Laboratorio 3 - Ciberseguridad

Fabián Valero Duque

Integrantes: Alejandra Campo Archbold, María Fernanda Rodríguez, Jham Pool Murillo

24 de agosto de 2022

Gestión de activos para la industria de alimentos

Para proteger la cadena de suministros de una industria de alimentos contra amenazas cibernéticas se busca medir la visibilidad total de las operaciones convergentes de IT/OT, la identificación de las vulnerabilidades antes que se conviertan en *exploits,* ejecución de registros de auditoría completos y constantes para cada cambio de configuración.

¿Cuál es la información más confidencial?

La infraestructura de una empresa puede tener dos tipos de tecnología: tradicional u operacional.

La tecnología operacional contiene estaciones de ingeniería, servidor OT, impresoras OT que son activos que necesitan estar disponibles en la planta industrial.

La tecnología tradicional donde se encuentra el servidor IT, estación IT e impresoras IT, que son parte de la Oficina Central.

En este sentido, la información más confidencial está en los servidores IT debido a que contiene datos importantes de los clientes, permite compartir archivos, administra estaciones de trabajo, incluye sistema de antivirus y actualización del sistema operativo.

¿Qué activos deben protegerse de riesgos de integridad?

Los activos que deberían protegerse de riesgos de integridad son: el servidor IT, la estación IT, el Firewall Corporativo, estación de ingeniería, servidor OT.

En caso de un ataque, es pertinente que los datos no sean modificados por personas no autorizadas debido a que la industria de alimentos podría tener datos sensibles de los programas que contienen los estados financieros en el servidor IT y la estación IT. Es pertinente tener protegido el Firewall Corporativo ya que tiene la capacidad de distribuir y priorizar el uso de Internet para balancear tráficos entre múltiples enlaces de Internet, intrusiones a la red, entre otras.

Por otro lado, la estación de ingeniería puede contener reportes que son importantes para la toma de las decisiones de la empresa y así como el servidor OT contiene la integración de software y hardware que sirven para poder comunicar, controlar y supervisar diversos dispositivos de las redes industriales.

¿Qué activos deberían ser considerados para el BCP (Plan de Continuidad Empresarial)?

Durante los eventos no planificados, deberían estar disponibles: el servidor IT, estación IT, servidor OT.

Estos activos permite mantener los archivos de diferentes clientes a través de una red, comunicación entre servidor (software) y cliente se basa en HTTP, correo electrónico, servidor DNS. Asimismo, que los procesos industriales de alimentos se mantengan los diversos dispositivos en las redes.

¿Qué activos confidenciales poseen datos personales?

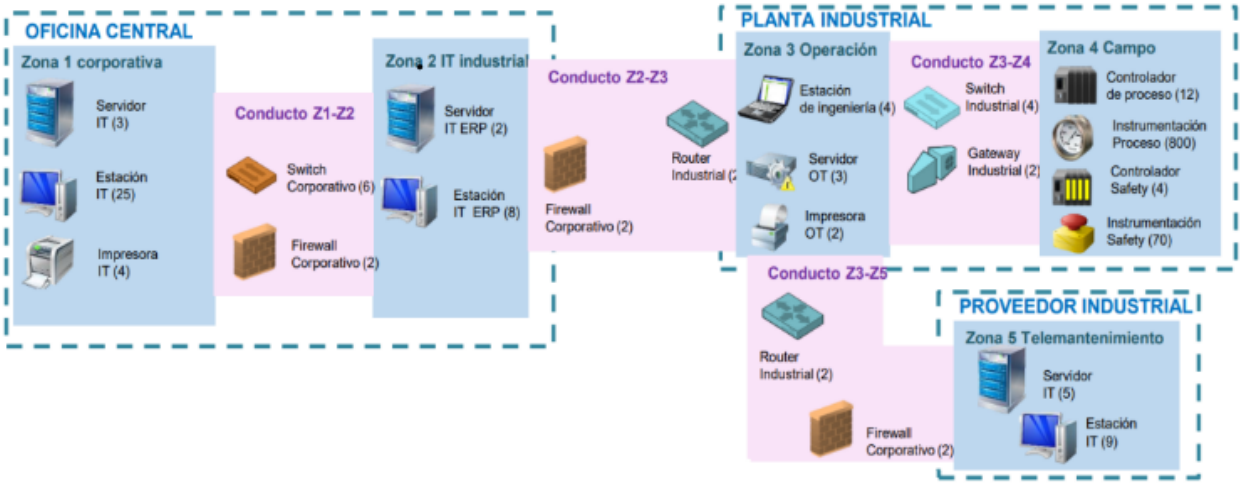
Los activos que poseen datos personales para la industria de alimentos son: el servidor IT, la estación IT y la estación de ingeniería, debido a que contienen datos del cliente mediante WEB, correo electrónico, bases de datos, reportes de analítica de datos.

