A[8] Celonis, ProM, bupaR o pm4py

Objetivo

El proceso crítico de la empresa "¡Te atrapé!" es **"Responder ante brecha de seguridad"**.

El objetivo de esta tarea es analizar logs de eventos de este proceso de negocio, para descubrir y analizar su funcionamiento aplicando técnicas de Minería de Procesos utilizando Celonis, ProM, pm4py o BupaR. Puedes basarte en las demos realizadas para cada uno de ellos al responder las preguntas de esta actividad.

Datos

Se cuenta con dos logs de eventos correspondientes a la ejecución del proceso:

- **log_gestionar_alarma_1.csv**: contiene registros de ejecuciones del proceso en los turnos diurnos (7:00h-15:00h, 15:00h-23:00h).
- **log_gestionar_alarma_2.csv**: contiene registros de ejecuciones del proceso en el turno nocturno (23:00h-7:00h).

El proceso y los datos provistos han sido específicamente **generados** para probar las técnicas de Minería de Procesos, por lo que los logs de eventos son más simples que el log de eventos de un proceso real. Sin embargo, te permitirán entender cómo funcionan las herramientas y algoritmos para realizar Minería de Procesos.

Una descripción más detallada del proceso puede encontrarse a continuación. Léela con detención antes de responder las preguntas de la actividad. Sin embargo, mayor detalle del funcionamiento del proceso deberás determinarlo a partir del análisis respectivo.

Proceso "Responder ante brecha de seguridad"

En el condominio "Vivir muy seguros", los vecinos se han organizado para tener un doble sistema de seguridad, el que tiene cada propiedad y una alarma comunitaria. La idea es que actúen de manera integrada ante la ocurrencia de cualquier brecha de seguridad. Tienen contratada una empresa de seguridad única que presta ambos servicios, "¡Te atrapé!", que aporta la tecnología de seguridad para las alarmas domiciliarias y la alarma comunitaria. Una de las características es que busca evitar que los intrusos ingresen a las casas, por lo que cuentan con sensores, luces perimetrales y cámaras de vigilancia que pueden ser monitoreadas de manera remota, y reducir la cantidad de activaciones de alarma (se sabe que si suenan alarmas todas las noches, la gente deja de tomarlas en cuenta).

El protocolo que tienen definido ante una brecha de seguridad es el siguiente:

Cuando se activa algún sensor de movimiento en el exterior de una casa, se prenden luces perimetrales en dicha vivienda y se envía una señal a la central de monitoreo. Un asistente de seguridad revisa todas las cámaras hasta identificar la acción que activó la alarma. Si es un hecho fortuito (un animal doméstico, movimiento de vegetación por el viento, una polilla o similar, entre otros), envía un mensaje al vecino correspondiente a través del App de la empresa. Si luego de 5 minutos no detecta nada, también envía un mensaje al vecino a través de la App de la empresa, solicitando revise su alarma. Si, en cambio, observa el movimiento de una persona, activa un micrófono ambiental y exclama "¡Te atrapé!". Si es una persona de la casa, dicha persona debe hacer una señal convenida a la cámara, y luego debe ir hasta la alarma e ingresar un código de seguridad. Cuando el asistente de seguridad constata el correcto uso del código de seguridad, simplemente registra la activación errónea en el sistema. Si es un intruso o no hace caso al primer contacto, el asistente continúa dándole mensajes disuasivos, alerta a un móvil de seguridad de la empresa para que concurra al lugar, y activa la alarma sonora de la casa afectada.

Si luego de 60 segundos el asistente de seguridad no logra que el intruso abandone la propiedad, activa la alarma comunitaria, indicando a través de la App cuál es el número de la propiedad afectada, luego escala el nivel de urgencia al móvil de seguridad, y, finalmente, contacta a Seguridad Ciudadana de la comuna. Tras esto último, el asistente de seguridad sigue buscando disuadir al intruso, a la vez que monitorea todas las cámaras de la propiedad afectada y sus vecinos. Mantiene lo anterior hasta que el móvil de seguridad llega a su destino. Por su parte, cada uno de los vecinos entra en acción, esto es, sale de su casa haciendo ruido y tocando silbatos, y se dirige a la casa afectada. No se pretende detener al intruso con las acciones de los vecinos, debido al riesgo que eso significa. Más bien, el objetivo que se busca es que el intruso arranque del lugar, se lleve un buen susto, y no vuelva a intentar entrar al condominio.

Una vez que el móvil de seguridad llega hasta el domicilio afectado, el guardia de seguridad a bordo toma contacto con el dueño de casa y luego comunica a la central que ya se encuentra en el lugar, por lo que toma el control de la situación. Ya en contacto con el guardia de seguridad, el dueño de casa procede a desconectar su alarma. Si se activó la alarma comunitaria, el dueño de casa también debe desconectar la alarma comunitaria. Además, se invita a los vecinos a regresar a sus viviendas, y revisar que todo esté en orden en sus casas. Finalmente, junto al guardia de la empresa, el dueño de casa recorre el lugar para revisar que no hayan ocurrido daños.

