FORMULARIO COMERCIAL
DE SOLICITUD DE INFORMACIÓN

LAB TOP SISTEMAS S.L.

ESPECIALISTAS EN CIBERSEGURIDAD

www.LABTOPSISTEMAS.COM

REVISADO
Por Lab Top SISTEMAS fecha 13:22 , 11/04/2018

Lab Top Sistemas
Especialistas en Ciberseguridad
info@labtopsistemas.com
www.labtopsistemas.com

Datos de la empresa

Razón Social:

Nombre Comercial:

C.I.F./N.I.F.:

Dirección:

C.P.:

Localidad:

Provincia:

Teléfono:

Email:

Actividad:

Observaciones:

Datos de la persona de contacto

Nombre:

Apellidos:

Cargo:

Telf. Contacto:

Email Contacto:

Ad. Juan Carlos I, 55. Edificio JC1, 9 planta CIF B73898108 C.P 30100. Murcia. 688310801

Lab Top Sistemas

Especialistas en Ciberseguridad

info@labtopsistemas.com

www.labtopsistemas.com

Información solicitada

1- ¿Dispone de red wifi o inalámbrica?

Si ○ No ○ No sabe ◉

2- ¿Dispone de un servidor de autentificación (Controlador de dominio)?

Si ○ No ○ No sabe ◉

3- ¿Realizan copias de seguridad externas?

Si ○ No ○ No sabe ◉

4- ¿Existe un firewall y un proxy de salida?

Si ○ No ○ No sabe ◉

5- ¿Qué tiempo de respuesta cree que existe ante un fallo del servidor en volver a estar activo?

6- ¿Usan métodos de encriptación en sus comunicaciones?

Si ○ No ○ No sabe ◉

7- ¿Cuántos caracteres mínimos son aceptables en sus contraseñas?

8- ¿Disponen de bases de datos de clientes?

Si ○ No ○ No sabe ◉

9- ¿Disponen de certificados digitales?

Si ○ No ○ No sabe ◉

10- ¿Pueden ver que empleado se conecta y cuando a cada recurso de red?

Si ○ No ○ No sabe ◉

11- ¿Los empleados pueden instalar aplicaciones en sus equipos?

Si ○ No ○ No sabe ◉

12- Cuando encienden un equipo, ¿salta una pantalla informativa en base a las exigencias de la LOPD?

Si ○ No ○ No sabe ◉

13- ¿Disponen de un plan de contingencia?

Si ○ No ○ No sabe ◉

14- ¿Existe algún gestor de incidencias donde se cataloguen y recopilen las incidencias técnicas?

Si ○ No ○ No sabe ◉

15- ¿Disponen de procedimiento por escrito ante bajas y despidos laborales?

Si ○ No ○ No sabe ◉

16- ¿Disponen de un control de inventario actualizado?

Si ○ No ○ No sabe ◉

17- ¿Existe un manual de buenas prácticas para los empleados?

Si ○ No ○ No sabe ◉

18- ¿Se destruyen correctamente los pendrive, disco duro u otro soporte digital cuando se averían?

Si ○ No ○ No sabe ◉

19- ¿Los servidores físicos de datos, son accesibles para cualquier empleado?

Si ○ No ○ No sabe ◉

20- ¿Disponen de la suficiente seguridad física para evitar el robo de la información empresarial?

Si ○ No ○ No sabe ◉

Notas. Indique aquí todos aquellos datos que considere de interés para Lab Top

Observaciones:

Centros de trabajo

Si dispone de diferentes centros de trabajo, a parte de la sede principal, indique cuantas:

Nº Total de Centros de Trabajo:

Nº de Centros de Trabajo sobre las que desea solicitar nuestros servicios

NOTA: En caso de disponer de varias delegaciones y si desea ofrecer nuestros servicios sobre ellas, debe adjuntar este formulario con los datos correspondientes a cada una de ellas especificando la parte correspondiente a la sección Datos para Lab Top de este formulario.
NOTA II: Una vez completado el formulario, rogamos nos lo envíe por correo electrónico a la dirección info@labtopsistemas.com

En las 20 preguntas anteriores se preguntan por el estado de los 20 puntos básicos de la seguridad de la información que deben cumplirse para asegurar un nivel de seguridad básico en los datos de los clientes y para el correcto funcionamiento de una red empresarial.

Estos son sólo 20 puntos que no requieren de un alto conocimiento técnico, pero existen muchos otros de igual o mayor gravedad que deben ser auditados y corregidos.

Incumplir un solo punto de los siguientes genera una vulnerabilidad grave que debe ser corregida lo antes posibles con todos los medios disponibles por la compañía auditada.

A continuacion se da una breve explicacion de cada punto.

1- ¿Dispone de red wifi o inalámbrica?
Las redes Wifi son la mayor vulnerabilidad existente en una red empresarial de cara a atacantes externos. Estas redes son fáciles de hackear y una vez logrado se puede interceptar absolutamente todo el tráfico de la red, incluyendo contraseñas.

