Lista de verificación para una auditoría a la seguridad informática

Seguridad en los sistemas computacionales y dispositivos periféricos.

Seguridad en la información institucional y bases de datos.

Seguridad en los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional.

Seguridad en los activos informáticos del área de sistemas.

Seguridad para el personal informático y los usuarios del sistema.

Seguridad en la protección y conservación de locales, instalaciones, mobiliario y equipos.

Seguridad en los accesos a las áreas de sistemas, así como a sus sistemas computacionales, información y software.

Seguridad en la arquitectura de las telecomunicaciones.

Seguridad en los sistemas de redes, sistemas mayores y PCs.

Seguridad contra la piratería informática.

Seguridad contra los virus informáticos.

- Auditoría de la seguridad en las condiciones e instalaciones físicas del área de sistemas
- Protección contra los riesgos y contingencias de origen natural relacionados con el ambiente de trabajo.
  - Las condiciones generales de trabajo de los sistemas computacionales, para el bienestar y comodidad de los empleados y usuarios del sistema.
  - Protección contra la humedad del ambiente.
  - Medidas para prevenir que los sistemas computacionales y las instalaciones eléctricas, telefónicas y de datos tengan contacto con el agua.
  - Protección contra las partículas de polvo y deshechos volátiles de cualquier tipo en el ambiente, a fin de evitar desperfectos en los sistemas computacionales y medios de almacenamiento, así como el deterioro de los activos informáticos del área de sistemas.
  - Protección contra la estática e imantación producidas por fibras sintéticas, metales, algunos plásticos y por el cabello humano y animal que pueden repercutir en el funcionamiento de los sistemas computacionales de la empresa.
  - Análisis de los sistemas de acondicionamiento y pisos falsos.
  - Análisis de la regulación de temperatura y aire acondicionado.
  - Análisis de los suministros de energía, comunicaciones y procesamiento de datos.
  - Análisis de la limpieza del área de sistemas.

- Protección contra riesgos y contingencias relacionados con el ambiente de trabajo en las áreas de sistemas de la empresa.
  - La iluminación artificial del área de sistemas y la iluminación por medio de luz solar.
  - Las instalaciones eléctricas, de datos y de comunicación.
  - Los accesos y salidas en las áreas de sistemas.
  - La repercusión de los aspectos de carácter ergonómico.
  - Las adaptaciones de los equipos de cómputo.
  - Las condiciones de trabajo con computadora.
  - Protección contra contingencias causadas por la temperatura del sistema de aire acondicionado.
  - La ventilación natural de las áreas y espacios.
- Protección contra riesgos y contingencias causados por factores meteorológicos, atmosféricos y desastres naturales incontrolables.
  - Por precipitación pluvial, de nieve, de granizo y otras precipitaciones.
  - Por vientos, huracanes, ciclones y fenómenos atmosféricos.
  - Por terremotos y temblores.
  - Por inundaciones, marejadas, maremotos y fenómenos marítimos.
  - Por tormentas eléctricas.
  - Por incendios accidentales.
  - Otros fenómenos de origen natural que afectan a las áreas de sistemas y a los propios sistemas computacionales.
- Protección contra riesgos y contingencias derivados del suministro de la energía eléctrica.
  - Prevención de interrupciones y falta permanente del suministro de energía eléctrica para el funcionamiento de los sistemas computacionales.
  - Continuidad del suministro de la energía eléctrica, por medio de la red pública o plantas de emergencia, fuentes ininterrumpidas de poder y no-breaks.
  - Previsión en la funcionalidad, distribución adecuada y seguridad de las instalaciones eléctricas del área de sistemas.
  - Prevención de fallas y deficiencias de la red pública de suministro de electricidad.
  - Protección contra las variaciones de voltaje, así como el uso de reguladores de corriente, contactos supresores de picos y sistemas de no-breaks.
  - El análisis del cableado público de las instalaciones eléctricas que están fuera de la empresa.
  - El análisis del cableado, construcciones y adaptaciones eléctricas, contactos, tierra física y demás instalaciones eléctricas internas del área de sistemas.
- Protección y seguridad de los espacios físicos de las instalaciones de cómputo.

