Escuela Politécnica Nacional

Objetivo:

- Realizar el análisis de riesgos de un proceso de negocio de una organización hipotética usando la metodología OCTAVE.
- Desarrollar habilidades de búsqueda y utilización de recursos de terceros, incluida información en la web, para la resolución de problemas relacionados con el análisis de riesgos.

Procedimiento:

- En la sección 1 se provee la descripción de un proceso de negocio que servirá como base para realizar el análisis de riesgos.
- Usted deberá responder a las preguntas/peticiones presentadas en la sección 2, presentar las hojas de trabajo, **explicaciones y supuestos** realizados que justifiquen sus respuestas.
  - Para realizar el análisis vamos a asumir una "**postura conservadora[1]"**, asumiendo que cualquier evento (ataque, amenaza, etc.) es factible.
  - Si cree que la descripción del proceso de negocio no es completa, podrá complementarlo con elementos adicionales que permitan justificar su respuesta.
- Debe subir al aula virtual **un solo PDF** con todas las respuestas generadas.

1. Proceso de negocio hipotético

La Unidad Médico Familiar (Unimedfam) es un consultorio general que provee primer nivel de atención de salud (categoría I-2). Unimedfam presta atención de diagnóstico y/o tratamiento de medicina general, obstetricia, odontología general y psicología, y exámenes de laboratorio.

Unimedfam tiene su matriz ubicada en el sector de El Inca y cuatro sucursales (Calderón, San Carlos, Pomasqui y San Isidro). Esta organización incluye las siguientes áreas funcionales:

- Gestión de la entidad de salud
- Gestión del personal de la entidad de salud, incluyendo a los médicos, auxiliares, técnicos de laboratorio, odontólogos, obstetricia, etc.
- No tiene un departamento de TI, aunque una persona (ingeniero en TI) esporádicamente es responsable del mantenimiento de las estaciones de trabajo y de la red; además brinda soporte (help desk) ante peticiones puntuales del personal

1.1. Estructura de la organización Unimefam

Diego Ortega es el administrador de Unimedfam, Liz Gutiérrez es la jefa del personal de salud y Edwin Rojas el jefe del laboratorio. Estos dos últimos reportan la situación de sus areas a Diego Ortega, aunque los tres son accionistas y conforman el Comité de Unimedfam (máxima entidad que toma las decisiones de la organización).

- Diego Ortega se encarga de la gestión de todos los consultorios médicos, la gestión del personal de mantenimiento y de contactar al Ing. en TI cuando sea necesario.
- Liz Gutiérrez se encarga del monitoreo de las atenciones médicas realizadas por el personal médico tanto en los consultorios médicos como en las visitas a domicilio.

[1] La postura conservadora o pesimista, asume que cualquier evento que atente a la seguridad de un activo crítico es posible.

- Edwin Rojas se encarga del monitoreo concerniente a la toma de muestras para los exámenes del laboratorio. UnimedFam se encarga de las analíticas sanguíneas, aunque PomasquiLab se encarga de las pruebas PCR y MediLab se encarga de Rayos X. Estas dos últimas son empresas externas.

1.2. Gestión médica y de laboratorios

Unimedfam no maneja un sistema con propósitos específicos, sino que usa Google Drive para crear las historias clínicas de los pacientes. Los médicos usan estaciones de trabajo ubicadas dentro de las instalaciones de UniMedFam para acceder a estas historias clínicas cuando sea necesario, y una Tablet para cuando tienen que hacer visitas a domicilio. Cada estación de trabajo es compartida por el personal médico de turno. La sesión con Google Drive siempre está activa, aunque cada estación de trabajo tiene un usuario y contraseña compartida por los médicos.

- En el consultorio médico matriz, varios médicos rotan a lo largo de la semana. En las sucursales atiende el mismo personal y esporádicamente van médicos de reemplazo.

La información de salud de cada paciente es actualizada en un documento de Google Drive desde las estaciones de trabajo. Las estaciones de trabajo están ubicadas en los consultorios médicos y laboratorio. Cuando un médico hace una visita a domicilio necesariamente accede a las historias clínicas a través de la Tablet disponible. El administrador de Unimedfam (Diego Ortega) es el único que puede acceder a las historias clínicas desde su computador personal (eventualmente es el único que conoce las credenciales de acceso).

Hay una persona externa dedicada a la gestión de TI a la que se acude cada vez que se necesita su soporte. Esta persona se encarga del mantenimiento de la red y estaciones de trabajo. Esta persona también brinda soporte cada vez que el personal lo requiere.

Ciertos exámenes de laboratorio son provistos por laboratorios externos (PomasquiLab y MediLab). Auxiliares de estos laboratorios van diariamente al laboratorio a recoger las muestras tomadas por personal de Unimedfam.

El comité de Unimefam ha decidido llevar a cabo una evaluación de riesgos de seguridad en su organización, dado que tienen dos años para alinear sus procesos a los requisitos establecidos en la Ley Orgánica de Protección de Datos Personales. Ellos han decidido usar OCTAVE-S para llevar a cabo este análisis.

2. Información solicitada (todas las respuestas deben ser justificadas con una explicación breve y concisa)

2.1. ¿Quién, en su opinión, debería formar parte del equipo de análisis? Defina explícitamente los integrantes junto con la justificación.

2.2. Defina al menos un criterio de evaluación de impacto para, al menos, dos categorías propuestas por OCTAVE.

2.3. Identifique los activos de los procesos de negocio de la organización, señalando explícitamente su tipo.

2.4. Seleccione el activo que, en su opinión, es el más crítico y elabore el árbol de amenazas únicamente para accesos humanos (físico y a través de la red)