Medidas de seguridad para salvaguardar la información del Centro de Ingeniería y Desarrollo Industrial

El presente documento describe las medidas y medios con que cuenta el Centro de Ingeniería y Desarrollo Industrial para tratar y manejar la información. Centrándose en dos rubros que son disponibilidad y resguardo de la información.

Disponibilidad:

En el rubro de la disponibilidad de la información se hablará de:

- ***Comunicaciones***
- ***Procesamiento***

Comunicaciones:

El Centro de Ingeniería y Desarrollo Industrial cuenta con redes de comunicaciones LAN y Wireless disponible en todas las sedes, dichas redes son redundantes a nivel de CORE, lo que permite una alta disponibilidad de los sistemas y del acceso a la información.
Ambas redes se monitorean de manera constante por medio del sistema dedicados al monitoreo de disponibilidad y performance de la red de comunicaciones.

Para la mitigación de fallas a nivel LAN se tienen sistemas redundantes en los equipos clave de la infraestructura de comunicaciones, para el caso de las comunicaciones se establecieron equipos Core redundantes.

Para el caso de las comunicaciones Wireless, se tienen tres Wireless LAN Controller, permitiendo una alta disponibilidad del servicio.

Los equipos son respaldados a nivel configuración de manera periódica o cuando se realizan cambios mayores en las configuraciones y se tiene resguardos de al menos 2 configuraciones por equipo con una retención de 3 meses.

Los equipos de comunicación principales se encuentran resguardados en centros de datos con medidas de operación TIER II, es decir, respaldados a nivel eléctrico por UPS y plantas de emergencia y a nivel temperatura por aires acondicionados de precisión o en su defecto sistemas redundantes de aire acondicionado.

Los permisos de acceso a los equipos de comunicaciones, solo se tiene un usuario bajo la administración del personal interno especializado, la cual pertenece al personal en sitio que administra los equipos del Centro de Ingeniería y Desarrollo Industrial.

La infraestructura de comunicaciones con que cuenta el Centro de Ingeniería y Desarrollo Industrial permite una alta disponibilidad de acceso a la información por parte de los usuarios.

Procesamiento:
El Centro de Ingeniería y Desarrollo Industrial cuenta con infraestructura de servidores físicos para la entrega servicios OnSite, disponible en todas las sedes, y basada en tecnologías virtuales, permitiendo disponibilidad y alta redundancia.

Los servidores locales se mantienen respaldados con base a calendario previamente establecido.

Todos los sistemas de procesamiento se monitorean de manera constante por medio del sistema dedicados al monitoreo de disponibilidad y performance de la infraestructura de servidores físicos, el monitoreo es a nivel físico y virtual.

Para la mitigación de fallas a nivel procesamiento se tienen sistemas tipo nodo en servidores lo que permite la creación de clusters en los equipos clave de la infraestructura.

Para el caso de equipo Locales, los equipos de procesamiento cuentan con sistemas de redundancia en conexión eléctrica, conectividad a LAN y Almacenamiento.

Los equipos de procesamiento principales se encuentran resguardados en centros de datos con medidas de operación TIER II, es decir, respaldados a nivel eléctrico por UPS y plantas de emergencia y a nivel temperatura por aires acondicionados de precisión o en su defecto sistemas redundantes de aire acondicionado.

Los permisos de Acceso a los equipos de procesamiento, solo se tiene un usuario bajo la administración del personal interno especializado, la cual pertenece al personal en sitio que administra los equipos del Centro de Ingeniería y Desarrollo Industrial.
La infraestructura de procesamiento con que cuenta el Centro de Ingeniería y Desarrollo Industrial permite una alta disponibilidad de acceso a la información por parte de los usuarios y un resguardo seguro de la información.

Resguardo:

En el rubro del resguardo de la información se hablará de:
- ***Acceso a la Información***
- ***Seguridad de la información***
- ***Almacenamiento y resguardo***
- ***Sistemas de seguridad física***

Acceso a la información:
El Centro de Ingeniería y Desarrollo Industrial cuenta con un sistema tipo FileService, dicho sistema almacena información de proyectos operativos y comerciales, este sistema ha sido configurado para trabajar de manera encriptada.

El proceso de encriptación contempla los siguientes procesos:

Authentication Encrypted (LDAPS)

La autenticación se realiza por el protocolo LDAPS (SSL) por el puerto 636.

Web Traffic (SSL Protect)

Se instala certificado de seguridad SSL (SHA2), para conexiones segura vía web por puerto 443.

Storage Encrypted (Application)

El repositorio trabaja bajo el esquema DARE (Data-At-Rest Encryption), este esquema encripta toda la información que se almacena en el repositorio.

SQL Traffic (SSL Protec)

La comunicación entre el aplicativo y la BD se encripta bajo un certificado con Algoritmo Hash SHA1 y un llave RSA (1024 bits).

File Traffic

Los clientes de equipos de cómputo y dispositivos móviles usan el login por medio de autenticación vía LDAPS y SSL SHA1 (Port:443) ya que se hace una conexión directa al aplicativo vía sitio web.

Seguridad de la información:

La seguridad de la información se compone de dos partes, nivel físico y nivel lógico.

Nivel Físico:

Se tienen equipos Firewall en cada sede.

La tecnología usada en Seguridad perimetral y cuenta con las principales herramientas de seguridad, como es monitoreo de entrada y salida, bloqueo de virus, detección de reputación de sitios, listas blancas y negras de acceso, sistema de VPN personal, sistemas de DNS público para monitoreo de reputación, entre otras.

