Propuesta metodológica para la implementación de buenas prácticas y procedimientos de verificación de ciberseguridad aplicado a los sistemas SCADA utilizados en el sector eléctrico

Christian Marcelo Gallardo Yanchapaxi, Escuela Politécnica Nacional (EPN), Quito – Ecuador
Gabriel Roberto López Fonseca, Escuela Politécnica Nacional (EPN), Quito – Ecuador
Franklin Leonel Sánchez Catota, Escuela Politécnica Nacional (EPN), Quito - Ecuador

Resumen **— Se cubre el estudio de los sistemas SCADA, los estándares NERC CIP V.5 e ISO/IEC 27002:2013. Con el conocimiento adquirido se realiza la integración considerando los requerimientos del NERC CIP-007-6 (Seguridad cibernética - Gestión de seguridad del sistema) y los objetivos de control de ISO/IEC 27002:2013 (Dominio en Seguridad en las telecomunicaciones), la integración es la base para la implementación de buenas prácticas y procedimientos de verificación de ciberseguridad aplicado a los sistemas SCADA utilizados en el sector eléctrico.**

Índices *— NERC CIP v 5; ISO/IEC 27002:2013; SCADA; informatics security*

I. Introducción

Los sistemas SCADA son utilizados en el sector industrial para adquirir la información en tiempo real, supervisar y controlar procesos industriales a distancia [1]. Uno de los sectores industriales, y el que es considerado para el presente trabajo, es el sector eléctrico, para el cual a fin de garantizar la seguridad informática se toman en cuenta los estándares NERC CIP V.5 y la norma ISO / IEC 27002:2013 que son utilizados para elaborar la guía de buenas prácticas de seguridad informática y los procedimientos para verificar la seguridad informática de los sistemas SCADA utilizados en el sector eléctrico.

II. Sistemas SCADA en el sector eléctrico

Los sistemas SCADA utilizados en el sector eléctrico son identificados como SCADA/EMS, el término Energy Management System (EMS, Sistema de administración de energía), hace referencia al software de gestión de datos mediante aplicaciones que monitorean las variables del sistema eléctrico (como ejemplo, las variables pueden ser de: voltaje, corriente, potencia, estado de interruptores, estado de seccionadores, temperatura de funcionamiento de equipos, devanados en transformadores, etc.), y que permite la generación de reportes sobre los cuales se basan las decisiones al momento de ejecutar acciones sobre el sistema eléctrico.

La arquitectura básica del sistema SCADA/EMS se presenta en la Fig. 1, los elementos que intervienen para su funcionamiento son descritos a continuación.

A. Human Machine Interface (HMI, Interface Hombre Máquina)

La HMI es la interfaz entre el proceso industrial y los operadores. Entre algunas de las funcionalidades de las HMI se tienen: sirven para traducir las variables del proceso complejas en información útil y aprovechable, mostrar la información operativa en tiempo real, proporcionan un conocimiento operacional del proceso, y permite a los operadores coordinan y controlan los procesos industriales.

B. Master Terminal Unit (MTU, Unidad Terminal Maestra)

La MTU es el componente principal del sistema SCADA, la MTU puede ser categorizada de dos maneras: Sistema SCADA pequeño, la MTU puede estar en un solo computador. Sistema SCADA grande, a MTU puede ser una infraestructura tecnológica que abarca servidores, equipos de networking, software, etc.

La MTU se encarga principalmente de:

- Adquisición de datos: recolección de datos de la Unidad Terminal Remota.
- Salvado de información: el almacenamiento se realiza en bases de datos, esta información al ser procesada es presentada al operador.
- Manejo de eventos: la información que es almacenada en las bases de datos proviene de unidades remotas, la MTU analiza esta información en busca de patrones fuera de lo normal que permitan identificar eventos que podrían causar daño en el sistema.
- Manejo de diagramas unifilares: son la representación gráfica de los equipos que se encuentran en campo y también representan los datos que los equipos están generando o recibiendo.
- Generación de reportes: esta funcionalidad permite elaborar automáticamente reportes con información que el operador haya seleccionado para el contenido, generalmente se dispone de un servidor dedicado para esta actividad a fin de evitar afectación del performance del sistema.
- Manejo de contingencias del sistema: una buena práctica es utilizar contingencias de la MTU a fin de garantizar la continuidad del servicio en caso de afectación a uno de los elementos que constituye el sistema, esta contingencia implica disponer de

equipamiento para el sistema principal y equipamiento de iguales prestaciones para el sistema de respaldo.