¿Qué activos deberían estar en la estrategia de DLP (Prevención de pérdida de datos?

Para evitar que las personas accedan a información sensible que no necesitan deberían estar: el Firewall Corporativo ya que tiene la capacidad de priorizar, dar permisos al uso de la red privada, provee protecciones para que no se cruce y se pierda los datos.

Arquitectura de la industria de alimentos.

Nuestra arquitectura está diseñada para el sector de la industria que se encarga de la **automatización de almacén**. Se utilizó la siguiente plantilla:



Oficina central

En la oficina central se tratan los temas administrativos de la empresa, suele guardarse mucha información importante sobre los clientes, la empresa, la industria y la planta empresarial.

Zona 1 corporativa

En esta zona se encuentran componentes de nivel 4, es decir los componentes de sistemas de información, por lo cual consideramos que la criticidad de la integridad y disponibilidad es **media** y la de la confidencialidad es **muy alta**.

- **Servidor IT:** Integridad y disponibilidad alta, pero confidencialidad muy alta ya que manejamos información importante.
- **Estación IT:** Mantenemos la criticidad de los 3 riesgos alta ya que se necesita que los temas administrativos de la empresa continuen estando seguros, intactos y disponibles.
- **Impresora IT:** La integridad de la impresora debe ser media para que no ocurran fallos técnicos, pero la disponibilidad y confidencialidad no son importantes en la impresora por lo que su criticidad es baja.

Zona 2 IT industrial

Esta es una zona corporativa cuyos componentes también son de nivel 4, por esto decidimos mantener las mismas criticidades a la Zona 1.

- **Servidor IT ERP:** Al ser un servidor de la industria mantenemos sus 3 criticidades altas.
- **Estación IT ERP:** Su integridad y disponibilidad son altas pero la confidencialidad es media ya que solo se manejaría seguridad física.

Planta industrial

En esta sección se manejan datos instructivos y maquinaria esenciales para la producción del servicio de la industria.

Zona 3 operación

En esta zona se manejan componentes de nivel 1 y 2, los cuales funcionan como control o supervisión en los procesos de la empresa. Consideramos que estos componentes son muy importantes ya que permiten que la automatización del almacen se desarrolle correctamente. Por esto mantenemos la criticidad de la integridad, disponibilidad y confidencialidad **altas**, de manera que nadie pueda afectar la calidad de la empresa y no se filtre su información importante.

- **Estación de ingeniería:** Su integridad y disponibilidad son altas ya que son necesarias para el control o supervisión de maquinaria pero la confidencialidad es media ya que solo se manejaría seguridad física.

- **Servidor OT:** Mantenemos altas las 3 criticidades para evitar fallas en la supervisión de procesos de la empresa.
- **Impresora OT:** Baja en las 3 criticidades ya que no es relevante para el funcionamiento de la planta industrial.

Zona 4.1 Campo

En esta zona manejamos componentes de nivel 0 y nivel 1 **safety**, por lo cual veremos la instrumentación que utiliza la empresa para producir su servicio y también algunos controladores que nos funcionen en casos críticos o de emergencia. Consideramos que esta es la zona esencial de la empresa ya que debemos estar preparados para cualquier posible falla en la industria que requiera segundas opciones; Por esto decidimos que la criticidad de la integridad, disponibilidad y confidencialidad deben ser **muy altas.**

- **Controlador Safety:** Muy alto en las 3 criticidades ya que en casos críticos de la empresa estos controladores podrían ser un blanco fácil en caso de no ser protegidos correctamente y podríamos acabar sin recursos a los cuales acudir para continuar su funcionamiento.
- **Instrumentación Safety:** Muy alta en temas de integridad y disponibilidad por la misma razón anterior, pero media en confidencialidad ya que la instrumentación no guarda información relevante.

Zona 4.2 Campo

En esta zona a diferencia de la anterior manejamos componentes de nivel 0 y 1 de **proceso avanzado.** Estos componentes son de funcionamiento constante y nos permiten producir el servicio de manera adecuada. Consideramos que su integridad debe ser alta ya que no nos podemos permitir un pequeño cambio en las máquinas. La disponibilidad es debe ser alta y la condifencialidad media ya que estos elementos no guardan mucha información importante al ser maquinaria de una industria de alimentos.

