GB: ☐ 50GB: ☐ 100GB: ☐ 500GB: ☐ 1.000GB: ☐

01

¿Por qué un plan de backup?

Informe

- Amenazas y Retos
- Conclusiones y Recomendaciones

¿Por qué debe mi empresa realizar copias de seguridad?

1. Por instinto de **supervivencia**
2. Porque la **Normativa** lo requiere y obliga

Si en mi empresa sucediese "como en el Ayuntamiento de León el 10 de agosto de 2012"… recordar que un incendio **quemó**, **por completo**, las 5 plantas del Ayuntamiento.

Todos los ordenadores se echaron a perder, incluida la sala ignífuga con los servidores. Y **todas las copias de seguridad** "en cintas y discos externos", que estaban allí, **también se perdieron**. Una catástrofe completa. Años después siguen surgiendo reclamaciones sobre documentos y expedientes que saben que, nunca podrán resolver correctamente.

Un Ayuntamiento nunca cesará su actividad, pero una empresa, probablemente, no podrá continuar y cerrará si algo así le sucede.

Si esto le sucediese a mi empresa, o algo más fácil, como… **un robo, una avería, un accidente, o un virus** (de estos que están, tan de moda) que secuestran los archivos y las copias de seguridad. Y después piden un rescate.

¿Disponemos de copias de seguridad?

¿Están actualizadas, a qué fecha?

¿Están, a cubierto, en otro edificio?

La **LOPD** establece en su **Reglamento** (Art.94) la **obligación**: "…se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción."

Además, **obliga en su Reglamento (Art.102) a las empresas** con datos de Nivel Alto, **a realizar copia diaria** de esos datos y **trasladarlos cifrados** y encriptados a otro lugar físico diferente, **a otro edificio**.

Informe – Amenazas y Retos en el Entorno Actual

Hasta hace muy poco tiempo la seguridad de la información podía verse comprometida por averías en los equipos, accidentes, sabotajes intencionados y virus. No era poco, pero entre algunas medidas de seguridad, copias más o menos actualizadas, buena voluntad y la confianza en el "a mi es poco probable que me pase…" los usuarios y administradores de TI han ido sobreviviendo.

Pero las amenazas no se quedaron ahí: el incesante incremento de tecnologías, la movilidad, la virtualización y otros factores han modificado para siempre la forma en que trabajamos. Frecuentemente todos estos cambios no han tenido en cuenta las implicaciones de seguridad.

Entre la frecuencia de las brechas de seguridad descubiertas y los perfiles de las empresas atacadas, el año 2015 dejó un mensaje muy claro: **Todo el mundo está en riesgo**.

Un estudio entre grandes corporaciones en 2015 reveló que:

- El **86%** de la organizaciones accedieron a sitios infectados
- El **83%** de la organizaciones tenían equipos infectados por bots
- Un **42%** tuvieron incidentes provenientes de sus dispositivos móviles
- El **96%** de la organizaciones usan aplicaciones de alto-riesgo
- Las pérdidas de información se han incrementado un **71%** en 3 años
- El malware nuevo ha crecido por encima del **70%** entre 2013 y 2015

Fuente: CheckPoint

Si pensamos en las empresas más pequeñas -carentes de los medios e infraestructuras de las grandes corporaciones- la conclusión es que el 99% de las PYMEs están afectadas por problemas de seguridad y presentan infecciones de diversa clase. **Sus datos y sus equipos están comprometidos.**

Riesgos por Factor/Error Humano

Generalmente lo encontramos al principio, en el intermedio o al final de la catástrofe, y no será raro hallarlo en todos los sitios a la vez.

Riesgos por Fallos hardware

Todas las máquinas son susceptibles de avería en alguno de sus componentes esenciales. Algunos son fácilmente reemplazables -si contamos con un servicio de mantenimiento adecuado- o simplemente no ponen en riesgo los datos que contienen. En otros casos -como los discos duros o sus controladoras- una avería puede ocasionar la perdida completa de la información relevante.

