GLENCORE

Ciberseguridad para las Tecnologías Operacionales – Principios Rectores

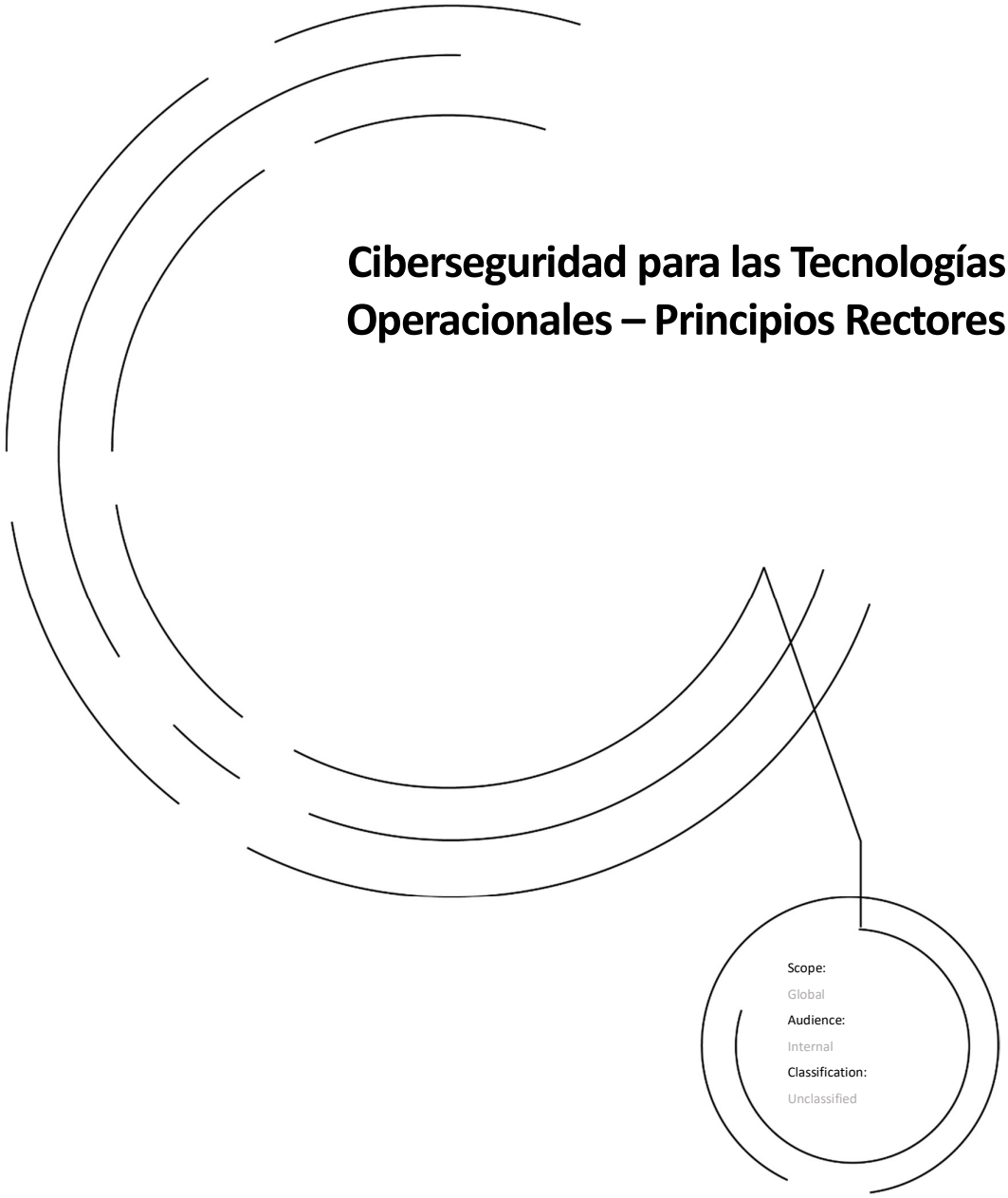


Table of Contents

Ciberseguridad para las Tecnologías Operacionales – Principios Rectores

1 Introducción

Glencore se compone de un gran número de activos industriales que usan Tecnología Operacional (OT) para dar soporte a los procesos productivos. Definimos OT como todo hardware o software que detecta o produce un cambio por medio de monitorización directa o el control físico de equipos como los usados en Longwall mining o sensores de medición de la calidad del aire.