- Conectividad entre sistemas: garantiza la inter operatividad entre sistemas mediante el manejo de protocolos de comunicación, esta funcionalidad permite agregar servicios de apoyo al sistema SCADA.
- Seguridad electrónica: el acceso a los dispositivos del sistema es controlado mediante políticas de seguridad, que al menos considera perfiles de los usuarios, tipo de usuarios, permisos de archivos y origen del acceso.
- Administración de la red SCADA: mediante el constante monitoreo de: redes LAN/WAN, performance de los servidores y consolas, accesos locales y remotos, y logs generados por cada uno de los elementos que constituyen el sistema.
- Bases de datos: permite la administración de la información almacenada que procede de campo, como la información generada localmente.
- Software de aplicaciones: En base a la información almacenada en la base de datos es posible recrear eventos de estudio, que permiten identificar el impacto en el sistema en caso de falla de sus componentes, esto permite identificar puntos de falla únicos y tomar decisiones sobre la implementación de contingencias.

C. Remote Unit (RU, Unidad Remota)

La unidad remota es un dispositivo que se encuentra en campo y es la encargada de realizar la supervisión y control del sistema, la información que es gestionada por la unidad remota es remitida hacia la MTU por enlaces de comunicación, algunos de los elementos considerados como unidades remotas son:

- *Remote Terminal Unit* (RTU, Unidad Terminal Remota). Las funcionalidades principales de las RTU son recopilar y procesar la información de los elementos que se encuentran en campo, aplicar medidas de seguridad para los accesos locales y remotos, y notificación de eventos considerados anormales que pudieran causar falla en el funcionamiento del sistema.
- *Programmable Logic Controller* (PLC, Controlador Lógico Programable). La funcionalidade principale de los PLC es realizar el control de la maquinaria, disponen de aplicativos embebidos que permiten realizar el procesamiento de información localmente sin la necesidad de remitir toda la información hacia las MTU para que este los procese.
- *Intelligent Electronic Device* (IED, Dispositivo Electrónico Inteligente). La funcionalidad principal de los IED son realizar el control de la maquinaria, mantener la comunicación con los elementos de campo y hacer auto configuraciones para mantener la regulación de los datos generados por la maquinaria en campo, esto se logra ya que los IED son considerados como elementos inteligentes por el software que mantiene embebido y mediante la ejecución de algoritmos es capaz de realizar tomas de decisiones y realizar ajustes sobre los equipos de campo.

D. Redes de comunicación industrial

Una de las funcionalidades de los sistemas SCADA es el control de maquinaria industrial, esto implica que, el ambiente en el cual se encuentran tanto el equipo de networking como medios de comunicación están expuestos a ruido electromagnético, es así que aparece el concepto de redes de comunicación industrial, este tipo de redes debe garantizar el transporte de información en tiempo real en condiciones ambientales extremas, este tipo de comunicaciones se clasifica en dos áreas:

- Comunicación desde los dispositivos de campo hacia el centro de control. Para esta comunicación se requiere de los protocolos orientados al telecontrol en sistemas SCADA.
- Comunicación entre dispositivos de capo. Para esta comunicación se requiere de los protocolos industriales utilizados en buses de campo. El bus de campo es un sistema de transmisión de datos entre los dispositivos que se encuentran en la planta industrial.

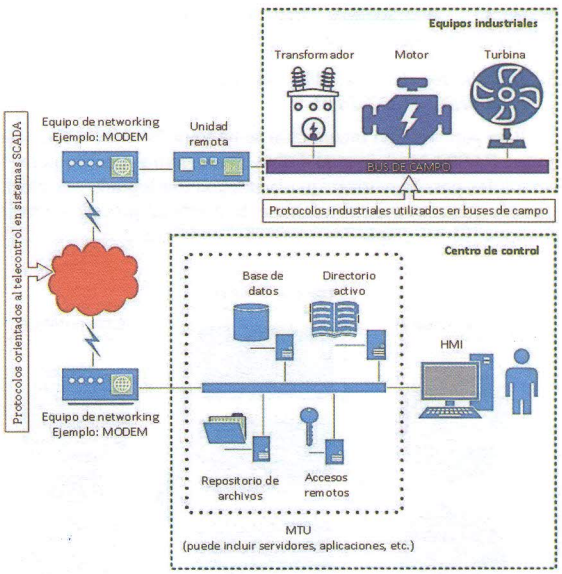

Fig. 1. Arquitectura básica del sistema SCADA/EMS.