Riesgos por Vulnerabilidades Software

Actualmente suponen el principal reto al que se enfrenta cualquier dispositivo conectado a una red. La colosal cantidad de amenazas, su nivel de complejidad creciente y la cantidad de sistemas ya afectados hacen pensar que nadie está a salvo. Que no es un problema de "*y si me pasara a mí*", realmente se ha convertido en "***cuándo me va a pasar a mi***".

Sus protagonistas son:

- El malware conocido, una peligrosa evidencia
- El malware desconocido, creciendo sin horizonte final
- Los dispositivos móviles, el sospechoso invitado BYOD
- Las aplicaciones cloud, un filón de riesgos en la nube
- El trasiego de datos, agua entre los dedos

Conclusiones y Recomendaciones

Es evidente que el cibercrimen NO está en retroceso. Es más, a la vista de los datos y hechos ya conocidos sobre los años 2014 y 2015 con seguridad veremos futuros crecimientos en múltiplos de diez.

Las amenazas provienen de cualquier lugar y es imposible asegurar que nadie ni ninguna organización se encuentren a salvo de un ataque. De hecho el peor error que nadie pueda cometer será pensar que se encuentra a salvo y deje de asignar recursos a mejorar y revisar su seguridad de modo continuado.

Cuando piense en su posición sobre los capítulos de seguridad, tome el tiempo necesario para comprender las amenazas y las vulnerabilidades. El directivo mejor preparado sabe que las políticas de seguridad precisan de planes estratégicos, objetivos empresariales y políticas corporativas. Además de controlar los procedimientos, requerimientos y resultados en todo los niveles de la organización.

Dibuje su propio proceso y asegúrese de incluir desde los procesos más básicos de parches y actualizaciones, hasta las relaciones con terceros y cómo se interrelacionan con sus procesos de seguridad.

02

Backup365

Soluciones específicas:

