Seguridad Informática: Cuestiones y Ejercicios.

1. ¿Qué diferencia hay entre el concepto de información y su calidad según lo entienda una empresa o los estudios de ingeniería?

   La diferencia entre el concepto de información y su calidad según lo entienda una empresa es que la información se refiere a los datos que se recopilan y procesan para tomar decisiones empresariales y mejorar el rendimiento de la empresa. La calidad de la información se relaciona con la precisión, relevancia y confiabilidad de los datos.

2. ¿Por qué se dice que la información de una empresa es su activo más valioso? Compare este activo con el personal de la misma y póngase en situaciones en las que ambos se pierden, ¿qué situación podría ser es más perjudicial para la continuidad de dicha empresa?

   Se dice que la información de una empresa es su activo más valioso debido a que la información proporciona una ventaja competitiva en el mercado. Además, la información puede ser utilizada para desarrollar nuevas estrategias de negocio, identificar nuevas oportunidades de mercado y mejorar la eficiencia de los procesos empresariales.

   Si la empresa pierde información crítica, como datos financieros o de clientes, esto podría ser muy perjudicial para su continuidad, ya que puede afectar la capacidad de la empresa para tomar decisiones informadas y mantener la confianza de sus clientes. Si la empresa pierde a su personal clave, como su equipo directivo o técnicos especializados, también podría ser muy perjudicial, ya que la empresa podría perder experiencia y conocimientos críticos.

   Sin embargo, si la empresa tiene un buen sistema de gestión de la información y cuenta con un equipo de personal talentoso y diverso, puede recuperarse más fácilmente de ambas situaciones y mantener su rendimiento y éxito a largo plazo.

3. Como responsables de seguridad hemos detectado que alguien está realizando acciones no lícitas, por ejemplo, copias no autorizadas de información. ¿Qué actitud debemos tomar?

   Si se detecta una actividad ilícita en nuestro sistema de datos, hay varias cosas que se pueden realizar para lograr una solución:

   - Buscar detener la actividad, desconectado el sistema de la red o, de alguna forma, anulando el acceso al mismo.
   - Recopilar toda la información posible que se tenga del atacante, así como las direcciones ip, nombre de usuario y archivos, etc.
   - Notificar a las autoridades que correspondan, como la de delitos informáticos del FBI, en el caso que se considere que la actividad es ilegal.
   - Actualizar el sistema, ya sea en software o, en las conexionado de las máquinas. Toda ayuda que pueda venir de un experto en seguridad es bienvenida.

4. ¿Qué medidas podrían ser las más adecuadas de cara a minimizar los ataques por virus en nuestra empresa?

   Hay varias medidas que se pueden implementar para minimizar los ataques por virus en una empresa:

   - Mantener actualizado el software: Es importante asegurarse de que todo el software utilizado en la empresa se mantenga actualizado con las últimas actualizaciones y parches de seguridad. Tener en cuenta que actualizar el sistema operativo, puede ocurrir que los programas utilizados pierdan compatibilidad, por lo que hay que probar si todo funciona antes de actualizar.
   - Capacitar al personal: Es fundamental capacitar al personal en cuanto a las mejores prácticas de seguridad informática. Esto incluye evitar abrir correos electrónicos sospechosos, descargar archivos de fuentes desconocidas y utilizar contraseñas seguras y robustas.
   - Utilizar software antivirus: El software antivirus puede detectar y eliminar virus, malware y otras amenazas de seguridad.
   - Realizar copias de seguridad: En caso de un ataque de virus, las copias de seguridad pueden utilizarse para restaurar los sistemas a un estado anterior.
   - Limitar el acceso: Es recomendable establecer diferentes niveles de acceso, de manera que solo aquellos empleados autorizados puedan acceder a la información más crítica.
   - Implementar medidas de seguridad física: Además de las medidas de seguridad informática, es importante implementar medidas de seguridad física, como controlar el acceso a las instalaciones de la empresa y asegurar que los sistemas informáticos estén protegidos contra el robo.

5. Si deseamos que nuestra empresa esté debidamente protegida tanto física como lógicamente, ¿qué deberíamos hacer?

   Para implementar seguridad lógica en nuestra empresa debemos tener en cuenta que la protección se realiza sobre el medio donde se transmite y en los protocolos.
   Se deben implementar medidas de seguridad lógica para proteger los datos y sistemas de la empresa de accesos no autorizados. Esto incluye el uso de contraseñas seguras, la implementación de un firewall y la instalación de software de seguridad actualizado.

   En cuanto a la seguridad física, debemos tener en cuenta la protección física del sistema, acceso de personal, incendio, agua, etc. Es importante implementar medidas de seguridad física para proteger los recursos críticos de la empresa, como los servidores y los datos almacenados. Esto incluye la instalación de sistemas de control de acceso físico, como cámaras de seguridad, alarmas y cerraduras de seguridad. Es decir, buscar un área apta donde correr el servidor, administración, etc.