III. CIBERSEGURIDAD EN SISTEMAS SCADA/EMS

Los sistemas SCADA han comenzado a trabajar con tecnologías y protocolos estándar y conocidos por todos, como suelen estar distribuidos geográficamente se conectan a centros de supervisión y control mediante tecnologías y protocolos estándar (como ejemplo: TCP. Protocolo de Control de Transmisión / IP. Protocolo de Internet.), y a su vez estos centros suelen estar conectados a la red corporativa de la empresa o institución propietaria del proceso, y a través de esta red, a Internet.

Por este motivo la preocupación por la seguridad de los sistemas industriales ha sido creciente, a fin de garantizar la seguridad informática en sistemas SCADA/EMS, se toman en cuenta los estándares de protección a infraestructuras críticas

NERC CIP V.5 (que es específico para el sector eléctrico) y la norma ISO/IEC 27002:2013 (que es general para cualquier organización), a fin de desarrollar una metodología para la implementación de buenas prácticas y procedimientos de verificación de seguridad informática aplicada al sistema SCADA/EMS.

IV. METODOLOGÍA

El objetivo de integrar el estándar NERC CIP V.5 y la norma ISO/IEC 27002:2013 es que se obtendrán controles de seguridad informática, que permitirán generar la guía de buenas prácticas para implementar los mecanismos de seguridad informática en el sistema SCADA/EMS, así como los procedimientos que permitan verificar que estas buenas prácticas se cumplan. La metodología dispone de fases que son descritas a continuación.

A. Identificación de activos de información

Se tiene como propósito, identificar y categorizar los activos cibernéticos críticos, basados en el impacto de sus instalaciones, sistemas y equipos asociados, los cuales, si son destruidos, degradados, mal utilizados o deshabilitados afectarían el funcionamiento del sistema eléctrico.

B. Integración de los estándares NERC CIP V.5 e ISO/IEC 27002:2013

Para garantizar la integración se ha tomado como referencia la norma PAS99:2012, la cual define cuatro etapas que requieren ser cumplidas para garantizar que la integración lograda sea efectiva y pueda fácilmente ser actualizada mediante un proceso de mejora continua [2], las etapas son mostradas en la Fig. 2.

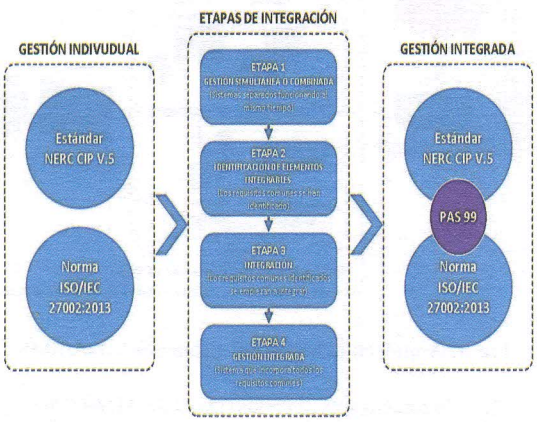

Fig. 2. Etapas de integración.

1) Etapa 1. Gestión simultanea o combinada.

Para iniciar con la integración del estándar NERC CIP V.5 y la norma ISO/IEC 27002:2013, se requiere identificar la forma en la cual se está realizando la gestión actualmente, generalmente se dispone de dos tipos de gestiones.

- Gestión simultánea, se considera que tanto NERC CIP V.5 como ISO/IEC 27002:2013 se están aplicando de forma separados funcionando al mismo tiempo.
- Gestión combinada, se considera que tanto NERC CIP V.5 como ISO/IEC 27002:2013 se están aplicando de forma no holística.

Se considera como punto de partida una gestión independiente de las normas. Los elementos que serán integrados son presentados tanto por el estándar NERC CIP V.5 en la Tabla I como la norma ISO/IEC 27002:2013 en la Tabla II.