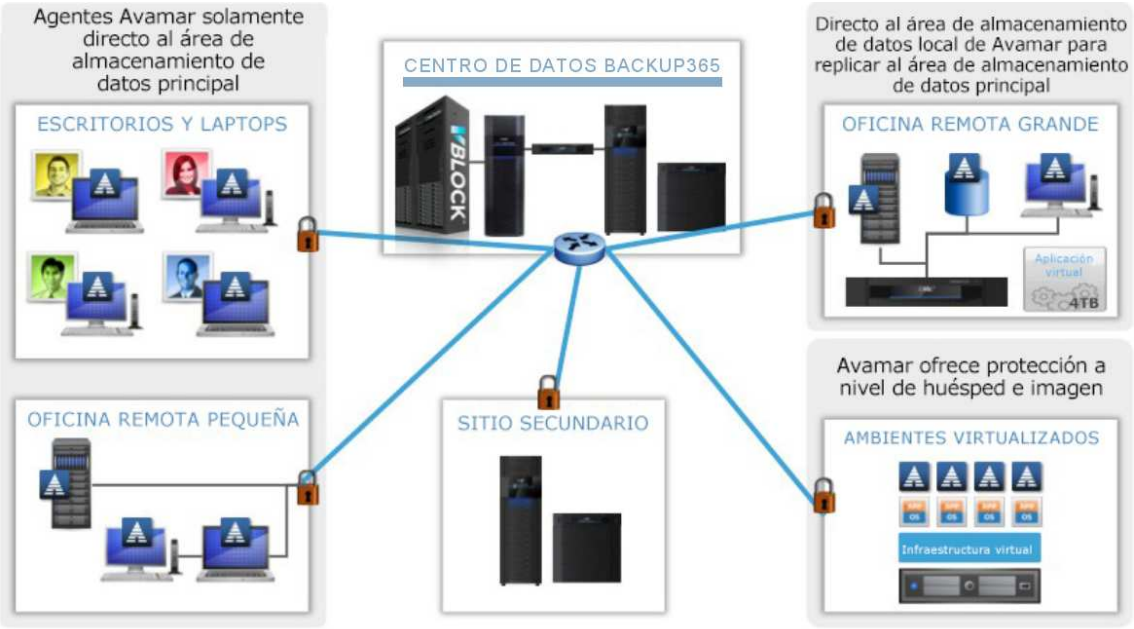
*** Backup OnLine**

*** Clonación de Sistemas para su Externalización Diaria**

*** DLP – Prevención de Perdida de Datos y Control de Usos**

Backup OnLine

Garantizar la existencia y disponibilidad de una copia externalizada que asegure los datos de cualquier sistema en cualquier lugar. Basándonos en la tecnología EMC Avamar, la solución de backup para entornos Enterprise más potente del mercado, ofrecemos su empleo bajo un modelo de pago por uso a cualquier Gran Empresa, PYME o usuario individual**. Sin costes de adquisición, implantación o licencias, sólo se paga por el volumen de datos acumulados mensualmente por la organización**.



Las empresas están redefiniendo el respaldo y la recuperación como resultado del aumento exponencial de la cantidad de datos, el cumplimiento de normas, los SLA en aumento y la reducción de las ventanas de respaldo. El equipo de TI enfrenta retos adicionales generados por la virtualización, la infraestructura y la necesidad de proteger mejor los datos en toda la empresa, incluidas las oficinas remotas. A diferencia de las soluciones de respaldo tradicionales, Avamar elimina segmentos de datos redundantes de subarchivos en el cliente antes de que los datos de respaldo se transfieran al servidor de copias. Como resultado, el ancho de banda requerido para el respaldo se reduce en hasta un 99 %, permitiendo realizar respaldos diarios, rápidos y completos por medio de la infraestructura WAN/LAN IP existente. Avamar deduplica los datos de respaldo de manera global, en sitios y servidores, reduciendo en hasta un 95% el espacio total de respaldo necesario. Los datos de respaldo se cifran cuando están en transferencia y en reposo, lo que garantiza que la retención en disco sea rentable y segura.

Clonación de Sistemas para su Externalización Diaria

Cuando la preferencia no es realizar copias a nivel de archivos o BBDD, y se busca una solución total que permita la clonación diaria y la puesta a salvo en el exterior de sistemas completos. Con un precio asumible y **como un servicio en pago por uso mensual**, sin costes de implantación.

Para hacer copias de seguridad, recuperar y migrar sus sistemas Windows y Linux tanto virtuales como físicos de manera rápida y fiable con una solución que le permite hacerse cargo de sus copias de seguridad (in situ, externamente y en la nube) ayudándole a organizar y administrar sus archivos de imágenes de copia de seguridad.

- Proteja servidores Windows y Linux tanto virtuales como físicos, así como ordenadores de sobremesa y portátiles Windows desde una misma interfaz de usuario.
- Arranque al instante imágenes de copia de seguridad como máquinas virtuales con la tecnología VirtualBoot.
- Vea y administre las imágenes de copia de seguridad desde el calendario de tareas patentado.
- Personalice la programación de copias de seguridad Continuas, Mixtas, Completas y Manuales.
- Compatible con más de 10 plataformas de hipervisor.
- Replicación completa basada en LAN y en WAN.
- Disfrute de la replicación local acelerada en su nube privada.
- Realice recuperaciones parciales o completas en minutos.

