

**Sección VI- Especificaciones Técnicas y Condiciones de
Cumplimiento**

Sección VI -VOLUMEN B

Capítulo 2 - Suministro

Anexo resumen seguridad y ciberseguridad

Tabla de contenidos

1. SUMARIO EJECUTIVO	3
1.1 General	3
2. DOCUMENTOS DE REFERENCIA.....	3
3. DOCUMENTACIÓN	4
3.1 Documentación para la gestión de equipamiento	4
3.1.1 As built	4
3.1.2 Documentación de arquitectura.....	4
3.1.3 Documentación para la continuidad del negocio.....	4
4. ESTRATEGIAS DE MITIGACIÓN Y CONTROLES	5
4.1 Repuestos de equipos físicos.....	5
4.2 Control de código	5
4.3 Medidas para el uso de puertos USB	5
4.4 Segregación de redes	5
4.5 Hardening.....	5
4.6 Actualizaciones	5
4.7 Control de acceso lógico	5
4.8 Seguridad física	6
4.9 Redundancias	6
4.9.1 Alimentación	6
4.9.2 Comunicaciones	6
4.9.3 Separación Física.....	6
5. SUPERVISION	7
6. RESPALDO y RESTAURACIÓN	7

1. SUMARIO EJECUTIVO

1.1 General

Las infraestructuras críticas son instalaciones, servicios y bienes que, en caso de ser interrumpidos o destruidos, tendrán un grave impacto social, económico y/o político. Por lo tanto, deben implementarse las medidas y controles necesarios para minimizar los riesgos y garantizar la continuidad de las operaciones.

Dada la criticidad de la temática, este documento tiene como objetivo ser un compendio y presentar a modo de resumen los principales requerimientos de ciberseguridad y seguridad físicas desarrollados a lo largo de las especificaciones técnicas, detallando para aquellos aspectos más relevantes los apartados y secciones de documentación donde se tratan los requerimientos de las ofertas. El mismo toma como base el anexo de la consultora Worley, donde aplican al alcance de la presente licitación.

2. DOCUMENTOS DE REFERENCIA

Los requerimientos presentes en las especificaciones técnicas han tenido como guía general los siguientes documentos de referencia.

Estándar	Descripción	Link
NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security	SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security CSRC (nist.gov)
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations	SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations CSRC (nist.gov)
NERC-CIP Standards	North American Reliability Corporation Critical Infrastructure Protection Standards	CIP Standards (nerc.com)
ISA/IEC 62443	Security for Industrial Automation and Control Systems (diversos documentos)	Search results for "IEC 62443" IEC Webstore

3. DOCUMENTACIÓN

3.1 Documentación para la gestión de equipamiento

3.1.1 As built

Todo el equipamiento que sea parte de la provisión deberá tener un conjunto de documentación llamado **As built**, para garantizar la resiliencia del ambiente de automatización. Se deberá suministrar la documentación que refleje de forma adecuada el sistema para la operación, el mantenimiento y el soporte, después de su aceptación y durante toda su vida útil según se detalla en **Sección VI – Volumen B – EETT Ítem I – Capítulo 2 – Inciso 10.3 “Documentación del Producto”**

3.1.2 Documentación de arquitectura

La infraestructura de automatización debe tener su documentación registrada y revisada periódicamente durante la duración del proyecto desde su creación (o para cada cambio significativo) y disponible únicamente para personas autorizadas.

Además, es recomendable que todos los elementos de automatización (lógica, herramientas de configuración y equipos físicos) tengan manuales de instalación actualizados a la fecha de entrega, guías de administración y guías de usuario para que el personal local pueda reinstalar y operar en caso de un evento de ruptura.

