Caso 1: Valoración de Activos en el Hospital Venus

1. **Contexto del Hospital Venus:**
    - El Hospital Venus realizauna valoración de activos, centrándose en la disponibilidad, confidencialidad e integridad de la información relacionada con sus procesos de negocio.
2. **Procesos de Negocio y Entrevistas:**
    - Se han realizado entrevistas para entender los impactos en diferentes procesos de negocio. El primero de ellos se enfoca en el sistema de transplantes.
3. **Sistema de Transplantes - Entrevista 1:**
    - **Responsable del Proceso:** El responsable de este proceso coordina las donaciones y transplantes en un área de 300 km a la redonda.
    - **Información Bajo su Responsabilidad:** Incluye una base de datos con listados de personas esperando donaciones, donantes autorizados y órganos disponibles para transplante.
    - **Percepción del Riesgo:** El responsable considera inaceptables varios impactos potenciales en la información, destacando la importancia crítica de la integridad y disponibilidad de los datos.
4. **Análisis de Impacto:**
    - **Uso de Plantilla de Valoración:** Para cada proceso de negocio, se debe utilizar una plantilla de valoración para determinar los impactos en términos de disponibilidad, confidencialidad e integridad.
    - **Tipos de Impactos:** En base a lo expuesto por cada propietario del activo, se deberán identificar los tipos de impactos posibles y utilizar las guías de valoración para asignar valores a estos impactos.
5. **Desarrollo de la Valoración:**
    - **Recolección de Datos:** Recopilar la información proporcionada durante las entrevistas para entender los riesgos y preocupaciones de cada responsable de proceso.
    - **Aplicación de la Plantilla de Valoración:** Utilizar los datos recopilados para completar la plantilla de valoración, asignando valores a los impactos en términos de disponibilidad, confidencialidad e integridad para cada proceso de negocio.
6. **Conclusión y Recomendaciones:**
    - **Síntesis del Análisis:** Resumir los hallazgos del análisis, destacando los riesgos y preocupaciones clave para cada proceso.

- **Recomendaciones:** Proponer medidas para mitigar los riesgos identificados y mejorar la gestión de los activos críticos del hospital.

Caso 2.

Paso 1: Creación del Árbol de Activos

1. **Transplantes**
    - Proceso: Transplantes
    - Servidor Unix "Ares"
    - Conexión a Internet
    - VPN
2. **RRHH**
    - Proceso: RRHH
    - Servidor Windows 2000 "Venus"
    - Cortafuegos
    - SAN (almacenamiento)
    - PCs en la sala de administración
3. **Gestión Hospitalaria**
    - Proceso: Gestión Hospitalaria
    - Sistema AS400 "Juno"
    - SAN (almacenamiento)
    - PCs en cada planta
    - Salas con acceso controlado

Valoración de Activos del Hospital Venus:

Activo / Proceso	Descripción del Impacto	Guía de Valoración
Sistema de Transplantes		
Servidor Ares	Interrupción crítica en la gestión de transplantes, riesgo de pérdida de vidas.	Alta prioridad en disponibilidad e integridad.
Conexión a Internet	Riesgo de filtración de datos cifrados, interrupción en el intercambio de información.	Alta prioridad en confidencialidad.
RRHH		
Servidor Windows 2000 Venus	Interrupción en la gestión de nóminas, impacto en operaciones administrativas.	Alta prioridad en disponibilidad.
Aplicación VenusERP	Riesgo de acceso no autorizado, pérdida de datos de nómina.	Alta prioridad en confidencialidad e integridad.
Gestión Hospitalaria		
Sistema AS400 Juno	Interrupción en el acceso a historias clínicas, impacto en la atención al paciente.	Alta prioridad en disponibilidad e integridad.
Base de datos de historias clínicas	Riesgo de filtración de información sensible del paciente.	Alta prioridad en confidencialidad.

Aplicación del Método de Herencia

- **Servidor Unix "Ares" (Transplantes)**
    - Hereda los valores de Transplantes
- **Servidor Windows 2000 "Venus" (RRHH)**
    - Hereda los valores de RRHH
- **Sistema AS400 "Juno" (Gestión Hospitalaria)**
    - Hereda los valores de Gestión Hospitalaria
- **SAN, Cortafuegos, VPN, Conexión a Internet, PCs**
    - Heredan los valores máximos de los procesos a los que dan soporte

Caso 3: Análisis de Amenazas y Asociación con Activos en el Hospital Venus

Metodología:

1. Identificación de amenazas.
2. Asociación de amenazas a activos específicos.
3. Evaluación del impacto de las amenazas.