Los equipos de seguridad perimetral se mantienen respaldados con base a calendario previamente establecido.

Todos los sistemas de seguridad perimetral se monitorean de manera constante por medio del sistema dedicados al monitoreo de disponibilidad y performance de los equipos.

Los equipos de seguridad perimetral principales se encuentran resguardados en centros de datos con medidas de operación TIER II, es decir, respaldados a nivel eléctrico por UPS y plantas de emergencia y a nivel temperatura por aires acondicionados de Precisión o en su defecto sistemas redundantes de aire acondicionado.

La temperatura de los centros de datos es importante, por la cantidad de calor que generan los equipos, debido a esto, se procura mantener una temperatura entre el rango de los 18º y los 21º, lo cual aplica para todas las sedes. Es importante mencionar que las temperaturas podrían variar según la sede en base a la orografía y temperatura ambiente de cada sede.

Los permisos de Acceso a los sistemas de seguridad perimetral, solo se tiene un usuario bajo la administración del personal interno especializado, la cual pertenece al personal en sitio que administra los equipos del Centro de Ingeniería y Desarrollo Industrial.

El acceso a los centros de datos donde se tienen los equipos de seguridad perimetral es restringido a solo personal autorizado por medios de tarjetas de acceso controladas por un sistema de Control de Acceso.

Nivel Lógico:
Se tienen servidores de directorio activo, en cada sede del Centro de Ingeniería y Desarrollo Industrial, la sede central Querétaro y el centro de datos externo cuenta con 2 servidores para distribuir la carga de trabajo debido a la cantidad de usuarios. Los servidores tienen réplicas de configuración e información entre todos lo que garantiza que si un equipo falla los otros pueden sostener la operación.

El acceso a información vía File Server o sistemas que accedan a información se hace por medio de autenticación vía Directorio Activo, por cuentas de usuarios legitimas o cuentas de administración de sistemas legitimas.

Almacenamiento y Resguardo:
La Administración de los sistemas de respaldo de información y almacenamiento de información se realiza de manera interna en el Centro de Ingeniería y Desarrollo Industrial.

Para el caso de los respaldos de información locales se tienen dos sistemas:
Avamar, consiste en una tecnología de respaldo a disco, con tecnología de duplicación, el objetivo de Avamar es respaldar información de manera granular y Bases de datos.

Veeam, consiste en software para el respaldo de servidores virtuales, con esta tecnología se respaldan todos los servidores virtuales de producción y permite una restauración de servidor completa.

La tecnología de resguardo de información se hace por medio de tecnologías basadas en SAN se compone de repositorios de almacenamiento en las 4 sedes con mayor densidad de población.

Todos los sistemas de respaldo de información y almacenamiento de información se monitorean de manera constante por medio del sistema dedicados al monitoreo de disponibilidad y performance de los equipos.

Para la mitigación de fallas en el caso de los equipos Avamar se tiene un sistema de réplicas entre sedes, se envían las bases de datos críticas hacia otras sedes con el fin de tener resguardo de la información fuera de la sede central.
Los sistemas de respaldo de información y almacenamiento se encuentran resguardados en centros de datos con medidas de operación TIER II, es decir, respaldados a nivel eléctrico

por UPS y plantas de emergencia y a nivel temperatura por aires acondicionados de Precisión o en su defecto sistemas redundantes de aire acondicionado.

Los permisos de Acceso a los sistemas de sistemas de respaldo de información y almacenamiento, solo se tiene un usuario bajo la administración del personal interno especializado, la cual pertenece al personal en sitio que administra los equipos del Centro de Ingeniería y Desarrollo Industrial.

El acceso a los centros de datos donde se tienen los equipos de sistemas de respaldo de información y almacenamiento es restringido a solo personal autorizado por medios de tarjetas de acceso controladas por un sistema de Control de Acceso.

Sistemas de seguridad física:
El servicio de seguridad física se compone de dos elementos, Sistema de control de acceso y Sistema de Videovigilancia.

La Administración de los sistemas de seguridad física como son Control de Acceso y Video Vigilancia se realiza de manera interna en el Centro de Ingeniería y Desarrollo Industrial.

Las tecnologías de seguridad física se encuentran hospedadas en servidores locales.

Se tiene configurado un sistema de monitoreo sobre los equipos. Para el caso del control de accesos se monitorea el servidor que contiene la aplicación y para el caso de Video Vigilancia se monitorea el servidor y las cámaras de manera individual.

Todos los sistemas de seguridad física se monitorean de manera constante por medio del sistema dedicados al monitoreo de disponibilidad y performance de los equipos.

Los equipos sistemas se encuentran resguardados en centros de datos con medidas de operación TIER II, es decir, respaldados a nivel eléctrico por UPS y plantas de emergencia y a nivel temperatura por aires acondicionados de Precisión o en su defecto sistemas redundantes de aire acondicionado.

Los permisos de Acceso a los sistemas, solo se tiene un usuario bajo la administración del personal interno especializado, la cual pertenece al personal en sitio que administra los equipos del Centro de Ingeniería y Desarrollo Industrial.

El acceso a los centros de datos donde se tienen los equipos de respaldos de información es restringido a solo personal autorizado por medios de tarjetas de acceso controladas por un sistema de Control de Acceso.