2- ¿Dispone de un servidor de autentificación (Controlador de dominio)?
No disponer de este tipo de autentificación de encriptado permite que cualquier persona pueda extraer la información de los discos de forma rápida y sencilla.

3- ¿Realizan copias de seguridad externas?
Dependiendo de la importancia y capacidad de la información empresarial, las copias de seguridad deben almacenarse encriptadas y de forma externa para solventar obstáculos naturales o provocados.

4- ¿Existe un firewall y un proxy de salida?
La salida de internet de toda la red informática empresarial debe estar controlada y securizada por un único punto de salida.

5- ¿Qué tiempo de respuesta cree que existe ante un fallo del servidor en volver a estar activo?
La disponibilidad de los servicios empresariales muestra la imagen de una empresa ante sus clientes o posibles clientes. El tiempo que los servicios están parados suponen un duro golpe a la imagen corporativa, además de pérdida de negocio y un estancamiento de la plantilla personal.

6- ¿Usan métodos de encriptación en sus comunicaciones?
Las comunicaciones, tanto internas, como externas, son fácilmente interceptadas, tanto por atacantes externos, como por desempleados descontentos.

7- ¿Cuántos caracteres mínimos son aceptables en sus contraseñas?
Los ataques en internet más usados son los llamados de fuerza bruta. Para evitar estos ataques las contraseñas deben disponer de un mínimo de caracteres, generando lo que se llama un doble HASH para considerarse realmente seguras.

8- ¿Disponen de bases de datos de clientes?
Las bases de datos de clientes, en especial las que contienen datos de carácter personal, son el principal objetivo de los hackers. Una vez obtenida esta información, los hackers realizan chantajes a las empresas a cambio de no publicarlas, lo que causaría fuertes sanciones económicas a la empresa, haciendo que incluso caiga en quiebra.

9- ¿Disponen de certificados digitales?
Los certificados digitales son de gran importancia, tanto a nivel de seguridad, como para demostrar una identidad, evitando así el falseamiento de las comunicaciones.

10- ¿Pueden ver que empleado se conecta y cuando a cada recurso de red?
Los sistemas auditores deben estar siempre activos de cara a depurar responsabilidades y disponer de un control de la información y recursos críticos de nuestra red.

11- ¿Los empleados pueden instalar aplicaciones en sus equipos?
Un empleado con permisos de instalación, es un empleado con permisos de ejecución de virus capaces de destruir toda la información empresarial.

12- Cuando encienden un equipo, ¿salta una pantalla informativa en base a las exigencias de la LOPD?
Los empleados deben ser conscientes de sus derechos y deberes de cara a depurar responsabilidades. Estos deben estar informados con las exigencias de las leyes vigentes.

13- ¿Disponen de un plan de contingencia?
Toda empresa debe disponer de un plan de contingencias bien definido. Ante un incendio, inundación o cualquier catástrofe, la empresa debe ser capaz de recuperar un alto nivel de operación de la forma más rápida posible.

14- ¿Existe algún gestor de incidencias donde se cataloguen y recopilen las incidencias técnicas?
Los gestores de incidencias son importantes para ver el origen y repetición de incidencias técnicas a la hora de solventar las incidencias reiteradas.

15- ¿Disponen de procedimiento por escrito ante bajas y despidos laborales?
Un alto % de los problemas de seguridad vienen del personal interno, ya sea por desconocimiento o de forma intencionada. Este procedimiento permite evitar, tanto incidencias, como robo de información por el personal descontento tras su despido.

16- ¿Disponen de un control de inventario actualizado?
Debe existir un inventario lo más completo y actualizado posible de todo el material de la red empresarial, tanto para el control, como para actuar ante robos. Uno de los puntos más importantes son las direcciones MAC de los equipos informáticos.

17- ¿Existe un manual de buenas prácticas para los empleados?
Un alto % de los problemas de seguridad vienen del personal interno, ya sea por desconocimiento o de forma intencionada. Este manual permite evitar incidencias por descuidos y desconocimiento de los empleados. Una red no es segura si su personal no está correctamente formado.

18- ¿Se destruyen correctamente los pendrive, disco duro u otro soporte digital cuando se averían?
Formatear los dispositivos ópticos no es suficiente para eliminar su contenido. Un disco duro por ejemplo, necesita ser formateado 32 veces para borrar totalmente su contenido.

19- ¿Los servidores físicos de datos, son accesibles para cualquier empleado?
Sólo el personal autorizado debe disponer de acceso físico a los servidores. Un simple puerto USB abierto en el servidor, es suficiente como para sacar su información en escasos minutos, incluso para borrar su contenido.

20- ¿Disponen de la suficiente seguridad física para evitar el robo de la información empresarial?
De nada sirve asegurar la información de forma lógica, si no disponemos de la seguridad física que nos permita asegurar los soportes físicos donde se encuentra esa información.