# Análisis de Riesgos

## Escenario 1: puntos de carga configurados en zonas abiertas

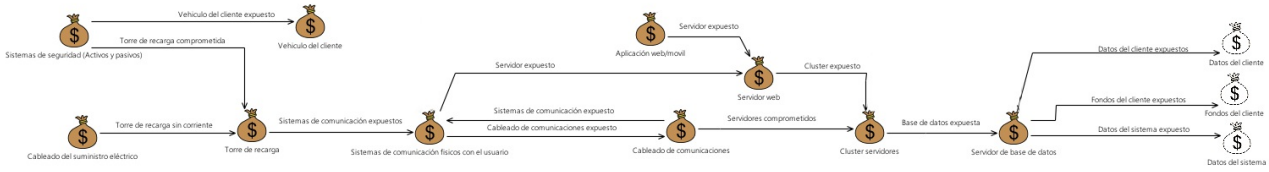
- **Área físico en el que se desarrolla el punto de carga**:
    - Grados de aislamiento y control: El aislamiento en este caso es nulo en cuanto a barreras físicas, tan solo existen medidas de seguridad pasivas o de supervisión monitorizadas.
    - Facilidad de acceso al área: Al tratarse de zonas abiertas, la facilidad de acceso es total.
    - Entorno: Al ser una zona abierta, las amenazas directas que requieran presencia física son más fáciles de llevar a cabo.
- **Comunicación entre el cliente y el punto de carga**:
    - Modos de acceso:
        - RFID / NFC: Funcionalidad incluida en los últimos smarthphones que permite una comunicación a muy corta distancia y que puede servir como identificación del usuario al ser este el portador univoco del dispositivo. Una ventaja es que hace las veces de clave física. Una desventaja podría ser que dispositivos más antiguos no tuvieran soporte para esta tecnología.
        - OTP (One Time Password): Método de autenticación basado en un envío de una contraseña temporal al usuario, por norma general, vía SMS, email...
        - Usuario / Contraseña: Sistema de identificación más popular y extendido hoy día.
        - QR Code: Similar a la identificación OTP, con la diferencia que el usuario no ha de leer / memorizar ningún código, siendo el móvil el que realiza esta actividad.
        - Huella dactilar: Sistema de seguridad biométrica basada en las hendiduras de las huellas dactilares de los dedos de la manos. Una ventaja es que el usuario no necesita ningún soporte. Un posible inconveniente es que habría que ajustar el equilibrio entre facilidad de acceso y seguridad de identificación.
- **El tipo de comunicación entre los diferentes actores y el sistema de control**:
    - **Listado de actores**:
        - Personal de mantenimiento.
        - Clientes (a través de interfaces web o móvil).
        - Puntos de carga.
        - Proveedores de energía.
        - Servidores.
    - **Obervaciones sobre las comunicaciones actor-sistema**: El hecho de que las comunicaciones se realicen a través de internet puede conllevar posibles ataques remotos. En el caso de las comunicaciones que usen tecnologías inalámbricas,

estos ataques serían más accesibles para los supuestos atacantes y más difíciles de detectar; mientras que en el caso de comunicaciones por cable, el ataque deviene más complejo, aunque no imposible.

## Escenario 2: puntos de carga configurados en zonas cerradas

- **Área físico en el que se desarrolla el punto de carga**:
    - Grados de aislamiento y control: El grado de aislamiento es superior al que podemos encontrar en los escenarios del primer tipo, lo que hace más fácil el control de acceso y puede perjudicar las comunicaciones inalámbricas.
    - Facilidad de acceso al área: Si la zona cerrada en concreto incluye un sistema de seguridad para el acceso, se limitaría el rango de actores humanos que podrían acceder a este servicio.
    - Entorno: Un entorno cerrado supone un mayor grado de aislamiento en cuanto a amenazas directas.
- **Comunicación entre el cliente y el punto de carga**:
    - Los medios de comunicación entre el cliente y el punto de carta en este tipo de escenario no difiere con los del primero.
- **El tipo de comunciación entre los diferentes actores y el sistema de control**:
    - Al igual que en el caso de las comunicaciones entre el cliente y los puntos de carga, no hay mucho que decir en cuanto a las comunicaciones entre actores y el sistema de control que no se haya dicho ya en los escenarios del tipo 1.
    - Un posible matiz a tener en cuenta: si el punto de carga se trata de uno privado, instalado en una propiedad privada y para uso de un único individuo propietario, se podrían evadir amenazas en cuanto a los métodos de identificación.