TABLA I
NERC CIP V.5

CIP	Descripción
CIP-002-5.1a	Seguridad cibernética - Categorización del sistema cibernético [3].
CIP-003-6	Seguridad cibernética - Controles de gestión de seguridad [4].
CIP-004-6	Seguridad cibernética - Personal y formación [5].
CIP-005-5	Seguridad cibernética - Perímetro electrónico de seguridad [6].
CIP-006-6	Seguridad cibernética - Seguridad física de los sistemas cibernéticos [7].
CIP-007-6	Seguridad cibernética - Gestión de seguridad del sistema [8].
CIP-008-5	Seguridad cibernética - Reporte de incidentes y planificación de respuesta [9].
CIP-009-6	Seguridad cibernética - Planes de recuperación de sistemas cibernéticos [10].
CIP-010-2	Seguridad cibernética - Gestión del cambio de configuración y evaluaciones de vulnerabilidad [11].
CIP-011-2	Seguridad cibernética - Protección de la información [12].
CIP-014-2	Seguridad física [13].

TABLA II
ISO/IEC 27002:2013

Dominio	Descripción
5	Políticas de seguridad [14].
6	Aspectos organizativos de la seguridad de la información [15].
7	Seguridad ligada a los recursos humanos [16].
8	Gestión de activos [17].
9	Control de accesos [18].
10	Cifrado [19].
11	Seguridad física y ambiental [20].
12	Seguridad en la operativa [21].
13	Seguridad en las telecomunicaciones [22].
14	Adquisición, desarrollo y mantenimiento de los sistemas de información [23].
15	Relaciones con suministradores [24].
16	Gestión de incidentes en la seguridad de la información [25].
17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio [26].
18	Cumplimiento [27].

2) Etapa 2. Identificación de elementos integrables.

En esta etapa se consideran a nivel macro los elementos que pueden o no integrarse de forma óptima, el resultado de esta identificación se presenta en la Tabla III y servirá de referencia para la etapa siguiente, en la cual la integración será realizada a detalle.

TABLA III
IDENTIFICACIÓN A NIVEL MACRO DE LOS ELEMENTOS QUE PUEDEN O NO SER INTEGRADOS

ISO/IEC 27002:2013 (Domain)	NERC CIP V.5 (CIP)
5. Políticas de seguridad	No aplica
6. Aspectos organizativos de la seguridad de la información	CIP-003-6. Seguridad cibernética - Controles de gestión de seguridad
7. Seguridad ligada a los recursos humanos	CIP-004-6. Seguridad cibernética - Personal y formación

ISO/IEC 27002:2013 (Domain)	NERC CIP V.5 (CIP)
8. Gestión de activos	CIP-002-5.1a. Seguridad cibernética - Categorización del sistema cibernético
9. Control de accesos	CIP-005-5. Seguridad cibernética - Perímetro electrónico de seguridad
10. Cifrado	CIP-011-2. Seguridad cibernética - Protección de la información
11. Seguridad física y ambiental	CIP-006-6. Seguridad cibernética - Seguridad física de los sistemas cibernéticos
12. Seguridad en la operativa	No aplica
13. Seguridad en las telecomunicaciones	CIP-007-6. Seguridad cibernética - Gestión de seguridad del sistema
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	CIP-010-2. Seguridad cibernética - Gestión del cambio de configuración y evaluaciones de vulnerabilidad
15. Relaciones con suministradores	Does Not apply
16. Gestión de incidentes en la seguridad de la información	CIP-008-5. Seguridad cibernética - Reporte de incidentes y planificación de respuesta
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	No aplica
18. Cumplimiento	No aplica
No aplica	CIP-009-6. Seguridad cibernética - Planes de recuperación de sistemas cibernéticos
No aplica	CIP-014-2. Seguridad física

3) Etapa 3. Integración.

En esta etapa la integración se realiza a detalle, en esta etapa tiene mucho valor el juicio de experto, el cual es un criterio emitido por el personal que por su formación académica y su experiencia laboral aporta con ideas claras y precisas dadas como válidas al momento de realizar la integración.

Hay que recordar que, el estándar NERC CIP V.5 trabaja con requerimientos, mientras que la norma ISO/IEC 27002:2013 trabaja con controles. Al momento de realizar la integración da como resultado los "controles de seguridad informática" que han sido así nombrados a juicio de experto. Finalmente, en la Tabla IV se presenta el resultado de la integración del estándar NERC CIP V.5 y la norma ISO/IEC 27002:2013.