Se deberá suministrar según se detalla **Sección VI – Volumen B – EETT Ítem I – Capítulo 2 – Inciso 10.2 “Documentación del Proyecto”**

3.1.3 Documentación para la continuidad del negocio

Con el objeto del restablecimiento del entorno normal de operación después de una o más fallas críticas en la infraestructura del Sistema de Control se deberá suministrar un Plan de Recuperación del Sistema de Control, según se solicita en **Sección VI – Volumen B – EETT Ítem I – Capítulo 2 – Inciso 10.4 “Plan de Recuperación del Sistema de Control (PRSC)”**

Documentación “As built” de todos los sistemas instalados en el nuevo edificio GOPE y demás obras edilicias contempladas dentro de **Sección VI – Volumen C – EETT Ítem II**, incluyendo planos con detalles de sus cableados y ubicación del equipamiento, manuales de operación y mantenimiento.

Documentación “As built” de nuevas canalizaciones y enlaces de potencia, FO y telefonía tendidos, que incluyen planos con sus recorridos, ubicación de cámaras de inspección y mojoneros; ubicación de reservas. Resultados de ensayos según detallado para cada tipo de canalización y enlace en la **Sección VI – Volumen C – EETT Ítem II**

4. ESTRATEGIAS DE MITIGACIÓN Y CONTROLES

4.1 Repuestos de equipos físicos

Los componentes críticos de los sistemas de automatización deben funcionar en equipos redundante. Además, las piezas de repuesto deberán estar disponibles para que el equipo responsable sustituya estos componentes críticos en caso de necesidad. Se deberá suministrar según se detalla en **Sección VI – Volumen B – EETT Ítem I – Capítulo 1 – Inciso 13 “Repuestos”**

4.2 Control de código

Para aquellos grupos de programas que realizan actividades maliciosas, no autorizadas y potencialmente destructivas, las formas de infección son diversas, por lo que los mecanismos de protección deben ser amplios para minimizar las posibilidades de incidentes.

Los controles específicos deben implementarse utilizando herramientas de protección de *endpoints*. Se deberá suministrar según se detalla en **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 11.4.1 “Antivirus – Endpoint Protection”**.

4.3 Medidas para el uso de puertos USB

En el caso de que el uso de discos extraíbles sea necesario en la solución presentada, los dispositivos deben escanearse en una estación de escaneo con características según se detalla en **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 11.4.3 “Escaner de Almacenamiento Removable”**

Los discos extraíbles escaneados deben ser los únicos autorizados para ser identificados y abiertos por las máquinas de destino de los archivos.

4.4 Segregación de redes

A los efectos de proceder a la segregación de redes, los equipos provistos deberán permitir la implementación de VLANs de acuerdo a **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 11.5.1 “VLANs”**.

4.5 Hardening

Los puertos físicos, puertos lógicos y servicios en desuso deberán deshabilitarse en todo el equipamiento provisto de acuerdo a **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 11.4.2 “Hardening” e Inciso 11.5.2 “Hardening”**.

4.6 Actualizaciones

Los sistemas generalmente tienen errores y vulnerabilidades que requieren actualizaciones o instalaciones de parches. Debe implementarse una metodología según indica **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 11.6 “Administración de Parches y Actualizaciones”**.

4.7 Control de acceso lógico

El acceso lógico a la infraestructura debe basarse en la identificación y autorización de usuarios. En términos generales, debe haber un proceso de autorización y registro para todos los usuarios, así como mantener los registros de acceso. Tanto las herramientas necesarias para ello como demás características que debe cumplir se detallan en **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 11.2 “Autenticación y Autorización”**.

4.8 Seguridad física

Deben aplicarse procedimientos de control de acceso físico para restringir el acceso a las áreas con equipos con capacidad de mando y control. En estos recintos se debe incluir al menos el uso de alarma contra intrusos, CCTV y Control de Acceso de acuerdo a lo especificado en **Sección VI – Volumen C – EETT Ítem II – Capítulo 1 – Inciso 22.2.8 “CCTV” e Inciso 22.2.10 “Control de Acceso”**.

Sistema de video vigilancia (CCTV) con grabación remota en servidor suministrado por SG y monitoreo 24 hs desde el Centro de Seguridad y protección según indicado en la **Sección VI – Volumen C – EETT Ítem II**.