Global IT ha desarrollado un conjunto de guías, diseños y estándares para crear una red y un modelo de infraestructura seguros y robustos. Muchos de estos diseños y conceptos se pueden transferir al área de las Tecnologías Operacionales y, por lo tanto, se ha requerido a Global IT que provea de algunos principios rectores acerca de cómo las redes industriales pueden interactuar con la red corporativa para impulsar la adopción de los estándares de Ciberseguridad de las TI.

En la tabla debajo, se pueden ver las guías, diseños y estándares de TI y su equivalente con los diseños y estándares de las OT que son parte de este proceso.

Este documento se centra en los Principios Rectores y la Arquitectura, así como en el desarrollo de un Catálogo de Servicios.

Tecnologias de la Informacion	Tecnología Operacional
Diseño de la Infraestructura de AnyAccess	Principios Rectores y su Arquitectura *1
Catálogo de Servicios de Infraestructura Global	Catálogo de Servicios Compartidos e Infraestructura *2
Estándar de Seguridad y Garantia de Seguridad	Subconjunto del Estándar de Seguridad *1,3 Evaluacion de Principios Rectores *1

*1 Vea Global IT Portal (https://globalit.glencore.net)

*2 Catálogo de Servicios – consulte la sección 3 de este documento

*3 Estándares aplicables: IT Service Continuity, Incident Management, Network Security, Vulnerability Management, Audit Logging and Monitoring, Malware Prevention and Physical Security

El proceso para conseguir el Status de Cumplimiento de la Ciberseguridad en OT, se puede dividir en 4 partes:

- Seguridad – Alinearse con las técnicas, políticas de seguridad de la información y mejores prácticas de Global IT, para asegurar la confidencialidad, integridad y disponibilidad de los activos.
- Alineamiento de la Infraestructura – Desarrollo de un catálogo de servicios de TI que puedan ser aprovechados, de forma segura por la red OT.
- Compartir Conocimiento – Comunicación continua entre IT y los ingenieros industriales es un factor clave para el éxito.
- Cumplimiento, Monitorización de la Seguridad y resolución.

1.1 Resumen

El presente documento describe los Principios Rectores de Global IT que, una vez implementados, ayudaran a los sitios industriales con entornos OT, a gestionar de forma segura su infraestructura, aprovechando la tecnología existente a la vez que mejoran su posición respecto a la ciberseguridad. Una vez en funcionamiento, el continuo escaneado y la monitorización servirán para asegurar el cumplimiento de los estándares.

2 Principios Rectores

Los entornos OT presentan una serie de desafíos únicos que los entornos de las TI normalmente no tienen. Mientras que TI normalmente se enfoca en la confidencialidad, la integridad y la disponibilidad; los entornos OT priorizan la disponibilidad.

Es bastante común que los entornos OT estén “aislados” de los entornos de las TI, por lo que es bastante común que los ingenieros desplieguen módems ADSL o GSM en el área de OT.

Un factor crítico para el éxito es tener muy presentes las diferencias en cuanto a la arquitectura y diseño que existen entre los entornos OT y TI.

