**Tabla 1.** Ejemplos por sector de la industria

| Industria | Perfil del Atacante | Deben estar en | | |
|---|---|---|---|---|
| | | **Oportunista** | **Estándar** | **Avanzado** |
| **Financiera y Seguros.** | Ataques oportunistas, por motivos financieros.<br><br>Búsqueda de datos o credenciales de cuentas a fin de realizar fraudes o beneficiarse directamente por el flujo de dinero (Transacciones B2B) que presentan estas aplicaciones.<br><br>Chantajes basados en secuestro de datos (ransomware).<br><br>Técnicas más comunes:<br><br>Robo de credenciales y claves.<br><br>Ataques a nivel de aplicación.<br><br>Ingeniería social. | Aplicaciones que son accesibles desde internet. | Aplicaciones donde se transfiere dinero entre cuentas de la misma organización.<br><br>Aplicaciones donde se realicen movimientos de dinero con ***Cámara de Compensación Automatizada*** **(Automated Clearing House network, ACH)** y con límites de transacción.<br><br>Aplicaciones donde se realizan transferencias en línea con un rango de tiempo determinado. | Software que poseen sustanciales volúmenes de información delicada de cuentas bancarias.<br><br>Aplicaciones donde las transferencias se realicen velozmente con sustanciales cantidades de dinero.<br><br>Aplicaciones donde se permita realizar transacciones por lotes o individuales de grandes sumas de dinero. |
| **Manufacturera.** | Ataques más organizados y con un | Aplicaciones que son | Aplicaciones donde la | Aplicaciones con |

| | | | | |
|---|---|---|---|---|
| **Profesional.**<br><br>**Transporte.**<br><br>**Tecnología.**<br><br>**Utilidades.**<br><br>**Infraestructura.**<br><br>**Defensa.** | objetivo concreto, teniendo tiempo de preparación, grandes habilidades y sobre todo recursos; debido a que, llegar a la fuente de la información preciada es complejo y difícil de localizar.<br><br>Haciendo uso de técnicas de ingeniería social avanzada se realizan ataques donde se requiere utilizar o manipular a los empleados de la organización o externos de la empresa pero con relación con alguno de los trabajadores.<br><br>Búsqueda de datos de propiedad intelectual para obtener ventajas estratégicas sobre la competencia y venderlas al mejor postor.<br><br>Ataques dirigidos a abusar de las funcionalidades para influenciar el comportamiento de forma directa o alterna, a fin de lograr beneficios personales, realizar chantajes, suplantar la identidad de otro, pagos de manera ilegal, o alterar partes sensibles del sistema.<br><br>Técnicas más comunes:<br><br>Robo de credenciales y claves.<br><br>Ataques a nivel de aplicación.<br><br>Ingeniería social avanzada. | accesibles desde internet. | información de los empleados se puede usar para modificar el núcleo del sistema.<br><br>Sistemas que poseen en su información material de secretos empresariales y derechos de autor o propiedad intelectual. | contenido de secretos empresariales, gubernamentales, que poseen derechos de autor o propiedad intelectual que representan el éxito y la supervivencia de una organización.<br><br>Aplicaciones que dentro de sus funciones existen controladores para operaciones muy delicadas donde un fallo expone la vida o amenaza la seguridad en general. |
| **Salud.** | Ataques más organizados y con un objetivo concreto, teniendo tiempo de preparación, grandes habilidades y sobre todo recursos; debido a que, | Aplicaciones que son accesibles desde internet. | Aplicaciones con información médica confidencial o sensible. | Aplicaciones que permiten controlar equipos sensibles en hospitales y salas de |

| | | | | |
|---|---|---|---|---|
| | llegar a la fuente de la información preciada es complejo y difícil de localizar.<br><br>Haciendo uso de técnicas de ingeniería social avanzada se realizan ataques donde se requiere utilizar o manipular a los empleados de la organización o externos de la empresa pero con relación con alguno de los trabajadores.<br><br>Búsqueda de datos de propiedad intelectual para obtener ventajas estratégicas sobre la competencia y venderlas al mejor postor.<br><br>Ataques dirigidos a abusar de las funcionalidades para influenciar el comportamiento de forma directa o alterna, a fin de lograr beneficios personales, realizar chantajes, suplantar la identidad de otro, pagos de manera ilegal, o alterar partes sensibles del sistema.<br><br>Técnicas más comunes:<br><br>Robo de credenciales y claves.<br><br>Ataques a nivel de aplicación.<br><br>Ingeniería social avanzada. | | | cirugía, o dispositivos que monitorean la salud de un paciente y se ponga en riesgo su vida. |
| **Venta por menor, alimento, hospitalidad.** | Ataques utilizando tácticas oportunistas de "aplaste y agarre".<br><br>Ataques Oportunistas, por motivos financieros o por motivos personales identificables. | Aplicaciones que son accesibles desde internet. | Aplicaciones que presenten sus catálogos empresariales con información sensible de sus productos o servicios, o datos corporativos de sus empleados o junta directiva | Aplicaciones POS que tienen multitud de información de transacciones que si se detectan se pueden usar para realizar robos o fraudes. |

| | | | | |
|---|---|---|---|---|
| | Ataques más orquestados y totalmente enfocados a sustraer información específica de propiedad intelectual, derechos de autor, entre otros, con el fin de tener una ventaja competitiva contra sus pares empresariales.<br><br>Técnicas más comunes:<br><br>Robo de credenciales y claves.<br><br>Ataques a nivel de aplicación.<br><br>Tácticas oportunistas de "aplaste y agarre".<br><br>Ingeniería social avanzada. | | y algunas aplicaciones que ocultan información a los usuarios.<br><br>Aplicaciones con ínfimas cantidades de funciones de datos o de confirmaciones de pagos. | Sistemas que gestionan un volumen sustancial de datos sensibles, que poseen información de tarjetas de crédito, nombres completos y documentos de identidad. |

**Tomado de (**OWASP. 2021)**.**