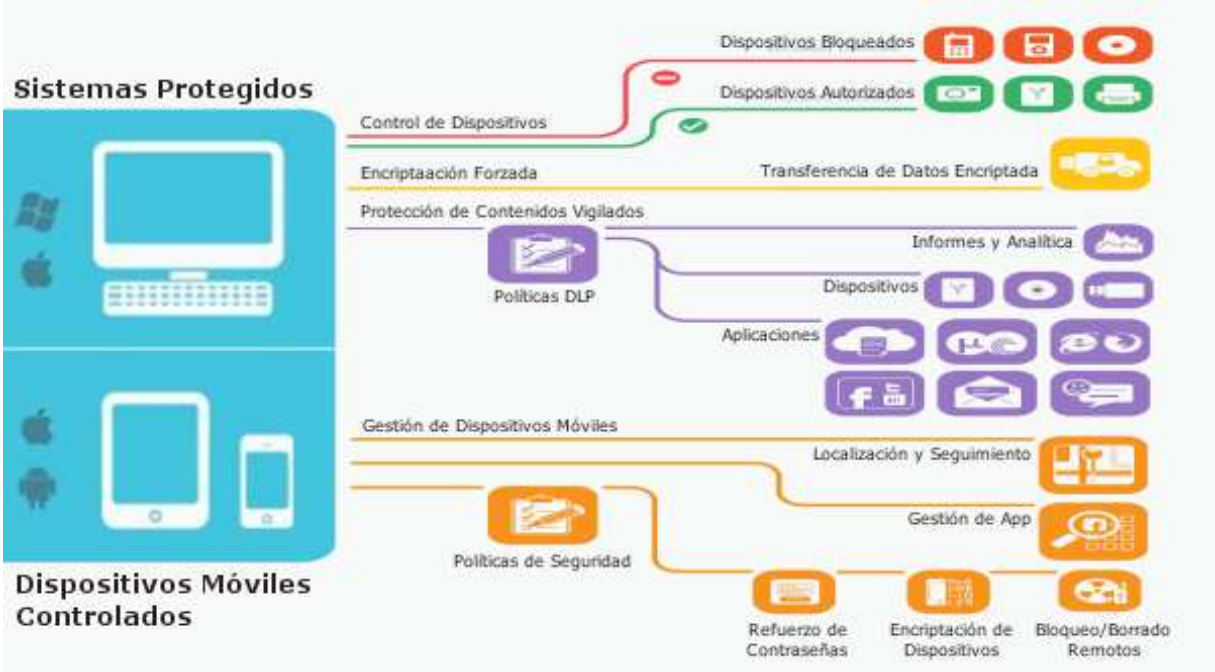
DLP – Prevención de Perdida de Datos y Control de Usos

Solución Data Loss Prevention, Control de Sistemas de Usuario y Gestión de Dispositivos Móviles iOS & Android para PYMES y grandes cuentas.

Para proteger los datos contra amenazas de los dispositivos, gestionar la Prevención de Pérdida de Datos y MDM.

En un mundo donde los dispositivos portátiles y la nube transforman la manera en que vivimos y trabajamos, este servicio está diseñado para proteger la información, mantener la productividad y hacer el trabajo más cómodo, seguro y agradable.

Disponible como servicio en pago por uso, y también en formato de appliance virtual o hardware, puede ser instalado en unos minutos.



La Claves

- El servicio, el hardware o la MV implementados en unos minutos
- Solución 3 en 1, Control de Dispositivos, DLP y MDM
- Interfaz de control basada en web
- Protección para Windows, Mac, Linux, iOS y Android
- Protección proactiva contra el abuso de dispositivos y datos
- TCO un 50% más bajo que la media del mercado
- Implementación, 70% menos tiempo comparada a otras soluciones
- Costes 45% inferiores contra soluciones similares

Seguridad de estaciones de trabajo, portátiles y Netbooks con Windows/Mac OS X y Linux

Protección contra amenazas planteadas por dispositivos portátiles extraíbles. Detiene la divulgación no autorizada de datos, el robo, la pérdida, o la infección con malware intencionados o imprevistos.

Controle Dispositivos, Aplicaciones y muchas otras actividades

Dispositivos USB, Clientes e-Mail, Navegadores Web, Mensajería Instantánea (Skype, ICQ,…), Servicios en Nube (Dropbox, GoogleDocs, SkyDrive, Torrent,…), Aplicaciones (TeamViewer, FileZilla,…)

Gestión centralizada basada en Web / Panel de control

Gestiona de forma centralizada el uso de dispositivos portátiles extraíbles y la transferencia de datos confidenciales a través de aplicaciones online en tiempo real.