## Assets:




- **Físicos**:
    - Torre de recarga.
    - Cableado de comunicaciones.
    - Cableado eléctrico.
    - Suministro eléctrico (comunicación unidireccional).
    - Terminal.
    - Cluster servidores.
    - Vehículo del cliente.
    - Sistemas de seguridad (activos y pasivos).
    - Sistemas de comunicación con el usuario (lector de tarjetas y de NFC).
    - Dispositivos de comunicación (dispositivos móviles, tarjetas de crédito/débito).
- **Digitales**:

    - Datos del cliente (datos de pago, datos de consumo, datos personales).
    - Datos de sistema (datos de pago, datos de consumo, datos personales).
    - Servidor web.
    - Servidor base de datos.
    - Aplicación móvil.
    - Aplicación web.

# Amenazas:

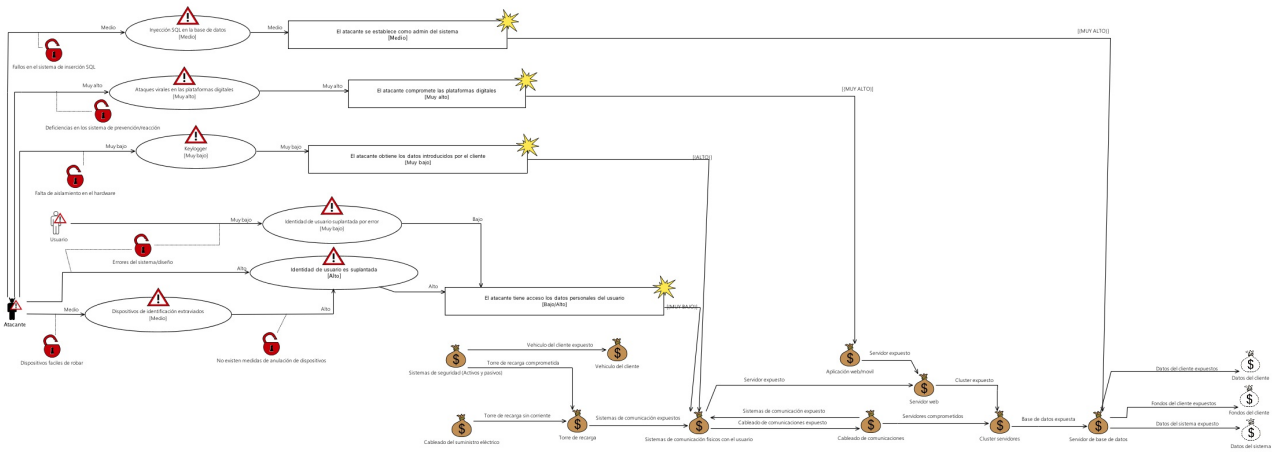
- **Directas**:
    - Corte del suministro eléctrico.
    - Destrozo por tercero.
    - Suplantación voluntaria de identidad.
    - Keyloggers.
    - Ataques virales.
    - Inyección SQL.
    - Session hijacking.
    - Vectores de ataque web.
    - Ataque DDoS.
- **Indirectas**:
    - Suplantación involuntaria.
    - Inclemencias metereológicas (tormentas).
    - Desastres naturales (movimientos sísmicos, maremotos...).
    - Sistemas de almacenamiento deteriorados.
    - Cuello de botella en la conexión servidor-aplicaciones.
    - Error en el servicio debido a operaciones de mantenimiento.
    - Pérdida de dispositivos de identificación.

# Vulnerabilidades

- Fallos en el sistema de parseado de sentencias SQL.
- Deficiencias en los sistemas de prevención/reacción.
- Falta de aislamiento en el hardware.
- Errores del sistema/diseño.
- Dispositivos fáciles de robar.
- No existen medidas de anulación de dispositivos.
- Sistema de respaldos durante mantenimiento inexistente.
- Falta de mantenimiento.
- Control de acceso ineficiente.
- Ausencia de firewall.
- Aislamiento insuficiente.
- Sistema eléctrico inseguro.

# Amenazas a la Confidencialidad

## Diagrama de amenazas




## Lista de amenazas

1. Suplantación voluntaria de identidad

- Descripción: el atacante consigue hacerse pasar, de forma fraudulenta, por un usuario sin consentimiento ni conocimiento por parte de éste, con la finalidad de acceder a los datos o assets del sistema.
- Impacto de riesgo: **bajo**
- Probabilidad de riesgo: **alta**
- Plan de contingencia y prevención: anulación del dispositivo o clave de identificación afectado por el ataque. Expedición de un nuevo dispositivo de identificación.