Algunos posibles incidentes a los que el entorno OT se tiene que enfrentar, pueden ser:

- El flujo de la información está bloqueado o sufre retrasos, los que puede interrumpir las operaciones.
- Cambios no autorizados, en las instrucciones, comandos o en los niveles de alarmas, que podrían dañar, deshabilitar o apagar los equipos, tener un impacto en el medio ambiente o poner en peligro vidas humanas.
- Información inexacta enviada a los operadores, con intención de disfrazar cambios no autorizados o llevar a los operadores a iniciar trabajos inapropiados que podrían tener consecuencias negativas
- Modificaciones en el software OT, en su configuración o infectarlo con malware, que puede tener efectos muy negativos.
- Interferencias en la operación de sistemas de seguridad, que pueden poner en riesgo vidas humanas.

2.1 Posibles Consecuencias

Dicho lo anterior, las consecuencias que podrían tener un incidente en el entorno OT son:

- Reducción o perdida de la producción en un sitio o en varios simultáneamente.
- Heridas o muerte de empleados.
- Heridas o muerte a miembros de la comunidad.
- Daño al equipamiento.
- Liberación, desvío o robo de materiales peligrosos.
- Daño al Medio Ambiente.
- Violación de normas legales.
- Contaminación del producto.
- Responsabilidades civiles o penales.
- Perdida de información privada o confidencial.
- Perdida de reputación de la compañía y de la confianza del cliente.

2.2 Implementación

Se espera que la implementación de la Ciberseguridad en el entorno OT, sea diferente en cada uno de los sitios debido a como las redes y la infraestructura fueron implementadas. En la siguiente lista se detallan los 10 principios rectores que todo sitio industrial debe seguir.

Principios	Estándares		Explicación	Prioridad
Separación	1	IT y OT deben estar separadas por un Firewall exclusivo (monitorizado por Proveedor Global y Global IT).	Controlar el flujo de tráfico y los protocolos entre los dos entornos. Todas las conexiones entre IT y OT debe ser a través del Firewall. Ninguna maquina puede existir en los dos entornos.	Obligatorio
	2	La Zona Expuesta de OT (DMZ) entre IT y OT. Todos los servidores y equipos de mesa que se encuentren en esta zona, deben cumplir con los estándares del Global IT (versionado e imágenes del SO, parcheado y anti-virus siempre que sea posible).	Impide la necesidad de comunicación directa entre los entornos IT y OT. Solo para aquellas maquinas que necesiten transmitir información entre los dos entornos. Ningún sistema con la capacidad de afectar la vida humana o que necesite estar en funcionamiento el máximo tiempo posible, debe estar en esta zona.	Opcional
	3	Las maquinas en el entorno OT, no deben pertenecer al dominio AnyAccess.	El entorno OT debe tener su propio entorno de autenticación. Puede ser un dominio separado en AD.	Obligatorio
Networking	4	IT y OT deberían usar esquemas de IP diferentes.	Las redes OT deben evitar rangos de IP que estén reservados para IT. La asignación de rangos IP en el entorno OT, no está gestionada globalmente.	Opcional
	5	Las redes de OT no deben ser enrutables fuera de su sitio. Cualquier ruteo externo debe hacerse por NAT.	Redes superpuestas impiden el ruteo global.	Opcional
	6	Equipos de soporte (portátiles, equipos de almacenamiento) no deben cruzar entre las redes.	El riesgo de llevar malware desde IT a OT es alto (Stuxnet entro a través de USB).	Obligatorio
	7	Network Access Control (NAC) debe ser adoptado.	Debe introducirse una Política para permitir solo equipos aprobados. Las redes inalámbricas debes ser aseguradas.	Obligatorio
Soporte Remote	8	Los módems ADSL o GSM no deben ser conectados directamente en el entorno OT.	VDI de 3as partes (Equipos Gestionados por Glencore) se pueden proveer en la Zona Segura para permitir el acceso a los sistemas OT.	Obligatorio
Gestión	9	Los equipos Windows y Linux en el entorno OT deben tener un antivirus certificado por el vendedor.	Los proveedores de OT pueden solo soportar el AV de un fabricante y una versión especifica. Esto puede llevar a tener muchos productos y versiones diferentes. Cuando sea posible, los proveedores deben poder trabajar con los AV estandarizados. Todas las soluciones AV, deben ser gestionadas y monitorizadas.	Opcional
	10	Las maquinas Windows y Linux en la zona OT deben tener instalados los últimos parches del fabricante.	Es posible que los proveedores OT, solo soporten algunos parches para el Sistema Operativo.	Opcional