- **Controlador de proceso:** Muy alta en cuanto a integridad ya que es esencial realicen bien su función, disponibilidad alta ya que son necesarios y confidencialidad media porque no tienen información relevante.
- **Instrumentación de proceso:** Integridad alta ya que la función de la instrumentación debe ser la misma siempre, la disponibilidad media debido a que contamos con 800 maquinas y confidencialidad media ya que no tienen información relevante.

Proveedor industrial

En esta sección se guardan y consultan los datos de la zona industrial.

Zona 5 Telemantenimiento

Esta es una zona de proveedor con componentes de nivel 4, es importante para que tengamos un servicio de supervisión y actuación remota. Por esto, su integridad y disponibilidad deben ser altas para mantener un servicio de calidad y la confidencialidad debe ser **muy alta** ya que mediante sus componentes se puede llegar a trabajar con información muy delicada.

- **Servidor IT:** Para realizar este servicio de supervisión remota es importante que el servidor sea altamente integro y disponible, su confidencialidad es muy alta porque allí se puede manejar información muy relevante acerca de toda la empresa.
- **Estación IT:** Por lo mismo mencionado anteriormente, la integridad y disponibilidad deben ser altas y la confidencialidad media ya que en la estación sólo se trabaja con seguridad física y ya protegimos altamente el servidor.

Conducto Z1 - Z2

Este conducto permite la comunicación entre las dos zonas de la oficina central. En este caos consideramos que su integridad y confidencialidad deben ser altas para que no se modifique o filtre información, pero su disponibilidad puede ser baja ya que se pueden comunicar de otras maneras dentro de la misma oficina.

- **Switch corporativo:** Integridad y confidencialidad altas pero disponibilidad media ya que no es esencial.
- **Firewall corporativo:** Integridad y confidencialidad muy altas y disponibilidad alta ya que es un dispositivo esencial para la seguridad de la empresa.

Conducto Z2 - Z3

Permite la comunicación entre zona 2 y 3, es decir entre secciones de oficina central y planta industrial. Por esto su integridad y confidencialidad debe ser muy alta y su disponibilidad alta ya que entre estas zonas es mas dificil la comunicación.

- **Router industrial:** Integridad y confidencialidad altas pero disponibilidad media ya que no es esencial.

- **Firewall corporativo:** Integridad y confidencialidad muy altas y disponibilidad alta ya que es un dispositivo esencial para la seguridad de la empresa.

Conducto Z3 - Z4.1

Permite la comunicación entre zona 3 y zona 4 con los dispositivos safety, su integridad debe ser alta pero consideramos que su disponibilidad y confidencialidad pueden ser bajas ya que pueden haber otras formas de comunicación a estos dispositivos y ya están altamente protegidos.

- **Switch industrial:** Su uso no es tan necesario por lo cual puede ser de criticidad media en las 3 componentes.
- **Gateway industrial:** Su uso no es tan necesario por lo cual puede ser de criticidad media en las 3 componentes.

Conducto Z3 - Z4.2

Permite la comunicación entre zona 3 y zona 4 con los dispositivos de proceso avanzado, su integridad debe ser alta pero consideramos que su disponibilidad y confidencialidad pueden ser bajas ya que pueden haber otras formas de comunicación a estos dispositivos, están bien protegidos y no manejan datos confidenciales.

- **Switch industrial:** Su uso no es tan necesario por lo cual puede ser de criticidad media en las 3 componentes.
- **Gateway industrial:** Su uso no es tan necesario por lo cual puede ser de criticidad media en las 3 componentes.

Conducto Z3 - Z5

Permite la comunicación entre zona 3 y 5, comunicando las secciones de planta industrial y proveedor industrial. Debido a que están muy correlacionadas necesitan buena comunicación por lo cual mantenemos las 3 criticidades altas.

- **Router industrial:** Su integridad y disponibilidad debe ser alta ya que es importante tener una buena comunicación. Su confidencialidad puede ser media.
- **Firewall corporativo:** El firewall es muy importante dentro de los procesos de la empresa. Debe permanecer altamente integro y con su disponibilidad y confidencialidad muy alta.

Referencias

- Cyber security: Global food supply chain at risk from malicious hackers. https://www.bbc.com/news/science-environment-61336659