- En los sistemas de vigilancia de las áreas de sistemas.
- En los accesos a las instalaciones de las áreas de cómputo.
- En las áreas restringidas y de accesos exclusivos.
- En las áreas de trabajo de sistemas, almacenamiento, cintotecas (bóvedas) y otros espacios de sistemas.
- En la administración y control de los medios de seguridad, y de la observación y vigilancia de los sistemas computacionales.
- En la vigilancia del mobiliario, equipo y activos informáticos de las áreas de sistemas.
- En la vigilancia del almacenamiento de información, datos y software institucional en las áreas de cómputo.
- En la vigilancia de accesos a los sistemas computacionales en las áreas ajenas al centro de cómputo.
- En la seguridad, salvaguarda y protección de las cintas, disquetes y otros medios magnéticos utilizados en el área de sistemas.
- En la seguridad y protección de manuales, instructivos, datos, información y reportes del área de sistemas.
- En la totalidad, veracidad y confiabilidad de la captura de información.

- El análisis de los planes de contingencias informáticas.
  - Evaluar la existencia, difusión, aplicación y uso del plan contra contingencias de sistemas.
  - Evaluar la aplicación de simulacros, así como del plan contra contingencias durante la ocurrencia de siniestros en los sistemas.
  - Evaluar la confiabilidad, veracidad y oportunidad en la aplicación de las medidas del plan contra contingencias.

- Auditoría de la seguridad y protección en el diseño de las instalaciones del área de sistemas de la empresa y/o empresas de cómputo.
  - En el análisis de los estudios de localización de planta para instalar el área de sistemas.
  - En el análisis para la localización de instalaciones físicas del área de sistemas.
  - En el análisis de los estudios de la densidad de población.
  - En el análisis de la infraestructura pública de servicios.
  - En el análisis de los medios de comunicación pública, y de los medios de transporte de pasajeros.
  - En el análisis de los estudios de composición del suelo para prevenir desastres naturales.
  - En el análisis del cableado telefónico interno para el funcionamiento del área de sistemas.
  - En el análisis del cableado externo y redes públicas del servicio telefónico, así como de telecomunicación para el funcionamiento del área de sistemas.

- Auditoría de la seguridad en los sistemas computacionales.
  - Evaluar el rendimiento y uso del sistema computacional y de sus periféricos asociados.
  - Evaluar la existencia, protección y periodicidad de los respaldos de bases de datos, software e información importante de la organización.
  - Evaluar la configuración, instalaciones y seguridad del equipo de cómputo, mobiliario y demás equipos del área de sistemas.
  - Evaluar el rendimiento, la aplicación y la utilidad del equipo de cómputo, mobiliario y demás equipos.
  - Evaluar la seguridad en el procesamiento de información.
  - Evaluar los procedimientos de captura, procesamiento de datos y emisión de resultados de los sistemas computacionales.
- Auditoría de la seguridad del hardware
  - Realizar inventarios de hardware, equipos y periféricos asociados.
  - Evaluar la configuración del equipo de cómputo (hardware).
  - Evaluar el rendimiento y uso del sistema computacional y sus periféricos asociados.
  - Evaluar el estado físico del hardware, periféricos y equipos asociados.
- Auditoría de la seguridad del software
  - Realizar inventarios de software, paqueterías y desarrollos empresariales.
  - Evaluar las licencias, permisos y usos de los sistemas computacionales.
  - Evaluar el rendimiento y uso del software de los sistemas computacionales.
  - Verificar que la instalación de software, paqueterías y sistemas desarrollados en la empresa sea la adecuada para cubrir las necesidades de esta última.
- Auditoría para verificar la captura, procesamiento de datos y emisión de resultados
  - Evaluar la totalidad, veracidad y confiabilidad de la captura de información.
  - Evaluar la existencia, difusión, aplicación y uso del plan contra contingencias en los sistemas.
  - Evaluar la aplicación de simulacros, así como del plan contra contingencias durante la ocurrencia de siniestros en los sistemas.
  - Evaluar la confiabilidad, veracidad y oportunidad en la aplicación de las medidas del plan contra contingencias.
- Auditoría de la prevención de actos premeditados que afecten el funcionamiento de los sistemas computacionales
- Protección contra los actos ilegales en contra de los sistemas, activos informáticos e información.
  - Contra sabotajes.
  - Por extorsión.

  - Por alteración o destrucción de datos.
  - Por fraudes.