2.3 Explicaciones

- **IT y OT deben estar separadas por un Firewall exclusivo (Proveedor Global y monitorizado por Global IT).**
  Implementación obligatoria
  El punto más importante de los Principios Rectores. Las redes IT y OT deben estar claramente separadas. Las redes industriales deben estar protegidas por una Firewall para evitar las amenazas que puedan venir desde el entorno IT, Internet u otras redes industriales. Esta separación debe ser por medio de un Firewall físico, preferiblemente por un clúster.
  Es importante tener en cuenta que las redes OT no deberían depender de la disponibilidad del Firewall. Todos los sistemas que necesiten acceso ininterrumpido entre ellos, no pueden estar en zonas diferentes sin contar con un diseño de Firewall robusto y una gran inversión.

- **La Zona Expuesta de OT (DMZ) entre IT y OT. Todos los servidores y equipos de mesa que se encuentren en esta zona, deben cumplir con los estándares del Global IT (versionado e imágenes del SO, parcheado y anti-virus siempre que sea posible).**
  Implementación opcional
  La implementación de una Zona Expuesta de OT anula la necesidad de una comunicación directa entre las redes de IT y OT. La comunicación directa entre ambas zonas está prohibida.
  En el caso que no haya sistemas que requieran la comunicación con las dos redes, entonces no sería necesario la creación de esta zona.
  Aquellos sistemas que necesiten comunicarse con las dos redes, deben situarse en esta zona. Todos los servicios que deban ser accesibles por las dos redes, deben usar un “proxy” / “reverse proxy” adecuado dentro de la Zona Expuesta de OT.
  Los sistemas dentro de esta zona deben estar habilitados únicamente para los que sea estrictamente necesario. No deberían situarse sistemas en esta zona simplemente porque sea conveniente o más fácil tenerlos ahí. Todos los sistemas en esta zona, deberán, preferiblemente, ser parte del Dominio OT y, debido a su exposición, cumplir con los estándares al crearse sus imágenes siempre que sea posible. Todos los sistemas parte del dominio Anyaccess solo están permitidos en esta zona si cumplen todos los estándares GIT.

  Ningún sistema con un riesgo de HSEC inherente o del que se dependa para las operaciones OT debe situarse en esta zona.

  Ningún sistema donde la falla del Firewall OT pueda tener un impacto en la operación debe situarse en esta zona.

  Ejemplos:
  - Un sistema con capacidad para controlar la ventilación en una mina no se permite en esta zona
  - Un sistema de CCTV que monitorea sitios o procesos sólo se permite en esta zona si hay un componente redundante en la zona OTN.
  - Un sistema que registra el uso de infraestructura y se usa para administrar mantenimiento predictivo está permitido en esta zona.

- **Las máquinas de OT no deben pertenecer al dominio AnyAccess.**
  Implementación obligatoria
  La mayoría de los sistemas en las Redes Industriales se construyen para que tengan una larga vida y suelen estas basados en tecnologías IT "viejas". A pesar de que estas tecnologías puedan ser bastante fiables, suelen estar expuestas a vulnerabilidades que nunca han sido solucionadas. Los servicios de Dominio son un clásico ejemplo. Las computadoras en Ingeniería o sistemas embebidos suelen tener versiones viejas de Windows que usan tecnologías obsoletas para la autenticación. Estas tecnologías y mecanismos, son un blanco fácil para la explotación por medio de malware como crypto lockers, virus o "backdoors". Al usar su espacio propio de autenticación, evitamos la necesidad de tener que abrir los firewalls. De esta forma, se reduce la exposición de las Redes Industriales a estas amenazas, a la vez que se evita la expansión de un malware, en caso de que un sitio haya sido infectado.