TABLA IV
RESULTADO DE LA INTEGRACIÓN DE LOS ESTÁNDARES NERC CIP V.5 E ISO / IEC 27002: 2013

CONTROLES DE CIBERSEGURIDAD	NERC CIP V.5	ISO/IEC 27002:2013
Inventario de dispositivos autorizados y no autorizados	CIP-002-5.1a R1 CIP-002-5.1a R2	8.1.1 9.1.2 13.1.1
Inventario de software autorizado y no autorizado	No aplica	12.5.1 12.6.2
Configuraciones seguras para hardware y software	CIP-007-6 R2 CIP-010-2 R2	14.2.4 14.2.8 18.2.3
Evaluación continua de la vulnerabilidad y remediación	CIP-007-6 R2 CIP-010-2 R3	12.6.1 14.2.8 14.2.9 14.3.1
Tipo de usuarios	CIP-004-6 R4 CIP-004-6 R5 CIP-007-6 R5	9.1.1 9.2.2 - 9.2.6 9.3.1 9.4.1 - 9.4.4
Registros de acceso y tráfico de red	CIP-007-6 R4	12.4.1 - 12.4.4 12.7.1
Protecciones de correo electrónico y navegador web	CIP-007-6 R2 CIP-010-2 R2	14.2.4 14.2.8 18.2.3
Prevención de código malicioso	CIP-007-6 R3	8.3.1 12.2.1 13.2.3
Puertos y servicios	CIP-007-6 R1	9.1.2 13.1.1 13.1.2 14.1.2
Respaldos	No aplica	10.1.1 12.3.1
Accesos electrónicos	CIP-005-5 R1 CIP-007-6 R2	9.1.2 13.1.1 13.1.3 14.1.1
Defensa de Límites	CIP-005-5 R1 CIP-005-5 R2 CIP-007-6 R4	9.1.2 12.4.1 12.7.1 13.1.1 13.1.3 13.2.3
Protección de Datos	CIP-011-2 R1 CIP-011-2 R2	8.3.1 - 8.3.3 10.1.1 - 10.1.2 13.2.3 18.1.5
Acceso Controlado Basado en la Necesidad de Saber	CIP-005-5 R1 CIP-005-5 R2 CIP-007-6 R4 CIP-011-2 R1	8.3.1 9.1.1 10.1.1
Control de acceso inalámbrico	CIP-007-6 R4	10.1.1 12.4.1 12.7.1
Cuentas genéricas	CIP-005-5 R1 CIP-005-5 R2 CIP-007-6 R4	9.1.1 9.2.1 - 9.2.6 9.3.1 9.4.1 - 9.4.3 11.2.8
Evaluación de habilidades de seguridad y capacitación apropiada para llenar vacíos	CIP-004-6 R1 CIP-004-6 R2	7.2.2
Seguridad del software de aplicación	No aplica	9.4.5 12.1.4 14.2.1 14.2.6 - 14.2.8
Respuesta y gestión de incidentes	CIP-008-5 R1 CIP-008-5 R2 CIP-008-5 R3	7.2.1 16.1.1 - 16.1.7
Pruebas de penetración y ejercicios de equipo rojo	No aplica	14.2.8 18.2.1 18.2.3
Integridad del software	CIP-010-2 R1	13.2.1 14.2.2 - 14.2.5
Permisos de archivos	No aplica	13.2.1
Comunicación segura	No aplica	13.1.1 13.2.1 13.2.2 14.1.3
Parches de seguridad	CIP-007-6 R2	No aplica
Autorización de accesos	CIP-007-6 R5	No aplica
Capacitación en seguridad informática	CIP-004-6 R1 CIP-004-6 R2 CIP-004-6 R3	7.2.2
Monitoreo de eventos	CIP-007-6 R4	No aplica
Acuerdos de confidencialidad	No aplica	13.2.4 18.2.2