4. Uso de una plantilla para marcar los impactos.

Paso 1: Identificación de Amenazas Las amenazas se clasifican en las siguientes categorías:

- **Desastres**: Incluyen terrorismo, fuego, accidente industrial, fenómenos meteorológicos, inundación, rayo, terremoto.
- **Errores:** Comprenden error de configuración, error de desarrollo, error de mantenimiento (HW y SW), error de operador, error de usuario.
- **Fallos:** Se refieren a corte de energía, deterioro de soporte, fallo de climatización, fallo de HW, fallo de SW, fallo de comunicaciones, falta de personal, incumplimiento SLA.
- **Intencionadas**: Engloban ataques DoS, cesión de información, vandalismo, escuchas, intrusión, robo, alteración de comunicaciones, software malicioso (virus), abuso del sistema, uso no autorizado de una aplicación.

Paso 2: Asociación de Amenazas a Activos y Determinación de Impactos Se hizo una asociación detallada delas amenazas con los activos críticos del hospital, evaluando el impacto potencial en términos de pérdida de disponibilidad, confidencialidad e integridad, así como otros impactos como daño físico o a la reputación.

Paso 3: Uso de Plantilla para Marcar Impactos

Amenaza	15m	3h	1d	1s	DP	DT	RI	RE	EPE	EGE	MD
Amenazas Lógicas											
Suplantación identidad por externos		X					X	X			
Uso no autorizado de una aplicación	X					X	X				
Abuso del sistema			X					X	X		
Amenazas a las Comunicaciones											
Alteración comunicaciones				X		X	X				
Fallo comunicaciones		X							X		
SW malicioso	X					X		X			
Fallos Técnicos											
Fallo servidor				X				X		X	
Fallo elemento de red		X							X		
Fallo de electricidad	X										X
Fallo de aire acondicionado			X				X			X	
Fallo de aplicaciones SW				X		X	X				

Caso 4: Análisis de un Ataque Dirigido por un Estado

1. **Selección del Caso:**
    - **Ataque:** Stuxnet.
    - **Año:** Descubierto en 2010.
    - **País involucrado:** Se sospecha que fue desarrollado por Estados Unidos e Israel.
2. **Descripción del Ataque:**
    - **Objetivo**: un objetivo principal de Stuxnet era sabotear las centrifugadoras de enriquecimiento de uranio en las instalaciones nucleares de Natanz, Irán.
    - **Método**: Stuxnet era un gusano informático extremadamente sofisticado que se propagaba a través de dispositivos USB y explotaba vulnerabilidades de día cero en Microsof Windows. Una vez en el sistema, buscaba controladores de sistemas de control industrial (SCADA) fabricados por Siemens, utilizados en las plantas nucleares.
    - **Efectos**: El gusano alteraba la velocidad de las centrifugadoras, causando daños físicos mientras enviaba informes de funcionamiento normal a los operadores. Esto resultó en una disminución significativa en la capacidad de enriquecimiento de uranio de Irán.
3. **Justificación de la Selección:**
    - **Relevancia geopolítica**: Este ataque no solo fue significativo en términos técnicos, sino también en su impacto en las relaciones y tensiones internacionales.
    - **Nivel de sofisticación**: Stuxnet marcó un hito en los ataques cibernéticos dirigidos por estados, destacando por su complejidad y el uso de múltiples técnicas avanzadas.
    - **Impacto físico directo**: Uno de los primeros ejemplos de un ataque cibernético que causó daño físico directo a una infraestructura crítica.
4. **Conclusiones:**
    - **Cambios en la Ciberseguridad**: Stuxnet cambió el panorama de la ciberseguridad, demostrando que los ataques cibernéticos pueden tener consecuencias físicas y geopolíticas serias.
    - **Desafíos para el futuro**: Plantea la necesidad de una mayor seguridad en sistemas de control industrial y una cooperación internacional más fuerte en ciberseguridad.

- **Lecciones aprendidas**: Este caso subraya la importancia de proteger las infraestructuras críticas contra amenazas cibernéticas avanzadas y la necesidad de estar preparados para ataques cibernéticos complejos y dirigidos.

Caso 5: Análisis de un Ataque Dirigido por el Crimen Organizado

1. **Selección del Caso:**
    - **Ataque:** Ataque a la cadena de suministro de software SolarWinds.
    - **Año:** Descubierto en 2020.
    - **Grupo involucrado:** APT29, también conocido como Cozy Bear, asociado con el crimen organizado ruso.
2. **Descripción del Ataque:**
    - **Objetivo**: El ataque tenía como objetivo infiltrarse en redes gubernamentales y de empresas privadas a través de una actualización troyanizada del software de gestión de redes SolarWinds.
    - **Método**: Los atacantes comprometieron el proceso de desarrollo de software de SolarWinds e insertaron un backdoor en su software Orion. Este backdoor se distribuyó a miles de clientes de SolarWinds, incluidas agencias gubernamentales y grandes corporaciones.
    - **Efectos**: El ataque permitió a los atacantes acceso a redes seguras, robo de información sensible y la posibilidad de realizar vigilancia a largo plazo sobre las víctimas.
3. **Justificación de la Selección:**
    - **Escala y alcance**: Este ataque es un ejemplo destacado de cómo el crimen organizado puede utilizar tácticas avanzadas para infiltrarse en múltiples organizaciones a gran escala.
    - **Impacto significativo**: El ataque afectó a importantes entidades gubernamentales y empresas, destacando la vulnerabilidad de las cadenas de suministro de software.
    - **Conciencia sobre la seguridad en la cadena de suministro**: Resaltó la importancia de asegurar no solo los propios sistemas de una organización sino también la cadena de suministro de software.

