Nombre: Santiago del valle

ID: 000427744

1. (Valor 2.0) A continuación se da un listado de vulnerabilidades encontrado en la empresa ODEBECE S.A. se le pide que, como oficial de seguridad, identifique el/ los activos afectados en caso de que una amenaza llegara a aprovechar esta vulnerabilidad y redacte el control respectivo.

Vulnerabilidad	Amenaza(s)	Activo que se ve afectado	Control (debe especificar si es preventivo, correctivo o detectivo)
No hay un control de acceso físico al cuarto donde se encuentra el sistema de alimentación ininterrumpida de la empresa en la sede de Bucaramanga.	Podría haber un incendio por parte de un tercero por un intento de robo/daño además de poner en riesgo la disponibilidad del servicio en el caso de un apagón de la entidad. (Cabe resaltar el daño a las maquinas por los cortocircuitos)	Daño a la infraestructura de la empresa. (Riesgo de incendio) Disponibilidad del servicio	Preventivo
No se realizan mantenimientos preventivos a los equipos de red la empresa.	Tanto el software como el hardware pueden correr riesgo: El software debido a la falta de actualizaciones de seguridad puede más fácil de acceder/controlar por parte de terceros. El hardware simplemente se puede dañar debido al uso constante y deterioramiento de los componentes físicos.	Routers , Switches , Servidores , e información sensible (en caso de un ataque)	Correctivo
5 computadores de la empresa tienen desactivadas las actualizaciones automáticas del S.O. Esto porque pertenecen a los gerentes de cada área quienes no quieren reiniciar los equipos asignados a ellos.	El equipo puede sufrir fallas respecto al rendimiento de la misma debido al uso obsoleto de drivers antiguos. Además , las versiones antiguas de SO son más vulnerables a todo tipo de ataque.	Información personal por parte de los gerentes. (Si escala el problema) información y control digítal de la entidad.	Correctivo
No se encuentra un mapa de la red de la empresa con la ubicación de los dispositivos (router, switches y access	Frente a cualquier control/mantenimiento/ modificación por parte del equipo de sistemas, se corre el riesgo de “tumbar” la	Disponibilidad (Comunicación) Componentes de red (Router, Switches, Servidores)	Preventivo

point).	red o el dispositivo desconfigurando el mismo o cualquier conexión relacionada a él (Salto de fe)		
El personal de soporte no lleva registro detallado de los mantenimientos correctivos que se les hacen a los equipos de cómputo.	Frente a cualquier instalación de software pirata la entidad puede llegar a tener problemas legales.	Buen nombre de la entidad Sanción económica	Preventivo

2. (Valor 2.0) Lea cada situación atentamente e identifique situaciones que puedan afectar la seguridad informática de la empresa ODEBECE S.A.

Situación 1
El DBA de la empresa ODEBECE decidió darle perfil de administrador de la base de datos de clientes y proveedores a los dos programadores de la empresa, esto con el fin de que ejecutaran pruebas de los desarrollos que vienen realizando. Al principio habilitaba este usuario administrador cuando los programadores hacían pruebas, con el tiempo, olvidó revocar estos privilegios.

Grave , muy grave , el acceso a la base de datos de una entidad con el rol “root” o administrador debe ser asignada únicamente al DBA y hay múltiples ejemplos en este problema.

1. Modificación/extracción de información por parte de los desarrolladores posteriormente al trabajo realizado
2. Post-Modificación por parte de los desarrolladores la cual TUMBE o BORRE la base de datos de producción.
3. Acceso no autorizado por parte de terceros mediante el perfil de los desarrolladores, en el caso que un desarrollador se vea afectado en un ataque informático, con las credenciales prácticamente le da acceso ilimitado a la base de datos de una entidad.

Situación 2
El sistema operativo de 50 computadores de ODEBECE S.A. posee licencia OEM ya que fueron adquiridos en las promociones de un almacén de gran superficie. El software de ofimática no está licenciado sin embargo los computadores tienen el software instalado en período de prueba.

Se corre el riesgo de sufrir ataques a razón de falta de parches de los SO en caso de vencimiento o piratería de la licencia, además si se llega a utilizar el software ofimática posterior a su periodo de prueba, la entidad podría llegar a tener problemas legales en caso de una auditoria.

Por último, el uso de software no licenciado puede hacer que sea difícil o imposible obtener soporte técnico oficial en caso de problemas.

Situación 3
El alcalde del Municipio de “Salsipuedes” es reacio a invertir en tecnología y los aplicativos de gestión pública tales como los que manejan el recaudo del impuesto predial y demás gravámenes que realiza el municipio en un servidor con Windows Server 2003 debidamente licenciado.

Aparte del hecho de robar y tumbar información sensible respecto a los impuestos de los ciudadanos , también se afecta la productividad e integridad de los datos cuando se hacen estos cálculos , tanto la tecnología como los aplicativos de gestión pública permitiría al municipio obtener los resultados muchísimo más rápido íntegramente y visible para personas de todo tipo de edad , salud y etnia (Accesibilidad).