Tableros de Nivel 1 con llave y sensores de puerta abierta según detallado en **Sección VI – Volumen B – EETT Ítem I – Capítulo 5**.

Sistema de protección contra intrusos (Alarma y barreras infrarrojas perimetrales), con conexión remota al Centro de Seguridad y Protección para su monitoreo según sección, según **Sección VI – Volumen C – EETT Ítem II**.

Cerco perimetral del Edificio del Centro de Control, según **Sección VI – Volumen C – EETT Ítem II**.

Sistema de extinción de incendios según, según **Sección VI – Volumen C – EETT Ítem II**.

4.9 Redundancias

4.9.1 Alimentación

Se deberán seguir los lineamientos de incorporación, en el COU, de fuentes de alimentación redundante (incluyendo múltiples acometidas, bancos de batería y generador diésel de emergencia) definidos en **Sección VI – Volumen C – EETT Ítem II**. Como así también los requisitos particulares definidos para el equipamiento, donde se solicita múltiples fuentes de alimentación.

4.9.2 Comunicaciones

Se deberán seguir los lineamientos de separación física de las distintas trazas de fibra óptica en aras de lograr independencia de caminos y redundancia según **"Anexo 01 Requerimientos enlaces FO", Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 3.3.4 “Cableado y Canalizaciones”**

4.9.3 Separación Física

Para el Nivel 3 y Nivel 2 de control, el equipamiento redundante deberá instalarse separado geográficamente en cada margen de la Central, de manera tal que el equipamiento en operación y su respaldo en stand by se encuentren separados geográficamente como se indica en **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 y Volumen B – EETT Ítem I – Capítulo 4.**

4.10 Controles para adecuación al modelo de zonas y conductos de la norma IEC 62443

Los equipos del ambiente de automatización que comparten características y requisitos de seguridad comunes deben organizarse en zonas físicas, lógicas y/o de seguridad.

Las zonas de confianza desde el punto de vista de IEC 62443 son redes que forman parte de la automatización y contienen dispositivos de campo. Las subredes de automatización deben segregarse con el control de aplicaciones, contenido y usuarios (enrutamiento a través de firewall de próxima generación) de modo que solo se produzca el tráfico necesario entre ellas.

Existe una zona que no es de confianza desde el punto de vista de IEC 62443, se trata de la DMZ. Se detalla las características del Ambiente DMZ en **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 9 “Ambiente DMZ”**. Los accesos remotos provenientes de redes no gestionadas y con destino equipos del Ambiente DMZ, se deberán resguardar de acuerdo a lo detallado en **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 11.1.3 “Acceso Remoto a DMZ”**.

Para el caso del conducto que vincula la Red DMZ con la Red N3 se deberá implementar una protección basada en Diodos de Datos según se describe en **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 11.1.2 “Protección entre Dominios”**.

Tanto estas conexiones a la DMZ como las demás conexiones entre zonas de distintas características de seguridad, deben también ser supervisadas permanentemente y protegidas por firewalls de próxima generación (NGFW) de acuerdo a **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 11.1.1 “Firewalls”**.

5. SUPERVISION

Debe haber un proceso de supervisión y control de las actividades del ambiente de automatización con el fin de analizar el estado de la instalación y permitir que se tomen medidas para tratar la situación, de acuerdo a lo especificado en **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 11.3 “Supervisión y Gestión”**.

6. RESPALDO y RESTAURACIÓN

En el contexto de exposición a riesgos tanto internos como externos, contar con un sistema de respaldo y restauración no solo es una buena práctica, sino una necesidad estratégica de acuerdo a los marcos de referencia y las familias de normas para sistemas de automatización. No se trata únicamente de salvaguardar información si no de la capacidad de restaurar rápidamente la operación de los sistemas a partir de copias confiables, verificadas y protegidas. En **Sección VI – Volumen B – EETT Ítem I – Capítulo 3 – Inciso 11.7**

“Respaldo y Restauración” e Inciso 6.7.4 “Procedimientos de Contingencia” se encuentran las características solicitadas para su cumplimiento.

Preliminar