

**LISTA DE VERIFICACIÓN #21**

**EVALUACIÓN DE AMENAZA CONTRA LA SEGURIDAD CIBERNÉTICA**

<b>LISTA DE VERIFICACIÓN DE SEGURIDAD</b>	<b>Si</b>	<b>No</b>
<b>SEGURIDAD DE LA PLANTA FÍSICA</b>		
1. ¿Están el área y equipo de computación físicamente seguros?		
2. ¿Hay procedimientos en pie para evitar que los terminales se dejen abiertos ni aún brevemente?		
3. ¿Se apagan las pantallas monitoras cuando no sean usadas por 10 minutos?		
4. ¿Están los módems designados a no aceptar llamadas (Auto-Answer OFF)?		
5. ¿Están su computadoras personales (PC) inaccesibles a personas no autorizadas (por ejemplo, alejadas de áreas publicas)?		
6. ¿Usan insignias identificativas sus empleados?		
7. ¿Corroboran los credenciales de contratistas independientes?		
8. ¿Hay procedimientos para proteger información mientras reparan el equipo?		
9. ¿Se trituran los papeles de importancia antes de botarlos?		
10. ¿Hay procedimientos para botar los residuos?		
11. ¿Cuando se deshacen de equipo de computadoras, hay forma de proteger contra pérdida de datos (por ejemplo, copiando los discos viejos y las unidades de discos)?		
12. ¿Tienen procedimientos para proteger la seguridad de las computadoras portátiles (laptops), por ejemplo, cierre del cable o almacenamiento seguro?		
<b>ADMINISTRACIÓN DE LA CUENTA Y CONTRASEÑA</b>		
13. ¿Hay seguridad que sólo el personal autorizado tenga acceso a las computadoras?		
14. ¿Se requiere tener y usar las contraseñas apropiadas?		
15. ¿Están seguras sus contraseñas (dificiles de adivinar, cambiadas regularmente, sin usar conraseñas temporeras o por defecto)?		
16. ¿Están sus computadoras localizadas en sitios donde nadie pueda ver a empleados entrando sus contraseñas?		
<b>DATOS CONFIDENCIALES Y DELICADOS</b>		
17. ¿Está usted ejerciendo su responsabilidad para proteger los datos de asuntos delicados bajo su supervisión?		
18. ¿Están sus datos más valuales y delicados codificados?		
<b>RECUPERACIÓN ANTE DESASTRES</b>		
19. ¿Tiene un plan de continuidad para empresas corrientes?		
<b>CONCIENCIA Y EDUCACIÓN SOBRE SEGURIDAD</b>		
20. ¿Se le está proveyendo información sobre la seguridad de la computación a los empleados?		
21. ¿Están los empleados adiestrados a estar alerta a posibles violaciones de seguridad?		