- **IT y OT deben usar esquemas IP separados.**
  Implementación opcional
  Para facilitar la gestión de nuestra red global, Glencore ha reservado partes de los rangos privados de IPv4, para cada caso específico. Las reservas son:

  - 10.0.0.0/8 Redes LAN Globales (Empresa)
  - 192.168.192.0/18 Redes DMZ Globales (Empresa)
  - 192.168.0.0/22 GroupGuest
  - 192.168.4.0/22 GroupMobility
  - **172.16.0.0/16 Redes OT (rango no gestionado globalmente)**
  - 172.31.0.0/16 IT:DMZ e IT:LAN

  Además de estos rangos, existe un rango especial reservado (RFC6598) que ha sido reusado para nuestras necesidades y destinado para grandes entornos OT:

  - **100.64.0.0/10 Large multi-site OT Networks (rango no gestionado globalmente)**

  No hay restricción en el uso de IP en el entorno de las Redes Industriales.
  Sin embargo, recomendamos encarecidamente el uso de los rangos mostrados arriba. Cualquier conflicto debido al uso de otra asignación, puede inutilizar la comunicación desde esa parte del área industrial a la Zona Expuesta y viceversa. Esto es porque el firewall de OT enviara, por defecto, las comunicaciones de vuelta al área OT (y no hacia la red IT). La red OT debe tener prioridad.
  Por lo tanto, vale la pena insistir en que las redes OT solo deberían, siempre que sea posible, usar los rangos 172.16.0.0/16 o 100.64.0.0/10 ya que son enrutables localmente. Evite usar cualquier rango que sea globalmente enrutable en las Redes Industriales.

- **Las redes OT no deben ser enrutables fuera de su localización. Cualquier enrutamiento externo debe ser por medio de NAT.**
  Implementación opcional
  Las redes superpuestas en los diferentes Entornos Industriales, impiden que sean enrutadas globalmente. Es más, el hecho que las redes OT no puedan ser enrutadas y, por lo tanto, no puedan ser accedidas externamente, añaden otra capa de seguridad para prevenir la propagación de malware o evitar el acceso no autorizado.

- **Los equipos de soporte (portátiles, dispositivos de almacenamiento) no deben cruzar entre las redes.**
  Implementacion obligatoria
  Cualquier equipo que se use en un entorno OT, no debe conectarse con ninguna red bien sea de IT o bien la red del hogar, ya que incrementa el riesgo de introducir malware en la red industrial. Stuxnet entro por medio un disco duro USB que se infectó en la computadora privada de un ingeniero en su casa.
  El personal que necesite trabajar en ambos entornos, o bien deben tener múltiples maquinas, o bien usar un "jump host" para acceder remotamente a la otra red a través de la Zona Expuesta de OT.

- **Network Access Control (NAC) debe ser adoptado.**
  Implementación obligatoria
  El acceso a las Redes Industriales, bien sea por cable o sin él, debe estar protegido por "Network Access Control". Este puede ser implementado por medio de sistemas como Cisco ISE o similares. De forma alternativa, NAC puede ser adoptado por medio de una política y sus correspondientes procesos, para asegurar que ningún aparato no autorizado, se conecta a la Red Industrial. Para redes inalámbricas también se requiere la implementación de mecanismos de autenticación seguros.

- **Los módems ADSL o GSM no se deben conectar directamente al entorno OT.**
  Implementación obligatoria
  La conectividad directa desde la Redes Industriales a Internet, está prohibida. Esto incluye el soporte remoto desde y hacia terceros. Ninguna máquina que pueda actuar como modem y abrir un enlace a internet, evitando el Firewall de OT y la Zona Expuesta, está permitido en las Redes Industriales.
  El acceso a las Redes Industriales se provee desde la Zona Segura. El acceso a páginas web especificas directamente desde la Red Industrial (por ejemplo, Soporte de Siemens o datos GPS de Caterpillar) debe ser enrutada por medio de un proxy.