4. **Conclusiones:**

    - **Necesidad de vigilancia continua**: Este caso subraya la necesidad de una vigilancia y una gestión de riesgos constantes, incluso en componentes de software confiables.
    - **Cooperación internacional contra el crimen organizado**: Resalta la importancia de la cooperación internacional en la lucha contra las amenazas cibernéticas del crimen organizado.
    - **Lecciones aprendidas**: Subraya la importancia de las auditorías de seguridad en la cadena de suministro de software y la necesidad de implementar prácticas de seguridad robustas en todas las etapas del desarrollo de software.

Caso 6: Análisis de un Ataque Dirigido por Grupos Terroristas

1. **Selección del Caso:**

    - **Ataque:** Ataque al Canal de TV Francés TV5Monde.
    - **Año:** 2015.
    - **Grupo involucrado:** ISIS (Estado Islámico).

2. **Descripción del Ataque:**

    - **Objetivo**: Interrumpir las operaciones de TV5Monde, una cadena de televisión francesa de alcance mundial, y difundir mensajes propagandísticos.
    - **Método**: Los atacantes utilizaron técnicas de phishing para obtener credenciales de acceso a los sistemas internos de TV5Monde. Luego, desplegaron un malware que les permitió tomar el control de los sistemas de transmisión y las cuentas de redes sociales de la cadena.
    - **Efectos**: La emisión de TV5Monde fue interrumpida durante horas. Los atacantes también publicaron documentos clasificados de empleados y militares franceses en las redes sociales, junto con mensajes de apoyo al ISIS.
    -

3. **Justificación de la Selección:**

    - **Impacto directo en los medios de comunicación**: Este ataque demuestra cómo los grupos terroristas pueden utilizar el ciberespacio para atacar infraestructuras críticas y medios de comunicación.

- **Propaganda terrorista**: El uso del ciberataque para difundir propaganda terrorista subraya la dimensión psicológica y mediática de estas agresiones.
- **Desafíos en la ciberseguridad**: Resalta la importancia de la seguridad de la información y la necesidad de proteger las infraestructuras críticas de ataques cibernéticos.

4. **Conclusiones:**
    - **Necesidad de medidas de seguridad robustas**: Este caso enfatiza la importancia de implementar medidas de seguridad sólidas para proteger contra ataques cibernéticos, incluyendo la concienciación sobre el phishing y otras técnicas de ingeniería social.
    - **Preparación para ataques dirigidos**: Subraya la necesidad de que las organizaciones estén preparadas para ataques dirigidos y sofisticados que puedan tener motivaciones políticas o ideológicas.
    - **Lecciones aprendidas**: Destaca la importancia de tener planes de respuesta a incidentes y de recuperación de desastres para asegurar la continuidad del negocio ante ataques cibernéticos.

Caso 7: Análisis de un Ataque Dirigido por Grupos Hacktivistas.

1. **Selección del Caso:**
    - **Ataque:** Ataque a Sony Pictures en 2014.
    - **Grupo involucrado**: Se sospecha que fue un grupo hacktivista denominado "Guardians of Peace".
2. **Descripción del Ataque:**
    - **Objetivo**: El ataque tenía como objetivo intimidar a Sony Pictures para evitar la publicación de la película "The Interview", que parodia al líder de Corea del Norte, Kim Jong-un.
    - **Método**: El ataque se inició con el envío de correos electrónicos de phishing a empleados de Sony Pictures, obteniendo así acceso a la red interna. Luego, los atacantes desplegaron malware que borró datos y desactivó computadoras. También se filtró información confidencial, incluyendo correos electrónicos y datos personales de empleados.
    - **Efectos**: El ataque resultó en daños a la infraestructura de TI de Sony, pérdida de datos críticos, y una gran exposición pública negativa debido a la filtración de información.

3. **Justificación de la Selección:**
    - **Impacto en la Industria del Entretenimiento**: Este caso es significativo por su impacto en una importante empresa de entretenimiento y la manipulación de la libertad de expresión.
    - **Naturaleza política y social del ataque**: El ataque tenía motivaciones políticas y sociales, características comunes de los hacktivistas.
    - **Lecciones sobre la seguridad de la información**: Resalta la vulnerabilidad de las grandes corporaciones frente a ataques cibernéticos y la importancia de la seguridad de la información.
4. **Conclusiones:**
    - **Importancia de la formación en ciberseguridad**: Este caso subraya la necesidad de formación en ciberseguridad para todos los empleados, especial en la prevención de phishing.
    - **Gestión de crisis y comunicación**: Enfatiza la importancia de una respuesta eficiente y comunicación efectiva durante y después de un ciberataque.
    - **Lecciones aprendidas**: Destaca la necesidad de una estrategia de seguridad de la información robusta, incluyendo la protección contra amenazas internas y externas, y la preparación para incidentes cibernéticos.