CONTROLES DE CIBERSEGURIDAD	NERC CIP V.5	ISO/IEC 27002:2013
Políticas de seguridad cibernética	CIP-003-6 R1 CIP-003-6 R2	5.1.1 5.1.2
Responsabilidad de las políticas de seguridad cibernética	CIP-003-6 R3 CIP-003-6 R4	6.1.1 6.1.2
Contacto interno	No aplica	6.1.3 - 6.1.5
Trabajo remoto	CIP-005-5 R2	6.2.1 6.2.2
Antecedentes de contratación de personal	No aplica	7.1.1 7.1.2
Sanciones para los empleados que han provocado alguna violación de seguridad	No aplica	7.2.3
Cese o cambio de funciones	No aplica	7.3.1
Administración de los activos de información	CIP-002-5.1a R1 CIP-002-5.1a R2	8.1.1 - 8.1.4 8.2.3
Etiquetado y manejo de información	No aplica	8.2.1 8.2.2
Seguridad física	CIP-006-6 R1 CIP-006-6 R2 CIP-006-6 R3 CIP-014-2 R5 CIP-014-2 R6	11.1.1 - 11.1.6 11.2.9
Plan de recuperación	CIP-009-6 R1 CIP-009-6 R2 CIP-009-6 R3	No aplica
Administración del riesgo	CIP-014-2 R1 CIP-014-2 R2 CIP-014-2 R3 CIP-014-2 R4	No aplica
Seguridad de los equipos	No aplica	11.2.1 - 11.2.7
Procedimientos de operación	No aplica	12.1.1 - 12.1.3
Seguridad de la información en las relaciones con suministradores	No aplica	15.1.1 - 15.1.3
Gestión de la prestación del servicio por suministradores	No aplica	15.2.1 - 15.2.2
Continuidad de la seguridad de la información	No aplica	17.1.1 - 17.1.3
Redundancias	No aplica	17.2.1
Cumplimiento de los requisitos legales y contractuales	No aplica	18.1.1 - 18.1.5

4) Etapa 4. Gestión integrada.

Una vez finalizada la integración del estándar NERC CIP V.5 y la norma ISO/IEC 27002:2013 debe realizarse un monitoreo constante para garantizar la continuidad y mejora del resultado de la integración obtenida, para lo cual se considera la metodología PDCA (Plan, Do, Check, Act).

La metodología PDCA, también conocida como Ciclo Deming, consiste en una serie cuatro pasos que deben ser ejecutados de forma ordenada para lograr la mejora continua de la calidad. En la Fig. 3 se presentan las etapas con una breve descripción del propósito de cada una de ellas.

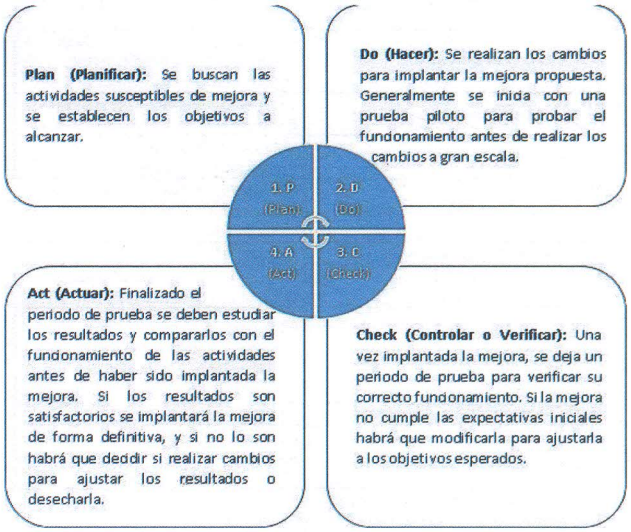

Fig. 3. Ciclo Deming.

C. Guía de buenas prácticas de ciberseguridad para sistemas SCADA/EMS

Se elabora la guía de buenas prácticas, la cual presenta requerimientos a manera de recomendaciones, que de ser acogidas, robustecerán la seguridad informática del sistema SCADA/EMS. La guía se encuentra jerárquicamente clasificada por categorías y controles como se indica en la Tabla V, los cuales son interpretados de la siguiente manera:

- Categorías, agrupa los controles que de acuerdo a su propósito mantienen relación.
- Controles de seguridad informática, son el resultado de la integración del estándar NERC CIP V.5 y la norma ISO/IEC 27002:2013, a fin de centrar el estudio en el centro de control, se consideran los controles de seguridad informática que hacen referencia al estándar CIP-007-6 (Seguridad cibernética - Gestión de seguridad del sistema) y la norma ISO/IEC 27002:2013 (Dominio 13. Seguridad en las telecomunicaciones).

  A fin de mantener un manejo didáctico de la guía de buenas prácticas, se considerará a los "controles de seguridad informática" solo con el nombre reducido de "controles".

TABLA V

RELACIÓN ENTRE CATEGORIAS Y CONTROLES

CATEGORÍA	CONTROLES	PROPÓSITO DEL CONTROL
Accesos locales y remotos	Registros de acceso y tráfico de red	Registrar los eventos relacionados con accesos de usuarios y tráfico de red, y generar evidencias.
	Autorización de accesos	Garantizar la correcta configuración de los métodos de autorización de acceso.