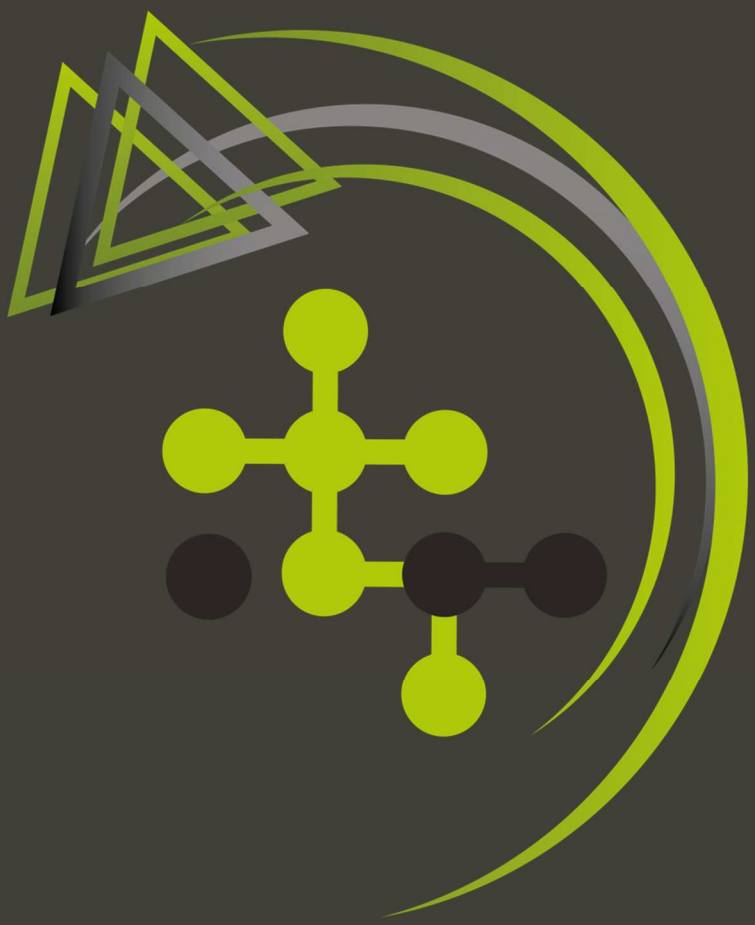
Mobile Device Management (MDM) para OSX, iOS y Android

Imponer Política de Contraseña y Seguridad; Localizar Dispositivos / Bloquear / Borrar Dispositivos; Desplegar ajustes E-mail, VPN, WiFi (dispositivos iOS); Geofencing, políticas a base de un perímetro seguro; Solución BYOD.

Gestión de dispositivos / Control de dispositivos
Content Aware Protection / Filtrado de contenido
Filtrado por Extensión / Contenido / Expresiones Regulares
Listas blancas de archivos/ Dispositivos / URLs / Dominios
Informes y Análisis / Panel de control y gráficos / Auditoría
Cumplimiento de las Políticas de Seguridad (Active Directory)
Desbloqueo Temporal de Contraseña / Modo de red “offline”
Gestión por departamentos
Autodefensa del Cliente
Encriptación forzada de datos en tránsito
Desactivar imprimir pantalla
Etc., etc…

“ Los fallos son parte de la vida. Es la capacidad de respuesta ante el error lo que cuenta ”

Cada año, cada día, cada minuto aparecen amenazas nuevas, más sofisticadas cada vez. Las estrategias habituales ya no sirven. La pregunta “¿Y si me pasara…? ya no es opcional, ahora es: ¿Cuándo me pasará …?



Teléfono gratuito: 900 831 135

https://www.backup365.es

clientes@backup365.es

Backup365 online