- Protección contra el mal uso de la información.
  - Por invasión de privacidad.
  - Para mal uso de la confiabilidad.
  - Por uso inadecuado de los datos.

- Protección contra la piratería y robo de información.
  - Con medidas preventivas.
  - Con la protección de archivos.
  - Con limitación de accesos.
  - Con protección contra robos.
  - Con protección ante copias ilegales.

- Protección para el almacenamiento de la información.
  - Respaldos de programas e información.
  - Almacenamiento y custodia de cintas, disquetes, etcétera.
  - Lugares adecuados, como cintotecas (bóvedas), discotecas, etcétera.
  - El control y uso de información, programas y paquetes.

- Protección contra actos no intencionales.
  - Por negligencia y descuido.
  - Por fallas del equipo y del sistema.
  - Por fallas de carácter externo.

- Protección contra virus informático.
  - Medidas preventivas y correctivas.
  - Uso de vacunas y buscadores de virus.
  - Protección de archivos, programas e información.

- Protección y seguridad para el desarrollo de programas y proyectos de sistemas.
  - Desarrollo de programas y nuevos proyectos de sistemas.
  - Protección contra deficiencias de programas y lenguajes.
  - Prevención de fallas del sistema operativo.
  - Protección en el establecimiento de estándares de proyectos.

- Protección y seguridad para los accesos al sistema computacional y a la información.
  - En el uso de contraseñas.
    - Establecimiento de niveles de acceso y uso de archivos.
    - Para el uso de sistemas de encriptación.
  - Para el uso de estándares de seguridad y protección.

- Protección y seguridad del hardware, componentes del sistema, periféricos y equipos asociados.
  - Protección a la CPU.
- Mantenimiento preventivo y correctivo a la CPU.
  - Medidas de seguridad y protección.
  - Rutinas internas para el inicio del sistema.
  - Rutinas internas de auditoría y verificación de componentes.
- Mantenimiento preventivo y correctivo al sistema.
  - Rutinas internas de auditoría y verificación de conexiones.
  - Con el uso de manuales e instructivos de operación.
- Mantenimiento preventivo y correctivo a los periféricos.
  - Rutinas internas de auditoría y verificación de periféricos.
  - Para el uso adecuado de los periféricos.
- Mantenimiento preventivo y correctivo al equipo adicional.
  - Rutinas internas de auditoría y verificación de equipos.
- Resultados de auditorías de sistemas.
- Seguridad ante fenómenos sociales
  - Protección contra mítines, revueltas, etc.
    - Prevención de huelgas.
    - Prevención ante cambios sociales, económicos, legales, etc.

Prevención ante cambios tecnológicos.

El levantamiento de inventarios (sección 9.5), a fin de hacer un recuento de los bienes informáticos del área de sistemas cuya seguridad se tenga que evaluar; para llevar a cabo esto, es recomendable realizar los siguientes inventarios:

- Inventarios de los equipos de cómputo, contemplando la seguridad, protección y salvaguarda de los bienes informáticos y sistemas computacionales, sus marcas, procesadores, tarjetas madre, velocidad, configuración, componentes, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo y todos los demás aspectos relacionados con el inventario de la seguridad de estos equipos.
- Inventario de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo licencias, resguardos, originales, copias autorizadas y copias piratas, a fin de valorar su protección y custodia.

- Inventario del personal informático y usuarios del sistema, a fin de evaluar la protección de este importante recurso.
- Inventario de las medidas de seguridad y protección para los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo sus licencias, resguardos y copias de seguridad.
- Inventario de los bienes muebles, inmuebles, materiales y consumibles del área de sistemas, a fin de valorar su protección y uso adecuados.
- Inventario de los accesos a los sistemas de redes o sistemas mayores, dependiendo del diseñado del sistema, así como del acceso a la información y a los sistemas operativos, lenguajes, programas y demás software institucional de esas redes o sistemas mayores.
- Inventario de las instalaciones físicas, a fin de evaluar la vigilancia y los accesos establecidos para la protección y seguridad de los bienes informáticos del área de sistemas.
- Inventario de las normas, políticas, reglamentos y medidas preventivas y correctivas del área de sistemas, a fin de evaluar la seguridad establecida para satisfacer las necesidades de protección en la función informática.
- Otros inventarios relacionados con la seguridad, protección y salvaguarda de los bienes informáticos del área de sistemas.