- **Las maquinas Windows y Linux en el entorno OT, deben tener un Antivirus certificado por el proveedor.**

  Implementacion opcional

  Todas las maquinas en la Red Industrial deberían estar protegidas por un Antivirus. No todos los proveedores certifican su equipo para la solución preferida: Corporate Symantec SEP o pueden limitar su certificación a una versión especifica.
  Esto puede llevar a que se desplieguen múltiples soluciones de AV. Siempre que sea posible, se debe solicitar al proveedor que use nuestro estándar Global de AV. Todos los AV deben ser gestionados y monitorizados.

  Aquellos sistemas que no puedan usar ningún AV se deben proteger con medidas adicionales como estar en una red separada, restringir el protocolo de red, control de aplicación o "whitelisting" la aplicación.

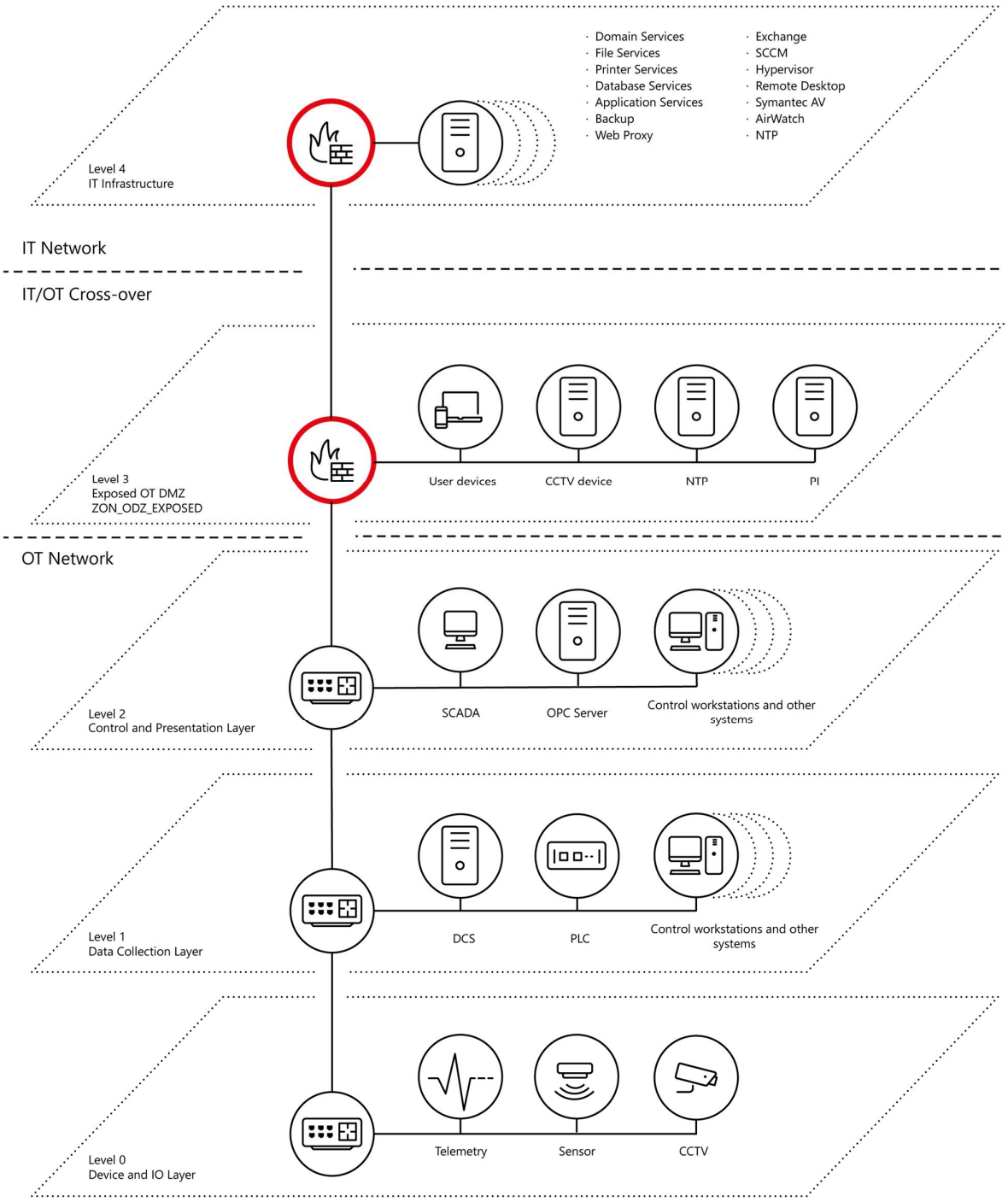
- **Las maquinas Windows y Linux en el entorno OT deben tener instalados los últimos parches del proveedor.**