2. Keyloggers

- Descripción: uso de un programa que guarda silenciosamente en un log cualquier pulsación de teclas que se lleve a cabo en la máquina de la víctima.
- Impacto de riesgo: **bajo**
- Probabilidad de riesgo: **muy baja**
- Plan de contingencia y prevención: aislamiento inmediato de la máquina afectada y análisis y limpieza posterior. Ofrecer formación a los empleados/usuarios de las máquinas.

3. Ataques virales

- Descripción: inyección de código malicioso en la máquina víctima con el fin de hacerse con el control de ésta de cualquier manera (trojans, worms, keyloggers...), con la intención de acceder a los datos o assets del sistema.
- Impacto de riesgo: **muy alto**
- Probabilidad de riesgo: **muy alta**
- Plan de contingencia y prevención: aislamiento inmediato de la máquina afectada y análisis y limpieza posterior. Ofrecer formación a los empleados/usuarios de las máquinas.

4. Inyección SQL

- Descripción: uso de scripts específicos de SQL con el fin de engañar al procesador de dichas sentencias y conseguir ejecutar una sentencia no autorizada en el servidor de la base de datos, pudiendo así insertar, modificar o eliminar datos de ésta.
- Impacto de riesgo: **muy alto**
- Probabilidad de riesgo: **media**

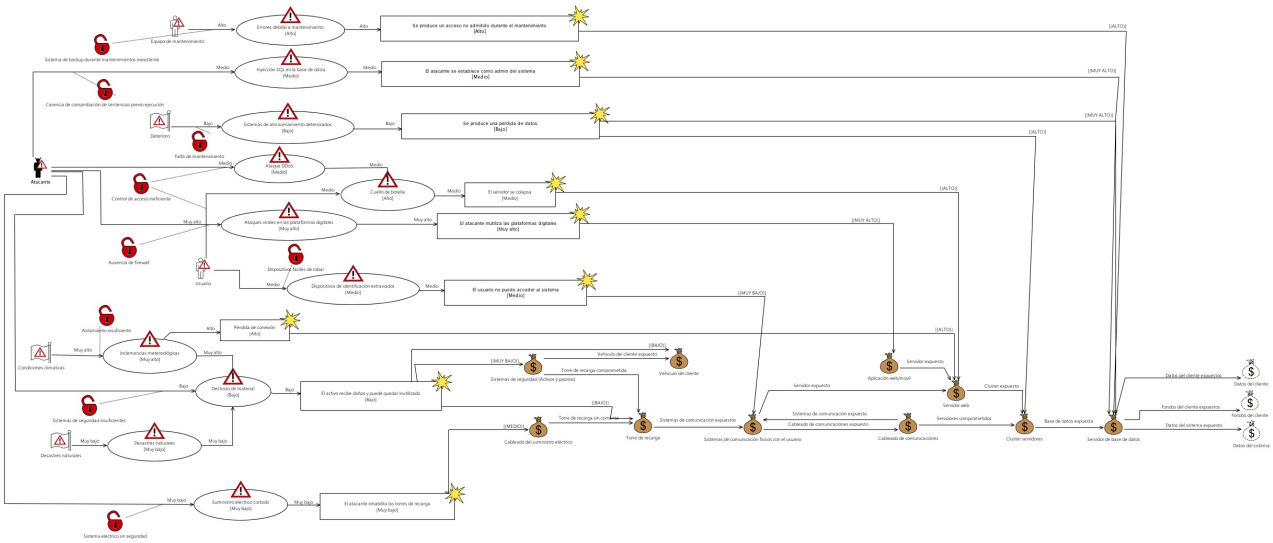
- Plan de contingencia y prevención: isolación de la base de datos inmediata y arreglo del sistema de parseo de sentencias SQL. Comprobación previa a ejecución de los campos introducidos por el usuario en busca de posibles intentos de explotación.

### Matriz P-I

| Impacto \ Probabilidad | Muy alto | Alto | Medio | Bajo | Muy bajo |
|---|---|---|---|---|---|
| Muy Alto | 3 | – | 4 | – | – |
| Alto | – | – | – | – | – |
| Medio | – | – | – | – | – |
| Bajo | – | 1 | – | – | 2 |
| Muy Bajo | – | – | – | – | – |

## Amenazas a la Disponibilidad

### Diagrama de amenazas



### Lista de amenazas

1. Corte del suministro eléctrico

- Descripción: si se consiguiese bloquear la conexión, mediante un corte en el suministro eléctrico, entre el SmartGrid y el servidor, el atacante podría interferir en dicha comunicación, modificando, robando o llevando a cabo cualquier otra finalidad que le interese.
- Impacto de riesgo: **medio**
- Probabilidad de riesgo: **muy baja**
- Plan de contingencia y prevención: instalación de generadores de energía dedicados a la alimentación de los servidores. Establecer un sistema de comprobación de cortes en el suministro eléctrico que cambie la fuente de alimentación a la ofrecida por dichos generadores.

