CHECKLIST DE CIBERSEGURIDAD PARA EMPRESAS

42 medidas que te ayudarán a mejorar la seguridad de los sistemas de información

KIPPEO
GET STARTED IN HOLISTIC SECURITY

CHECKLIST DE CIBERSEGURIDAD PARA EMPRESAS

Hoy las empresas están expuestas a nuevas amenazas que pueden afectar su normal funcionamiento como consecuencia de ataques o incidentes de ciberseguridad.

Algunas de las más comúnes son el robo de información, suplantación de identidad, la infección con virus o malware o la pérdida de información de sus clientes o proveedores.

50% de los profesionales no creen que su empresa esté preparada para repeler un ciberataque.

El Checklist básico de Ciberseguridad para Empresas es una herramienta que permite realizar una evaluación de su nivel de ciberseguridad.

Este documento contiene 42 sencillas medidas para mejorar el nivel de seguridad de tu empresa en poco tiempo.

Te recomendamos utilizar este checklist como base para mejorar o bien detectar si se requiere la asistencia de un profesional para definir un plan de acción.

¡A comenzar!

I SENSIBILIZANDO

- [ ] 1. Capacitar al personal operativo sobre la seguridad en los sistemas de información.
- [ ] 2. Sensibilizar a los usuarios sobre buenas prácticas básicas de seguridad informática.
- [ ] 3. Control de riesgos sobre las maneras de compartir información.

II CONOCIENDO EL SISTEMA DE INFORMACIÓN

- [ ] 4. Identificar la información y servidores más sensibles y tener actualizado un diagrama de red.
- [ ] 5. Tener un inventario de todas las cuentas, usuarios y permisos, siempre actualizado.
- [ ] 6. Desarrollar los procedimientos de llegada, de salida y cambio de funciones de usuario.
- [ ] 7. Permitir la conexión a la red de la empresa sólo a equipos controlados.

III AUTENTIFICANDO LOS ACCESOS

- [ ] 8. Identificar por nombre cada persona que acceda a la red y distinguir roles de usuario/administrador.
- [ ] 9. Asignar derechos correctos sobre la información sensible del sistema de información.
- [ ] 10. Proteger contraseñas almacenadas en los sistemas.
- [ ] 11. Cambiar los elementos de autenticación por default sobre equipos y servicios.
- [ ] 12. Definir y verificar reglas para elegir y dimensionar contraseñas.
- [ ] 13. Cada vez que sea posible, privilegiar sistemas de autenticación fuerte.

IV ESTACIONES DE TRABAJO SEGURAS

- [ ] 14. Establecer un nivel de seguridad mínimo en general para los equipos informáticos.
- [ ] 15. Cómo protegerse de las amenazas en medios extraíbles (memorias, USB)
- [ ] 16. Habilitar y configurar el firewall de las estaciones de trabajo.
- [ ] 17. Cifrar datos confidenciales transmitidos por Internet.
- [ ] 18. Usar una herramienta de administración centralizada para estandarizar las políticas de seguridad.

V ASEGURANDO LA RED

- [ ] 19. Segmentar las redes por departamentos.
- [ ] 20. Garantizar la seguridad de las redes de acceso Wi-Fi.
- [ ] 21. Configurar una puerta de acceso seguro a Internet.
- [ ] 22. Proteger el servicio de correo electrónico profesional.
- [ ] 23. Controlar y proteger el acceso a la sala de servidores.
- [ ] 24. Use protocolos de red seguros tan pronto como estén disponibles.
- [ ] 25. Segregar servicios visibles desde Internet del resto del sistema de información.
- [ ] 26. Proteger las interconexiones de red dedicadas con contratistas y proveedores de servicios.

VI ADMINISTRACIÓN SEGURA

- [ ] 27. Prohibir el acceso a Internet desde las estaciones de trabajo o servidores utilizados para la administración del sistema de información.
- [ ] 28. Utilizar una red dedicada y separada para la administración del sistema de información.
- [ ] 29. Limitar a la necesidad estricta los permisos de administrador en las estaciones de trabajo.
- [ ] 30. Tomar medidas para proteger físicamente los equipos portátiles

VII SEGURIDAD PARA EQUIPOS PORTÁTILES

- [ ] 31. Cifrar datos confidenciales, especialmente en los equipos vulnerables al robo.
- [ ] 32. Asegurar la conexión red de estaciones de trabajo utilizadas en situación nómada.
- [ ] 33. Adoptar políticas dedicadas a la seguridad de dispositivos portátiles.
- [ ] 34. Tomar medidas para proteger físicamente los equipos portátiles

VIII MANTENER ACTUALIZADO EL SISTEMA DE INFORMACIÓN

- [ ] 35. Definir una política de actualización de componentes del sistema de información.
- [ ] 36. Anticipar la obsolescencia de software y sistemas.

IX SUPERVISAR, AUDITAR Y REACCIONAR

- [ ] 37. Definir y aplicar una política de copias de seguridad para componentes críticos.
- [ ] 38. Realizar controles y auditorías de seguridad periódicos y luego aplicar acciones correctivas asociadas.
- [ ] 39. Designar un responsable de seguridad del sistema de la información y darlo a conocer al personal.
- [ ] 40. Definir un procedimiento de gestión de incidentes de ciberseguridad.
- [ ] 41. Habilitar y configurar los registros de los componentes más importantes.
- [ ] 42. Definir y aplicar una política de respaldo de componentes críticos.

KIPPEO
GET STARTED IN HOLISTIC SECURITY

INÍCIESE EN LA SEGURIDAD HOLÍSTICA

Tenemos todas las soluciones en ciberseguridad holística que necesita para **mantener su organización segura** de las amenazas de seguridad más peligrosas.

¿Cómo lo hacemos?

Elegimos las mejores soluciones de seguridad con base en sus necesidades para ofrecerle la respuesta más eficaz para combatir sus ciberamenazas específicas.

Una vez que se ha diseñado el modelo que cumpla con sus requerimientos, le enseñamos las reglas del juego cibernético y nos aseguramos de que usted pueda jugar mejor que nadie más.

Nuestras soluciones de prevención, detección y rehabilitación establecen prácticas de seguridad altamente resilientes para combatir las ciberamenazas, siempre cambiantes.

Equiparemos su organización con todo lo necesario para determinar lo que es realmente importante. Motivaremos a su personal en todos los niveles para que hagan algo por la ciberseguridad.

¡Estamos aquí para ayudarle!

SOLICITAR COTIZACIÓN