# Fraude en procesos de pago

Tu seguridad es nuestro motor

Últimamente, cada vez que ocurre un fraude relacionado con un sistema y dinero, **se apunta a la Ciberseguridad**. **Sin embargo, los factores que se combinan para que un fraude se concrete ocurren en diferentes dimensiones**. Sin perder de vista que “La oportunidad hace al defraudador”, lo más común suele ser:

**Archivo de Pago Editables o Interceptables**; si bien los procesos de asignación de permisos para procesar y autorizar un pago pueden ser apropiados, puede ocurrir que:

- El archivo de pago o nómina que se carga a la entidad pagadora es un **archivo de texto (.txt) o archivo Excel estandarizado, sin protección** para evitar su edición.

- **El mecanismo de carga del archivo de pago sea vulnerable** y pueda ser interceptado por un tercero para su edición.

- **El archivo de pago sea procesado por un tercero (Proveedor) sin supervisión posterior.**

- **El proveedor de pago no tenga controles robustos** para asegurar que el archivo de pago se mantenga seguro. (típico de falta de supervisión de cadena de suministro).

**Segregación Funcional:**

- Problemas en la gestión de accesos, tales como; omisiones de revisión o contraste con las tareas del Colaborador, conflicto de segregación con roles y privilegios asignados previamente (concentración de funciones) y falta de un control que contraste que los permisos asignados a nivel de sistema corresponden a los autorizados.

- Selección del Backup genera concentración funcional.

- Selección de personas con antecedentes de fraude en otras instituciones.

**Diseño del Proceso:**

- Falta de supervisión y verificación del contenido de las nóminas de Pago.
- Flujo de aprobación de un pago permite la modificación por “corrección de un dato” sin necesidad de volver a pasar por el proceso de aprobación.
- Creación o edición de proveedores o receptores de pago sin supervisión. Esto generalmente ocurre tanto a nivel de sistema de origen como a nivel de ERP.