  Implementacion opcional

  Todas las maquinas en la Red Industrial deben ser regularmente actualizadas con los últimos parches para el sistema operativo y las aplicaciones. Vendors of OT equipment might restrict patch deployment to certified patches only. Esto debe ser tenido en cuenta, a la hora de diseñar la solución local para la gestión de parcheado. Siempre que sea posible, se debe pedir al proveedor que certifique los últimos parches para sus sistemas.

  Aquellos sistemas que se ejecutan sobre Sistemas Operativos fuera de soporte (como Windows XP) o que no puedan usar ningún AV se deben proteger con medidas adicionales como estar en una red separada, restringir el protocolo de red, control de aplicación o "whitelisting" la aplicación.

2.4 Ejemplo de Arquitectura



** Zone naming according to the 'Global IT - Firewall Naming Standards'.*

3 Catalogo de Servicios

Los servicios que la red OT provea, no deben incluir Navegación Web, Correo o Servicios de Dominio/Autenticación. Estos solo serán provistos por la Zona Segura (capa 3).

Aquellos sistemas o servicios que necesiten estar en funcionamiento lo máximo posible, no deben estar en la Zona Expuesta de la OT, ya que la pérdida del firewall interrumpirá las comunicaciones.

Servicio	Descripción
Servicios de Archivo	Instalación para el almacenamiento compartido para archivos, con acceso seguro y copia de seguridad programada por IT.
Servicios de Impresión	Uso de las impresoras existentes y servicios como "follow-me printing" y similares.
Servicios de Base de Datos	Bases de datos de alto rendimiento usando Oracle o SQL Server con redundancia definida y monitorización del rendimiento, del espacio en discos y copias de seguridad programadas por IT.
Copia de Seguridad	Servicios de copia de seguridad usando la infraestructura y licencias de IT.
Gestión de Parches	La infraestructura de OT no debe estar en el dominio AnyAccess y, por lo tanto, no puede usar el SCCM Global. Puede usarse WSUS.
Hypervisor	Infraestructura base para sistemas virtuales.
Escritorio Remoto	Infraestructura de acceso remoto a la red OT, para ingenieros y proveedores, en un entorno controlado.
Anti-Virus	Solución AV que provee versionado y actualizaciones de patrones, controladas y monitorizadas.
Navegación Web	VDI, RDP "jump host" o una solución proxy deben usarse para navegar por la web cuando sea necesario. No se debe permitir la conexión directa desde OT a Internet.

4 Referencias

Para apoyar la implementación de estos Principios Rectores, desde la perspectiva técnica o de diseño, hemos creado un documento con el Diseño General para OT. Este documento describe las arquitecturas de referencia y las tecnologías adecuadas para la implementación de las Redes Industriales y las Zonas Expuestas de OT.

Por favor, consulte en el portal de Global IT para más detalles:

https://globalit.glencore.net/

-> Global IT Operations -> Technology Documents -> Operational Technology Cyber Security