Análisis de riesgos.

Para realizar este análisis de riesgos vamos a tomar en cuenta cada uno de los procesos que se realizan dentro de la aplicación y cada una de sus partes.

Dentro de los riesgos asociados a los usuarios tipo “admin” tenemos, la filtración de las credenciales, esto podría resultar en la eliminación de usuarios tipo “requesters” afectando la accesibilidad a la información para terceros. Podría generar la eliminación de restricciones, esto puede comprometer la integridad de la información.
La información de las credenciales de un administrador es confidencial, su acceso solo se permite al personal interno autorizado. Si la información de las credenciales de un administrador es filtrada a personal no autorizado, podría llevar a una magnitud de daño alta (pérdida de información, elevación de privilegios, negación de servicios) el interés por parte de individuos externos es alto. El impacto del daño lo recibe la empresa y terceros, generando costos de pérdida de confiabilidad y recursos de información.
Las restricciones son de carácter sensible, se permite su acceso a personal interno y público con permiso. Si estas restricciones son filtradas para personal no autorizado, podría llevar a una magnitud de daño baja, el interés por parte de terceros es bajo. El impacto es bajo y quien lo recibe es la empresa, existirían pérdidas de confiabilidad de la empresa.

Pensando en los riegos asociados con los usuarios de tipo “requesters”, observamos que si existe una filtración en las credenciales de este tipo de usuario, se podría ingresar a los datos confidenciales de ubicación, nombre, información de tarjeta de crédito, entre otros, de los clientes.
La información de los clientes contiene PCI su acceso se permite a personal interno y público autorizado. Si la información de PCI de un cliente es filtrada a personal no autorizado, podría llevar a una magnitud de daño alta (suplantación, daños económicos) el interés por parte de individuos externos es alto. El impacto del daño lo recibe la empresa y terceros, generando costos de pérdida de confiabilidad en la empresa, pérdidas económicas de la empresa, daños emocionales a terceros, daños económicos a terceros.

En los riesgos asociados con la base de datos, existe el riesgo de que la máquina que sirve como host para la base de datos sea intervenida de manera física o digital que comprometería toda la operación. La magnitud del daño es alta (destrucción de información, denegación de servicios, elevación de privilegios, robo de información, suplantación de identidad) el interés por parte de terceros es algo. El impacto del daño lo recibe la empresa y terceros, generando costos de pérdida de confiabilidad en la empresa, pérdidas económicas de la empresa, daños emocionales a terceros, daños económicos a terceros, recursos de información de la empresa.