2. Destrozo por tercero

- Descripción: cualquier daño producido en el sistema por la actuación física de un atacante.

- Impacto de riesgo: **bajo**
- Probabilidad de riesgo: **baja**
- Plan de contingencia y prevención: arreglo de las instalaciones afectadas. Asegurar las instalaciones con aseguradoras.

3. Ataques virales

- Descripción: inyección de código malicioso en la máquina víctima con el fin de hacerse con el control de ésta de cualquier manera (trojans, worms, keyloggers...), con la finalidad de impedir el uso de cualquier servicio que ofrezca el sistema.
- Impacto de riesgo: **muy alto**
- Probabilidad de riesgo: **muy alta**
- Plan de contingencia y prevención: aislamiento inmediato de la máquina afectada y análisis y limpieza posterior. Ofrecer formación a los empleados/usuarios de las máquinas.

4. Inyección SQL

- Descripción: uso de scripts específicos de SQL con el fin de engañar al procesador de dichas sentencias y conseguir ejecutar una sentencia no autorizada en el servidor de la base de datos, pudiendo así insertar, modificar o eliminar datos de ésta.
- Impacto de riesgo: **muy alto**
- Probabilidad de riesgo: **media**
- Plan de contingencia y prevención: isolación de la base de datos inmediata y arreglo del sistema de parseo de sentencias SQL. Comprobación previa a ejecución de los campos introducidos por el usuario en busca de posibles intentos de explotación.

5. Ataque DDoS

- Descripción: ataque consistente en el envío repetitivo y masivo de paquetes de red a un servidor que esté expuesto, de manera que éste se sobrecarge y no sea capaz de responder peticiones legítimas.
- Impacto de riesgo: **muy alto**
- Probabilidad de riesgo: **media**
- Plan de contingencia y prevención: uso de firewalls o servicios de terceros, como CloudFlare (https://www.cloudflare.com/), que eviten las ocurrencias de dichos ataques.

6. Inclemencias metereológicas

- Descripción: daños producidos en las interfaces físicas debido a desgaste, erosión, por el clima.
- Impacto de riesgo: **bajo**
- Probabilidad de riesgo: **muy alta**
- Plan de contingencia y prevención: arreglo de las instalaciones afectadas. Asegurar las instalaciones con aseguradoras.

7. Desastres naturales (movimientos sísmicos...)

- Descripción: daños producidos en las interfaces físicas debido a condiciones naturales extremas.
- Impacto de riesgo: **muy alto**
- Probabilidad de riesgo: **muy baja**
- Plan de contingencia y prevención: arreglo de las instalaciones afectadas. Asegurar las instalaciones con aseguradoras.

8. Error en el servicio debido a operaciones de mantenimiento

- Descripción: errores de consistencia e integración entre componentes del sistema introducidos por operaciones de desarrollo o mantenimiento del mismo.
- Impacto de riesgo: **alto**
- Probabilidad de riesgo: **alta**
- Plan de contingencia y prevención: bloquear el uso de las aplicaciones de cliente o terminales durante las operaciones de mantenimiento. Información previa a los usuarios de cuándo se establecerán dichas operaciones.