Caso 8: Análisis de Incidentes de Seguridad en Diferentes Fases del Ciclo de Vida de los Datos

1. **Incidentes a Analizar:**
    - a. Robo a eBay de datos de 145 millones de clientes en 2014.
    - b. Robo a la empresa de vinos y licores Specs de más de medio millón de datos de clientes entre 2012 y 2014.
    - c. Robo de datos a turistas hospedados en hoteles de Europa y Oriente Medio mediante el uso de la WiFi gracias a la vulnerabilidad EternalBlue en 2017.
    - d. El FBI declaró haber perdido 160 ordenadores portátiles con información confidencial en 2007.
2. **Análisis de Cada Incidente:**
    - **a. Robo a eBay (2014):**
        - **Fase del Ciclo de Vida**: Almacenamiento y Acceso.

        - **Descripción**: Los atacantes obtuvieron acceso a la base de datos que contenía los datos de los clientes. La brecha se produjo debido a la falta de medidas de seguridad adecuadas en el almacenamiento y acceso a los datos.

    - **b. Robo a Specs (2012-2014):**
        - **Fase del Ciclo de Vida**: Almacenamiento y Transmisión.
        - **Descripción**: Los atacantes accedieron a la base de datos de clientes y extrajeron la información durante un período prolongado. El incidente involucró tanto el almacenamiento inseguro como la transmisión de datos.
    - **c. Robo de datos a turistas (2017):**
        - **Fase del Ciclo de Vida**: Transmisión.
        - **Descripción**: La vulnerabilidad EternalBlue fue explotada para interceptar datos transmitidos a través de redes WiFi. Este incidente se centra en la fase de transmisión de los datos.
    - **d. Pérdida de ordenadores del FBI (2007):**
        - **Fase del Ciclo de Vida**: Almacenamiento y Transporte.
        - **Descripción**: La pérdida de dispositivos físicos que contenían información confidencial indica una falla en la fase de almacenamiento y transporte de los datos.

3. **Conclusiones:**
    - **Importancia de la Seguridad en Todas las Fases**: Estos incidentes demuestran que las brechas de seguridad pueden ocurrir en cualquier fase del ciclo de vida de los datos, desde el almacenamiento hasta la transmisión y el transporte.
    - **Necesidad de Medidas Integrales de Seguridad**: Se subraya la necesidad de implementar medidas de seguridad robustas en todas las fases del ciclo de vida de los datos para prevenir brechas y proteger la información confidencial.

Caso 9: Diseño de una Normativa o Procedimiento sobre el Uso de los Recursos TIC.

1. **Introducción:**
    - Presentación de la necesidad y el propósito de la normativa.

- Alcance: Aplicable a todos los empleados, oferentes ócontratistas y visitantes que utilicen recursos TIC de la organización.

2. **Definiciones y Terminología:**
    - Clarificación de términos clave como "recursos TIC", "seguridad de la información", "usuarios autorizados", etc.
3. **Políticas Generales de Uso:**
    - Uso aceptable de los recursos TIC.
    - Prohibiciones específicas (por ejemplo, uso de software no autorizado, actividades ilegales, etc.).
    - Directrices para el uso de correo electrónico, Internet y redes sociales.
4. **Seguridad y Confidencialidad:**
    - Responsabilidades de los usuarios en la protección de datos y la confidencialidad.
    - Directrices para la creación y gestión de contraseñas.
    - Procedimientos en caso de incidentes de seguridad.
5. **Mantenimiento y Soporte:**
    - Procesos para solicitar soporte técnico.
    - Directrices para la actualización y mantenimiento de equipos y software.
6. **Acceso y Control de Accesos:**
    - Políticas para la asignación y revocación de accesos a sistemas y aplicaciones.
    - Reglas para el uso de dispositivos móviles y teletrabajo.
7. **Uso de Equipos y Software:**
    - Normas para el uso de equipos proporcionados por la empresa.
    - Políticas sobre la instalación de software y uso de licencias.
8. **Gestión de Incidentes y Continuidad del Negocio:**
    - Procedimientos para la gestión de incidentes de seguridad TIC.
    - Planes de continuidad del negocio y recuperación ante desastres.
9. **Formación y Concienciación:**
    - Programas de formación en seguridad TIC para empleados.
    - Campañas de concienciación sobre riesgos y mejores prácticas.

10. **Cumplimiento y Revisión de la Normativa:**
    - Mecanismos de supervisión y control del cumplimiento de la normativa.
    - Procesos para la revisión y actualización periódica de la normativa.