Finalmente, el guardia se comunica con la central de monitoreo, para finalizar el operativo.

Nota: la descripción que aquí aparece es sólo una referencia; podría variar con el proceso real.

Análisis

1. Análisis exploratorio

Análisis individual. Para cada log de eventos, haz un análisis exploratorio (esto es, antes de aplicar ningún filtro) y descríbelo en base a las siguientes preguntas.

- ¿Cuántas ejecuciones del proceso (casos) contiene el log de eventos?
- ¿A qué período de tiempo corresponde?
- ¿Cuáles son las actividades que se realizan más a menudo o menos a menudo?
- ¿Con qué actividad se inicia el proceso? ¿Con qué actividades termina el proceso?
- ¿Cuántas variantes existen?
- ¿Cuáles son los ejecutores que participan realizando más actividades o menos actividades?
- ¿Cuál es el tiempo (mediana / promedio) que tarda el proceso en ejecutarse?
- ¿Están todos los casos completos? Justifica tu respuesta.

Análisis comparativo. Compara ambos logs de eventos respecto a las distintas dimensiones analizadas.

- ¿Qué diferencias observas?

2. Descubrimiento de proceso – general

Análisis individual. Para cada log de eventos, analiza los modelos obtenidos con la herramienta y describe cómo se está ejecutando el proceso según ellos.

- Incluye al menos tres diagramas del proceso
    - Incluye un diagrama del proceso mostrando todo el comportamiento posible.
    - Incluye en un diagrama los casos que terminan sin requerir la concurrencia de un móvil.
    - Incluye en otro diagrama los casos que requieren la concurrencia de un móvil.
    - Para ello, filtra los casos según actividad final.
- ¿El comportamiento es el esperado?

Análisis comparativo. Compara ambos logs de eventos respecto a las distintas dimensiones analizadas.

- ¿Qué diferencias observas?

3. Filtrar log de eventos

Análisis individual. Para cada log de eventos, filtra el log y analiza los modelos obtenidos con la herramienta y describe cómo se está ejecutando el proceso según ellos.

- Completa la **Tabla 1** para describir la frecuencia de ocurrencia de distintos tipos de casos.
    - Puede serte útil filtrar actividades específicas o caminos específicos.

Tabla 1. Frecuencia de ocurrencia de distintos tipos de casos

Tipo de caso	Frecuencia Log 1	Frecuencia Log 2
Hecho fortuito		
Hecho no precisado		
Persona de la casa		
Intruso – no se requiere alerta comunitaria		
Intruso – se requiere alerta comunitaria		
Total		

- Compara la ejecución del proceso para cada uno de los tipos de casos descritos en la Tabla 1.
    - Incluye un diagrama del proceso resultante.
    - Describe los filtros aplicados, y describe los modelos resultantes.
    - ¿Se filtraron ejecutores?
    - ¿Cuántas variantes quedan?
    - ¿Se ejecuta el proceso de acuerdo a lo esperado?
    - ¿Cuál es la proporción de casos en relación al total?
    - ¿Te parece razonable lo observado en los distintos modelos?

Análisis comparativo. Compara ambos logs de eventos filtrados.

- ¿Qué diferencias observas?
- ¿Te parecen razonables?

Observación

El resultado de tu análisis deberá estar fundamentado. Por lo tanto, dado que se ha definido explícitamente qué debes hacer, tu mayor aporte deberá ser el análisis que pueda hacer de los resultados. Por simplicidad, al menos que se te pida explícitamente, utiliza los parámetros por defecto de todos los algoritmos.

Formato del entregable

Se espera que cada estudiante/grupo entregue un informe en formato PDF que muestre el análisis realizado y los resultados obtenidos (pantallazos obtenidos con la herramienta seleccionada). Para cada pregunta, responde combinando textos explicativos e imágenes (pantallazos mencionados anteriormente y otros que consideres conveniente para justificar su análisis). Debe quedar explícito el origen de los resultados en el informe (pantallazos del código en el caso de bupaR y pm4py, pantallazos del software en el caso de Celonis y ProM), pues la ausencia de esto en el informe provocará el descuento de puntaje en las preguntas correspondientes.

Entrega el informe en formato PDF a través del buzón habilitado para esta actividad en Canvas.

Forma de evaluación

El entregable será evaluado de acuerdo con los siguientes criterios:

1. Buen uso de las herramientas de Minería de Procesos.
2. Capacidad de interpretación de los resultados obtenidos con las herramientas utilizadas.
3. Capacidad de análisis que considere los distintos aspectos de un proceso de negocio.
4. Presentación y pulcritud, es decir, que el trabajo no tenga errores de forma (ortografía, redacción, orden, etc.)

Ojo: cualquier sospecha de copia será sancionada de acuerdo con los criterios establecidos en el programa del curso.

Notas acerca del trabajo

1. El trabajo puede ser realizado en forma individual (solo los análisis individuales para el primer log de eventos) o en grupos de **dos** estudiantes (incluir análisis comparativos considerando ambos logs de eventos).
2. El plazo para entregar la tarea es hasta el **miércoles 18 de mayo antes de las 23:55 horas**, a través de Canvas.