9. Pérdida de dispositivos de identificación

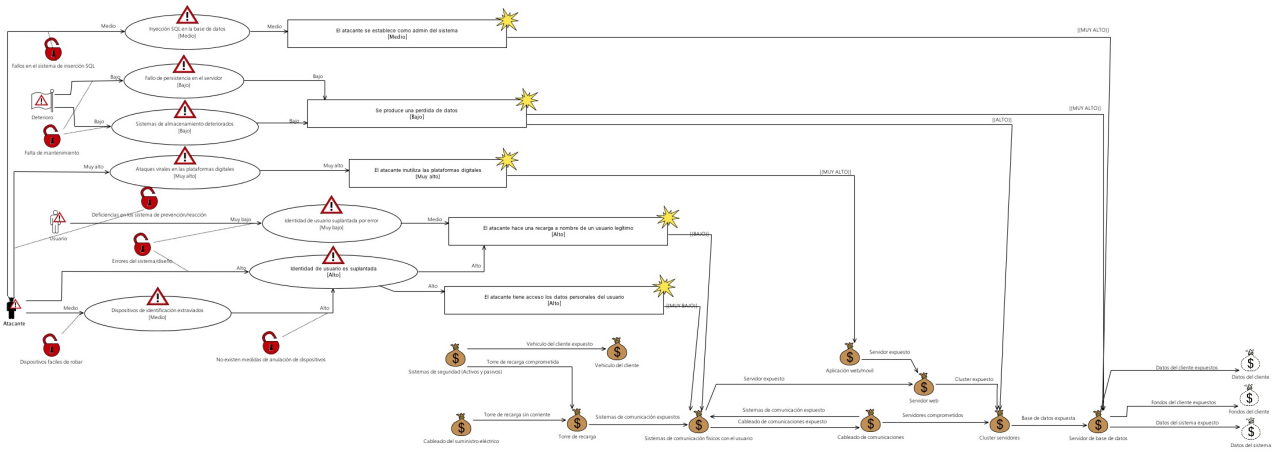
- Descripción: pérdida por parte del usuario de cualquier artefacto que le sirva para identificarse en el sistema (contraseña, tarjeta identificativa...).
- Impacto de riesgo: **muy bajo**
- Probabilidad de riesgo: **media**
- Plan de contingencia y prevención: anulación del dispositivo o clave de identificación afectado por el ataque. Expedición de un nuevo dispositivo de identificación.

### Matriz P-I

| Impacto \ Probabilidad | Muy alto | Alto | Medio | Bajo | Muy bajo |
|---|---|---|---|---|---|
| Muy Alto | 3 | – | 4, 5 | – | 7 |
| Alto | – | 8 | – | – | – |
| Medio | – | – | – | – | 1 |
| Bajo | 6 | – | – | 2 | – |
| Muy Bajo | – | – | 9 | – | – |

## Amenazas a la Integridad

### Diagrama de amenazas




### Lista de amenazas

1. Suplantación voluntaria de identidad

- Descripción: el atacante consigue hacerse pasar, de forma fraudulenta, por un usuario con permisos elevados sin consentimiento ni conocimiento por parte de éste, con la finalidad de modificar el correcto funcionamiento del sistema.

- Impacto de riesgo: **bajo**
- Probabilidad de riesgo: **alta**
- Plan de contingencia y prevención: anulación del dispositivo o clave de identificación afectado por el ataque. Expedición de un nuevo dispositivo de identificación.

2. Suplantación involuntaria

- Descripción: la identidad de los usuarios se ve alterada por un error en el sistema, haciendo que el usuario no tenga acceso a sus datos.
- Impacto de riesgo: **muy bajo**
- Probabilidad de riesgo: **muy baja**
- Plan de contingencia y prevención: anulación del dispositivo o clave de identificación afectado por el ataque. Expedición de un nuevo dispositivo de identificación. Corrección de errores.

3. Ataques virales

- Descripción: inyección de código malicioso en la máquina víctima con el fin de hacerse con el control de ésta de cualquier manera (trojans, worms, keyloggers...), con la finalidad de introducir malfuncionalidades en el sistema.
- Impacto de riesgo: **muy alto**
- Probabilidad de riesgo: **muy alta**
- Plan de contingencia y prevención: aislamiento inmediato de la máquina afectada y análisis y limpieza posterior. Ofrecer formación a los empleados/usuarios de las máquinas.

4. Inyección SQL

- Descripción: uso de scripts específicos de SQL con el fin de engañar al procesador de dichas sentencias y conseguir ejecutar una sentencia no autorizada en el servidor de la base de datos, pudiendo así insertar, modificar o eliminar datos de ésta.
- Impacto de riesgo: **muy alto**
- Probabilidad de riesgo: **media**
- Plan de contingencia y prevención: isolación de la base de datos inmediata y arreglo del sistema de parseo de sentencias SQL. Comprobación previa a ejecución de los campos introducidos por el usuario en busca de posibles intentos de explotación.

5. Fallo de persistencia

- Descripción: error en las operaciones de guardado o sincronización de datos entre las aplicaciones y el servidor de base de datos.
- Impacto de riesgo: **muy alto**
- Probabilidad de riesgo: **baja**
- Plan de contingencia y prevención: isolación de la base de datos inmediata y arreglo de los errores. Creación periódica de backups.

## Matriz P-I

| **Impacto \ Probabilidad** | **Muy alto** | **Alto** | **Medio** | **Bajo** | **Muy bajo** |
|---|---|---|---|---|---|
| Muy Alto | 3 | – | 4 | 5 | – |
| Alto | – | – | – | – | – |
| Medio | – | – | – | – | – |
| Bajo | – | 1 | – | – | – |

| | | | | | |
|---|---|---|---|---|---|
| Muy Bajo | – | – | – | – | 2 |