Caso 10: Identificación de Activos Críticos en Pérez e Hijos y Sánchez (PHS)

Objetivo: Analizar los procesos de negocio clave de Pérez e Hijos y Sánchez (PHS) para identificar los activos críticos más importantes a proteger.

Desarrollo del Caso:

1. **Descripción de la Organización:**
    - Pérez e Hijos, fundada en 1980, es un importante distribuidor español de productos de papelería y oficina.
    - En la década de los 90, se fusionó con Sánchez, una firma de diseñadores comerciales y expertos en patentes, formando PHS.
    - PHS diseña, imprime y distribuye productos de papelería en España y tiene una presencia activa en varias capitales europeas.
2. **Procesos de Negocio Clave:**
    - La producción y distribución de elementos de papelería y materiales de oficina a medida.
    - El mantenimiento de una revista trimestral, considerada un proceso de negocio crítico.
3. **Infraestructura de IT y Red:**
    - Redes locales Ethernet en cada localización.
    - Conexiones a Internet y acceso remoto para mantenimiento y trabajo remoto.
    - Servidores Windows Server 2012 y sistemas IBM RS6000 mantenidos interna y externamente.
4. **Identificación de Activos Críticos:**
    - **Datos de Clientes y Proveedores**: Información crítica para las operaciones comerciales y las ventas.
    - **Infraestructura de TI**: Incluyendo servidores, redes y sistemas críticos que soportan todas las operaciones de negocio.
    - **Propiedad Intelectual**: Diseños y patentes de productos, fundamentales para la ventaja competitiva de PHS.

- **Instalaciones Físicas**: Oficinas en Valencia y Madrid, y varias oficinas de ventas pequeñas.
- **Publicación Trimestral**: Un elemento clave para el marketing y la comunicación con los clientes.

5. **Problemas de Seguridad Potenciales:**
    - Riesgos de seguridad en la red debido a la alta rotación de empleados y a las diversas interfaces tecnológicas.
    - Competencia directa y posibles amenazas internas por parte de antiguos empleados.
    - Necesidad de proteger la propiedad intelectual y los datos sensibles de la compañía.
6. **Conclusiones:**
    - PHS debe priorizar la seguridad de sus activos críticos para proteger su información sensible, mantener la continuidad del negocio y salvaguardar su reputación.
    - Es esencial implementar políticas de seguridad robustas, concienciar a los empleados sobre las prácticas de seguridad y asegurar la infraestructura de TI y los datos.

Caso 11: Selección de Controles de la ISO 27002 para el Hospital Venus.

Controles ISO 27002 Seleccionados

15. **Relaciones con Suministradores:**
    - **15.1.1 Política de seguridad de la información para suministradores:** Establecer políticas de seguridad específicas para suministradores, asegurando que manejen la información del hospital de manera segura.
    - **15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores:** Evaluar y tratar los riesgos asociados a los suministradores, especialmente aquellos que tienen acceso a datos sensibles.
    - **15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones:** Gestionar los riesgos en la cadena de suministro de TIC para prevenir vulnerabilidades y asegurar la continuidad del servicio.
    - **15.2.1 Supervisión y revisión de los servicios prestados por terceros:** Monitorizar y revisar regularmente los servicios prestados por terceros para asegurar su conformidad con las políticas de seguridad.
    - **15.2.2 Gestión de cambios en los servicios prestados por terceros:** Gestionar los cambios en los servicios de terceros para mantener la seguridad y la protección de los datos.

16. **Gestión de Incidentes en la Seguridad de la Información:**

    - **16.1.1 Responsabilidades y procedimientos:** Establecer un plan de respuesta a incidentes y un proceso de gestión de incidentes para abordar efectivamente los eventos de seguridad.
    - **16.1.2 Notificación de los eventos de seguridad de la información:** Implementar un proceso para notificar eventos de seguridad, permitiendo una respuesta rápida.
    - **16.1.3 Notificación de puntos débiles de la seguridad**: Fomentar la notificación de vulnerabilidades detectadas para su pronta corrección.
    - **16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones:** Evaluar los eventos de seguridad para determinar el impacto y las acciones necesarias.
    - **16.1.5 Respuesta a los incidentes de seguridad**: Desarrollar procedimientos para responder eficazmente a incidentes de seguridad, minimizando el impacto.
    - **16.1.6 Aprendizaje de los incidentes de seguridad de la información**: Analizar los incidentes para aprender de ellos y mejorar las medidas de seguridad.
    - **16.1.7 Recopilación de evidencias**: Establecer procedimientos para la recopilación de evidencias en caso de incidentes, lo que puede ser crucial para investigaciones legales o auditorías.

17. **Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio:**

    - **17.1.1 Planificación de la continuidad de la seguridad de la información:** Desarrollar un plan de continuidad que incluya la seguridad de la información para asegurar la operatividad en situaciones adversas.
    - **17.1.2 Implantación de la continuidad de la seguridad de la información:** Implementar y mantener las medidas necesarias para la continuidad de la seguridad de la información.
    - **17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información:** Verificar y revisar periódicamente las medidas de continuidad para garantizar su efectividad y adecuación.