CATEGORÍA	CONTROLES	PROPÓSITO DEL CONTROL
Usuarios de dominio del sistema	Cuentas genéricas	Retirar todas las cuentas genéricas y por defecto.
	Tipo de usuarios	Verificar la definición del tipo de usuarios para acceso al sistema operativo, servidores, consolas, aplicativos y equipos de comunicación, definir permisos por cada usuario para realizar tareas estadísticas y/o modificación de la configuración en los equipos, incluyendo pero no limitados a los siguientes grupos: súper usuarios, administradores de la aplicación y usuarios locales.
Actualizaciones del Sistema	Parches de seguridad	Verificar que todo el software hubiese sido actualizado con los parches de seguridad más recientes y aplicables al sistema.
	Prevención de código malicioso	Mantener activa y actualizada la herramienta (s) de prevención de código malicioso.
	Integridad del software	Prevenir y detectar cambios no autorizados en el sistema cibernético mediante la gestión de cambios de configuración.
	Respaldos	Garantizar que se realice el respaldo de información necesaria para restablecer las actividades en caso de ser requerido.
Configuraciones de hardening	Puertos y servicios	Habilitar los puertos y servicios necesarios para el funcionamiento del sistema.
	Permisos de archivos	Validar que todos los permisos de los archivos (escritura, lectura y/o ejecución) de los servidores y consolas sean los exclusivamente necesarios, para el buen funcionamiento del sistema SCADA y software de base.
	Comunicación segura	Mantener la protección de la información que pasa por medios de telecomunicaciones.
	Accesos electrónicos	Mantener configuraciones de hardening en los equipos de networking.
Monitoreo del Sistema	Monitoreo de eventos	Configurar el envío de logs de los equipos del sistema a un repositorio con capacidad de almacenar la información y generar estadísticas.
Recurso humano	Capacitación en seguridad informática	Revisar la vigencia de capacitación en seguridad informática del personal que tiene acceso al sistema.
	Acuerdos de confidencialidad	Mantener acuerdos de confidencialidad del personal, de tal manera de garantizar el acceso y utilización responsable de los recursos del sistema

D. Procedimientos de verificación de ciberseguridad aplicados al sistema SCADA/EMS

Una vez identificados los controles de seguridad informática, se requiere validar cuantitativamente el grado de cumplimiento de los controles, para lo cual se elaboran los procedimientos de verificación de seguridad informática que serán ejecutados sobre los activos que forman parte del centro de control.

Los valores obtenidos como resultado de la ejecución de los procedimientos de verificación serán contrastados con una escala de cumplimiento definida a fin de identificar el nivel de seguridad del sistema SCADA/EMS.

E. Escala de cumplimiento

La escala de cumplimiento, que se presenta en la Tabla VI, permite cuantificar el nivel de madurez del control de seguridad informática e identificar cual activo presenta o no falencias en cuanto a protección. Para identificar la escala de cumplimiento se tomó como referencia:

- Los criterios de evaluación estipulados por la ISO/IEC 15504 [28]
- El criterio del personal que forma parte del sector eléctrico, que por su trayectoria y conocimientos son considerados especialistas en sistemas SCADA/EMS.

TABLA VI
ESCALA DE CUMPLIMIENTO

Scale	Description	Rank
Completamente alcanzado	Hay evidencia de una aproximación o logro total de que el control cumpla con su objetivo.	85% al 100%
Ampliamente alcanzado	Hay evidencia de un logro significativo de que el control cumpla con su objetivo, puede presentarse inconsistencias en algunas consideraciones del control.	50% al 85%
Parcialmente alcanzado	Hay alguna evidencia de que el control cumpla con su objetivo, pero algunos aspectos del control no han sido implementados completamente.	15% al 50%
No alcanzado	Hay poca o ninguna evidencia de que el control cumpla con su objetivo.	0% al 15%

Se considera que el control de seguridad informática cumple con su propósito cuando el nivel alcanzado se encuentra en la escala "Completamente alcanzado".

F. Contraste de los valores obtenidos como resultado de la ejecución de los procedimientos de verificación de ciberseguridad con la escala de cumplimiento

Mediante la ejecución de los procedimientos de verificación se validó cuantitativamente el grado de cumplimiento de los controles de seguridad informática, estos valores son contrastados con la escala de cumplimiento a fin de identificar el nivel de seguridad informática del sistema SCADA/EMS.