Situación 4

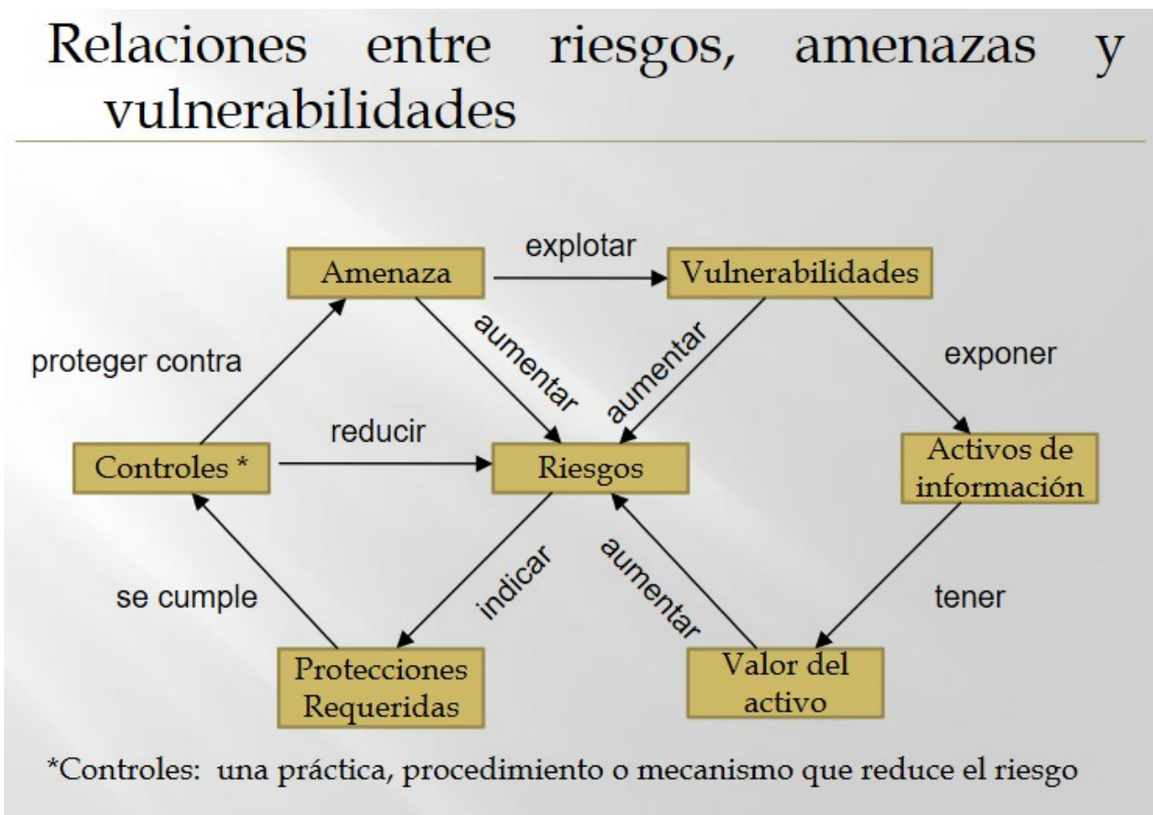
5 empleados de la empresa ODEBECE, traen su propio computador para realizar labores propias de su trabajo, esto es lo que se conoce como BYOD y la empresa lo viene practicando con los programadores que contrata desde hace un año.

Afecta factores tanto legales como de seguridad

1. Legales: En el caso de que uno de estos utilice programas piratas o sin licenciamiento dentro del contexto comercial de la empresa para llevar a cabo las labores asignadas.

2. Seguridad: Como se tiene acceso (En teoría) a la red de la empresa, cualquier tipo de virus externo podría verse propagado fácilmente mediante la red, además de que si estos descargan información "confidencial" o "sensible" para el uso de sus labores podría verse afectada.

3. (Valor 1.0) Escoge una de las amenazas del primer punto y completa de acuerdo con ésta un diagrama como el que sigue a continuación. Explica y personaliza el diagrama de acuerdo con la amenaza escogida. Puedes elaborarlo a mano.



Amenaza	Vulnerabilidad	Riesgo	Control	Activo	Valor Activo	Protección
Uso de computadores externos por parte de los desarrolladores	El uso de computadores externos los cuales se conecten a una red laboral.	Virus externo que afecte la disponibilidad e integridad tanto del servicio como de los datos.	Existe dos opciones De raíz, bloquear el acceso de la red a computadores los cuales no sean de la entidad De control,	La información sensible y lógica del negocio	Activos medibles Firewall de la red "administrativa" $4.300.000 - $17.000.000 Activos no medibles	El firewall configurado con el acceso de los dispositivos permitidos

			Aplicar controles más rigurosos en la red con el fin de aislar la subred “administrativa” la cual contiene los servidores y bases de datos.		Información Disponibilidad y trazabilidad del servicio	