18. **Cumplimiento:**

    - **18.1.1 Identificación de la legislación aplicable:** Asegurar que las prácticas de seguridad estén en conformidad con las leyes y regulaciones aplicables.
    - **18.1.2 Derechos de propiedad intelectual (DPI):** Proteger los derechos de propiedad intelectual, incluyendo software y documentación.

- **18.1.3 Protección de los registros de la organización:** Asegurar la protección y conservación adecuada de los registros de la organización.
- **18.1.4 Protección de datos y privacidad de la información personal:** Asegurar la protección de los datos personales y la privacidad según la legislación aplicable.
- **18.1.5 Regulación de los controles criptográficos:** Gestionar y regular el uso de controles criptográficos para proteger la confidencialidad, integridad y disponibilidad de los datos.
- **18.2.1 Revisión independiente de la seguridad de la información:** Realizar revisiones independientes de la seguridad para asegurar la efectividad de las medidas implementadas.
- **18.2.2 Cumplimiento de las políticas y normas de seguridad:** Verificar regularmente el cumplimiento de las políticas y normas de seguridad de la información.
- **18.2.3 Comprobación del cumplimiento técnico:** Realizar auditorías técnicas para verificar el cumplimiento de las normativas y estándares de seguridad.

Caso 12: Diseño de un Programa de Ciberseguridad para GreenChayote Exporters.

Perfil de GreenChayote Exporters: GreenChayote Exporters cuenta con una extensa red de cultivo, procesamiento y logística. La empresa utiliza tecnología avanzada para la gestión de la cadena de suministro, sistemas de información para el seguimiento de envíos, y plataformas digitales para transacciones comerciales y comunicaciones con clientes internacionales.

Desarrollo del Programa de Ciberseguridad:

1. **Políticas y Estrategia de Seguridad:**
    - Crear políticas de seguridad que aborden específicamente las necesidades del negocio de exportación, como la seguridad de la cadena de suministro y la protección de datos comerciales y financieros.
    - Desarrollar una estrategia de seguridad que se alinee con los objetivos empresariales, como la expansión de mercado y la eficiencia operativa.
2. **Organización de la Seguridad de la Información:**
    - Establecer un equipo de seguridad de la información con roles bien definidos, responsabilidades y autoridad para implementar la estrategia de seguridad.
    - Crear un comité de seguridad que incluya a representantes de diferentes departamentos para asegurar una visión integral y colaborativa.

3. **Gestión de Activos y Clasificación de la Información:**
    - Realizar un inventario completo de los activos de TI, incluyendo hardware y software utilizados en la cadena de suministro y logística.
    - Clasificar la información según su importancia para el negocio, como datos financieros, información de clientes y detalles de envíos.
4. **Control de Accesos:**
    - Establecer políticas de control de acceso basadas en roles para garantizar que solo el personal autorizado tenga acceso a información crítica.
    - Implementar soluciones de autenticación fuerte para sistemas críticos, especialmente aquellos utilizados para transacciones financieras y gestión de clientes.
5. **Criptografía:**
    - Utilizar la criptografía para proteger la información sensible, especialmente la transmitida a través de Internet, como ordenes de compra y contratos.
    - Gestionar las claves criptográficas de manera segura, manteniendo su confidencialidad y disponibilidad.
    -
6. **Seguridad Física y Ambiental:**
    - Proteger las instalaciones físicas, incluyendo almacenes y centros de datos, con controles de acceso y medidas de seguridad como cámaras de vigilancia.
    - Implementar medidas para proteger contra riesgos ambientales y físicos, como incendios o inundaciones.
7. **Seguridad en Operaciones:**
    - Establecer procedimientos operativos seguros para la administración de sistemas y redes.
    - Instalar y mantener soluciones de seguridad como antivirus y firewalls para proteger contra malware y ataques cibernéticos.
8. **Seguridad en las Comunicaciones:**
    - Asegurar las comunicaciones dentro de la red corporativa y con socios externos mediante VPNs y otras tecnologías de encriptación.
    - Establecer políticas para el intercambio seguro de información con clientes y proveedores.
9. **Adquisición, Desarrollo y Mantenimiento de Sistemas:**

- Integrar requisitos de seguridad en el desarrollo y adquisición de sistemas de TI, particularmente aquellos utilizados en la gestión de la cadena de suministro.
- Realizar pruebas periódicas de seguridad en aplicaciones y sistemas para detectar y remediar vulnerabilidades.

