LABORATORIO 4 CYBERSEGURIDAD

1. **Activo Critico:** Un activo critico es un recurso o servicio que es indispensable en una empresa, estos se caracterizan por ser la parte mas importante de esta y sin alguno de estos la empresa no funcionaría correctamente.
   Activos críticos dentro de la empresa de comercio:
   - Productos
   - Base de datos
   - Servidores
   - Sito web

   Dentro de estos activos el más crítico es la Base de datos ya que de ahí están la información de las tarjetas de créditos de los compradores y por ende es muy importante proteger este activo, después tenemos a los servidores que es donde se van a llegar los datos del Sitio Web y también este mismo ya que es por donde entraran los datos de las compras y por último los productos, que es la mercancía que se va a vender

2. **Amenazas Probables:**
   -Phishing: Ya que los compradores podrían recibir un enlace falso de la empresa y por ende podrían caer ante este ataque
   -Ingeniería Social: Si un trabajador de la compañía burla seguridad de la empresa podría dar con los servidores o con la base de datos y de ahí afectar seriamente los activos.
   -Ataque DDOS y DoS: Podrían afectar seriamente al sitio web afectando su correcto funcionamiento e incluso colapsarlo en caso de que la pagina no soporte tantas consultas.

   Dentro de las amenazas la mas critica seria con respecto a la Ingeniería Social ya que cualquier trabajador que tenga una fuerte conexión sobre la Base de Datos o con los servidores afectaría directamente a toda la empresa junto con los clientes, después le sigue los ataques DDos y Dos ya que afectaría directamente al sitio web y provocar el colapso de la página, y ya como ultimo el phishing ya que solo afectaría a aquellos que no se den cuenta de que la pagina no es la de la tienda virtual y por ende caer en ese ataque.

3. Se deben tener ciertos criterios mas que todo en la empresa y es que solo deben ingresar trabajadores autorizados a los recursos generales y es por eso que para ello deben a ver ciertos roles como por ejemplo un técnico en sistemas que se encargue de dirigir los servidores, al igual que un

encargado de las comunicaciones, que definirá cómo va la comunicación entre los sitios web con los servidores, también debe haber un encardo de supervisar cada movimiento de los trabajadores y ah si tener confianza de que ninguno de ellos afecte directamente a la empresa, ya por parte de los usuarios toca tener a una persona encargada de ayudar a cualquier solicitud que tenga el usuario.

4. Para la detección de cualquier problema tenemos a las personas encargadas para es que son:
   Técnico en Sistema: Encargado de supervisar los equipos conectados al sitio web y verificar correctamente que no haya ningún problema, estos analizan la entrada de los datos proporcionados, también en caso de que hallan virus o algún tipo de malware dentro de la empresa buscaran directamente como eliminarlo.
   Encargado en las comunicaciones: El supervisara si la comunicación entre el servidor y el sitio web, también puede ver si hay algún ataque tipo DDos que pueda interferir con la conexión de estos dos, y ah sí buscar rápidamente como restringir la amenaza

   De parte de los administradores de los servidores estos verificaran si todo el equipo está en correcto estado además verán si algún personal entre ellos no está autorizado y en dado caso se le dará un aviso para que este fuera de la sala y no pueda afectar directamente a los equipos.

5. Como se ha visto en este transcurso se pueden identificar los riesgos claros en esta empresa, pero toca tener en cuenta de que, si llega a formarse un ataque, se debe rápidamente solucionarlo, a esto se le llama plan de contención que es básicamente implementar medidas para solucionar el incidente en dado caso ocurra para eso se puede abordar lo siguiente:

   Desconectar el Servidor de los equipos: Si los dispositivos reciben un ataque de virus lo más primordial es desconectar el servidor de los equipos, ya que si el virus se llega a infectar en alguno servidor afectaría a todos los dispositivos directamente.
   Desconectar la red de equipos infectados: También es importante desconectar la red si algunos de los equipos están infectados, y por ende se debe desconectar la red de los equipos, hasta que haya una correcta eliminación en el virus.
   Cambiar contraseñas y usuarios: Dado que el equipo infectado contendrá información de la contraseña del usuario, lo más acertado seria cambiar de

usuario y colocarle una nueva contraseña a otro dispositivo, y también bloquear la cuenta del dispositivo infectado para que ah si no exista forma en la cual el virus puede acceder a información valiosa.
Eliminación de la amenaza: Ya teniendo protegidos correctamente a los sistemas, se puede proceder a la eliminación correcta del virus o amenaza que esté afectando a los dispositivos, para esto se pueden integrar antivirus o softwares capaces de eliminar el virus por completo, y ah sí limpiar todas las amenazas del dispositivo.

6. Ya teniendo listo y eliminadas las amenazas, lo que se debe hacer es dar recuperación a los datos, para esta ya luego de examinar el equipo se debe ir a la copia de seguridad de este, la cual todo dispositivo debe tener, con la copia de seguridad se garantiza la recuperación de los datos y dado a prevención de que el equipo fue infectado, estos datos deben integrarse a un nuevo dispositivo para que ah si no se repita el mismo escenario, también a los clientes se les puede notificar que los datos en caso de que los hayan perdido se han recuperado gracias a la copia de seguridad que hay en la empresa.

7. En conclusión, pudimos ver que todos estos escenarios son muy posibles en cualquier empresa y más si la información integrada de esta es muy valiosa, es por eso que esta debe tener conocimiento muy amplio sobre la seguridad y aplicar cada concepto sobre las amenazas, además debe tener siempre un plan de contingencias para abordar todos estos problemas en dado caso ocurran y sobre todo hacer lo posible para recuperar la información que haya sido afectada por alguna de estas amenazas, ya que como se saben los datos para un empresa es lo más valioso que tiene y por ende deben hacer todo lo posible para recuperarlos.