10. **Gestión de Incidentes de Seguridad de la Información:**
    - Desarrollar y mantener un plan de respuesta ante incidentes para gestionar de manera eficaz cualquier brecha de seguridad.
    - Capacitar al personal en la identificación y manejo de incidentes de seguridad, incluyendo la detección y reporte de actividades sospechosas.
11. **Aspectos de la Seguridad de la Información en la Gestión de la Continuidad del Negocio:**
    - Incorporar consideraciones de seguridad de la información en la planificación de la continuidad del negocio, especialmente para procesos críticos como logística y procesamiento de pedidos.
    - Realizar pruebas y simulacros regulares para garantizar la eficacia de los planes de continuidad del negocio.
12. **Cumplimiento y Auditoría:**
    - Asegurarse de que las prácticas de seguridad estén en conformidad con las leyes y regulaciones de los países a los que se exporta, así como con las normativas internacionales.
    - Realizar auditorías internas y externas de seguridad de la información para evaluar la efectividad de las medidas implementadas y garantizar el cumplimiento continuo.

Caso 13: Análisis de Seguridad para "GreenChayote Exporters"

1. **Diagramar la Arquitectura:**
    - **Sistema de Gestión de Cadena de Suministro (SCM):** Este sistema gestiona todo, desde el cultivo hasta la distribución de chayotes, integrándose con datos de agricultores, logística, y control de calidad.

- **Sistema de Planificación de Recursos Empresariales (ERP):** Utilizado para la administración de recursos, finanzas, y relaciones con clientes. Ambos sistemas están alojados en la nube y accesibles a través de una red corporativa segura.
- **Red de Comunicaciones:** Conexiones cifradas para comunicaciones con socios comerciales en Europa y Norteamérica, y conexiones internas para el personal en Costa Rica.

2. **Identificación de Amenazas con STRIDE:**
    - **Spoofing:** Riesgo de suplantación de identidad de usuarios en los sistemas SCM y ERP.
    - **Tampering:** Potencial manipulación de datos de inventario, envíos, y transacciones financieras.
    - **Repudiation:** Desafíos en la verificación de transacciones y comunicaciones.
    - **Information Disclosure:** Riesgo de exposición de datos confidenciales del negocio y de clientes.
    - **Denial of Service:** Posibles ataques que podrían interrumpir el funcionamiento de los sistemas críticos.
    - **Elevation of Privilege:** Amenazas internas o externas que busquen obtener accesos no autorizados a información privilegiada.
3. **Estrategias de Mitigación del Riesgo:**
    - **Spoofing:** Implementación de autenticación multifactor y protocolos de seguridad estrictos.
    - **Tampering:** Cifrado de datos y auditorías regulares para asegurar la integridad de la información.
    - **Repudiation:** Uso de firmas digitales y sistemas de trazabilidad para validar transacciones.
    - **Information Disclosure:** Políticas de acceso basadas en roles y encriptación de datos sensibles.
    - **Denial of Service:** Planes de redundancia y recuperación ante desastres para asegurar la continuidad del negocio.
    - **Elevation of Privilege:** Revisiones periódicas de derechos de acceso y aplicación del principio de mínimo privilegio.

CASO 14

Desarrollar un análisis de amenazas completo para "GreenChayote Exporters" utilizando Microsoft Threat Modeling Tool 2016.

Informe de modelado de amenazas

Creado en 1/7/2024 22:35:39

Nombre del modelo de amenaza: Exportadores de GreenChayote

Dueño: Germán Rivera

Crítico:

Colaboradores:

Descripción:

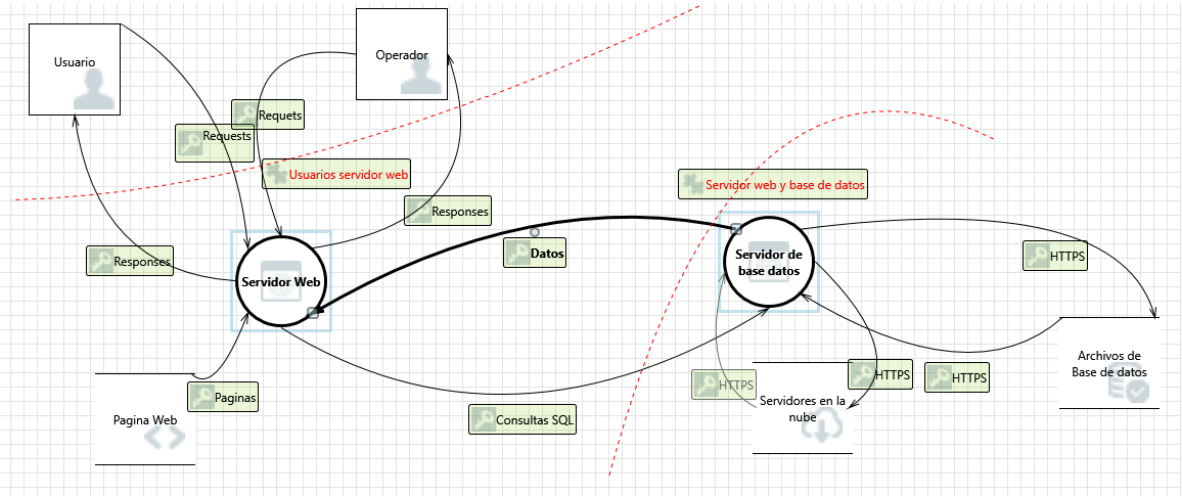
Suposiciones:

Dependencias externas:

Resumen del modelo de amenazas:

No iniciado	44
No aplicable	0
Necesita investigación	1
Mitigación implementada	0
Total	45
Total migrado	0

Diagrama: Diagrama 1



Caso 15: Diseño de un Plan de Recuperación de Incidentes para una Organización Ficticia

Plan de Recuperación de Incidentes:

1. **Preparación e Identificación de Incidentes:**
    - **Equipo de Respuesta a Incidentes:** Formar un equipo de respuesta a incidentes con roles y responsabilidades claramente definidos.
    - **Herramientas y Recursos**: Asegurar que el equipo tenga las herramientas necesarias para detectar y analizar incidentes.
2. **Respuesta a Incidentes:**
    - **Notificación de Incidentes**: Establecer procedimientos para la notificación inmediata de incidentes al equipo de respuesta.
    - **Evaluación del Incidente:** El equipo debe evaluar rápidamente el alcance y el impacto del incidente.
3. **Contención, Erradicación y Recuperación:**
    - **Contención:** Tomar medidas inmediatas para limitar el alcance del incidente.
    - **Erradicación:** Identificar y eliminar la causa del incidente.
    - **Recuperación:** Restaurar los sistemas a su operación normal y confirmar que el sistema está libre de amenazas.
4. **Comunicación:**

- **Comunicación Interna y Externa:** Mantener comunicación constante con las partes interesadas, incluyendo empleados, clientes y, si es necesario, el público.

5. **Análisis Post-Incidente:**
    - **Análisis:** Revisar y analizar el incidente para entender qué sucedió y por qué.
    - **Lecciones Aprendidas:** Identificar mejoras en los procesos y estrategias para prevenir incidentes futuros.
6. **Actualización del Plan de Recuperación:**
    - **Revisión del Plan**: Actualizar el plan de recuperación de incidentes basándose en las lecciones aprendidas.
7. **Entrenamiento y Simulacros:**
    - **Capacitación Regular:** Capacitar al personal en la identificación y manejo de incidentes de ciberseguridad.
    - **Ejercicios de Simulación:** Realizar simulacros periódicos para probar y mejorar la efectividad del plan.

Documentación del Plan: El plan debe estar documentado de manera detallada y accesible para todos los miembros relevantes de la organización. Debe incluir:

- Procedimientos y protocolos de respuesta.
- Listado de contactos del equipo de respuesta a incidentes.
- Guías para la comunicación durante un incidente.
- Plantillas y formularios para la documentación de incidentes.

Caso 16: Diseño de un Programa de Concienciación en Ciberseguridad

Organización Seleccionada: Para este caso, continuaremos utilizando la organización ficticia "GreenChayote Exporters".

Información Principal de "GreenChayote Exporters":

- **Áreas de negocio:** Exportación de chayotes**.**
- **Líneas de servicio:** Logística, gestión de cadena de suministro, ventas.
- **Datos sensibles y personales:** Información de clientes, datos logísticos, detalles de transacciones.
- **Infraestructura TIC:** Sistemas de gestión de cadena de suministro (SCM), ERP, redes internas y externas, bases de datos.

Programa de Concienciación en Ciberseguridad:

1. **Evaluación Inicial y Definición de Necesidades (Mes 1):**
    - Realizar una evaluación inicial para identificar el nivel de conocimiento de ciberseguridad en la empresa.
    - Definir las necesidades específicas de capacitación basadas en el perfil de los empleados y la naturaleza del negocio.
2. **Desarrollo de Materiales Educativos (Meses 2-3):**
    - Crear materiales de formación adaptados a las necesidades identificadas, incluyendo guías, videos, y presentaciones interactivas.
    - Incluir temas como seguridad de la información, protección contra malware, seguridad en correos electrónicos y redes sociales, y buenas prácticas de seguridad digital.
3. **Implementación de la Capacitación (Meses 4-6):**
    - Lanzar sesiones de capacitación en línea y presenciales.
    - Realizar talleres y seminarios interactivos para involucrar a los empleados en escenarios prácticos de ciberseguridad.
4. **Evaluación y Refuerzo Continuo (Meses 7-12):**
    - Evaluar la efectividad de la capacitación mediante pruebas y encuestas.
    - Implementar un plan de refuerzo continuo que incluya recordatorios periódicos, actualizaciones de seguridad y formación adicional según sea necesario.
5. **Programa de Concienciación Continua (Anual):**
    - Planificar actualizaciones anuales del programa para abordar nuevas amenazas y tendencias en ciberseguridad.
    - Incluir sesiones de actualización y reciclaje para todos los empleados.

Comunicación y Participación:

- Comunicar regularmente la importancia de la ciberseguridad a través de boletines internos, correos electrónicos y reuniones.
- Incentivar la participación activa de los empleados en el programa de concienciación.