V. Resultados

De la ejecución de los procedimientos de verificación es posible validar cuantitativamente el grado de cumplimiento de los controles definidos en la guía de buenas prácticas de seguridad informática, estos valores al ser contrastados con la escala de cumplimiento permite identificar cual activo presenta o no falencias en cuanto a protección e identificar el nivel de seguridad informática del sistema SCADA/EMS.

A manera de caso práctico, la metodología fue aplicada a una empresa del sector eléctrico Ecuatoriano que dispone de un SCADA/EMS, obteniéndose los resultados que son presentados a continuación.

A. Resultados individuales

En la Fig. 4 se presenta gráficamente el contraste de los valores obtenidos como resultado de la ejecución de los procedimientos de verificación de ciberseguridad con la escala de cumplimiento, de lo cual se evidencia que:

- Los controles que si alcanzaron la escala "Completamente alcanzado" son: registros de acceso y tráfico de red, autorización de accesos, prevención de código malicioso, integridad del software, permisos de archivos y comunicación segura. Para estos casos, no se requiere tomar acciones preventivas ni correctivas.
- Los controles que no alcanzaron la escala "Completamente alcanzado" son: cuentas genéricas, tipo de usuarios, respaldos, puertos y servicios, parches de seguridad, accesos electrónicos, monitoreo de eventos, capacitación en seguridad informática y acuerdos de confidencialidad. Para estos casos, se han identificado los activos de información que provocaron el no cumplimiento y sobre los cuales se requiere tomar acciones correctivas.

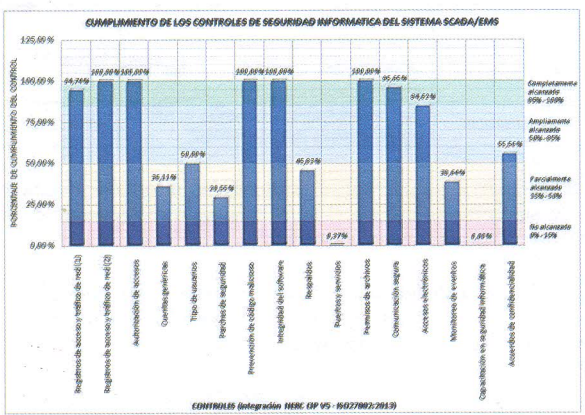

Fig. 4. Contraste de los valores obtenidos como resultado de la ejecución de los procedimientos de verificación de ciberseguridad con la escala de cumplimiento.

B. Resultado global

En la Fig. 5 se presenta gráficamente el contraste del valor global obtenido obtenidos como resultado de la ejecución de los procedimientos de verificación de ciberseguridad con la escala de cumplimiento, de lo cual se evidencia que:

El valor del cumplimiento global de seguridad informática del sistema SCADA/EMS no alcanza la escala "Completamente alcanzado", es decir, se considera que el sistema es altamente propenso a sufrir ataques informáticos exitosos, los cuales afectarían las funcionalidades del sistema SCADA/EMS. Considerando esta realidad, ahora identificada de forma cuantitativa, se requiere buscar soluciones que permitan ubicar el porcentaje de cumplimiento global en la escala "Completamente alcanzado".

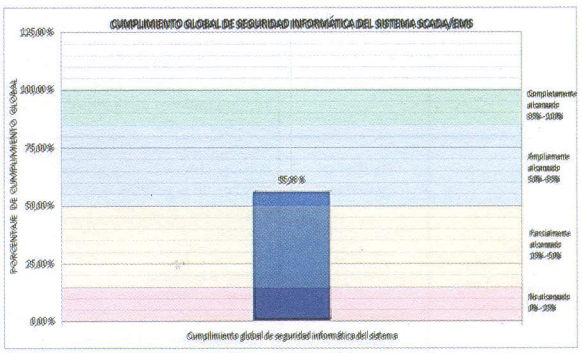

Fig. 5. Contraste del valor global obtenido obtenidos como resultado de la ejecución de los procedimientos de verificación de ciberseguridad con la escala de cumplimiento

VI. Conclusiones

La metodología propuesta ha permitido generar la guía de buenas prácticas de seguridad informática para el sistema SCADA/EMS y sus procedimientos de verificación, con lo cual es posible determinar el nivel de seguridad informática del sistema SCADA/EMS.

La elaboración de la guía de buenas prácticas de seguridad informática para el sistema SCADA/EMS y la elaboración de procedimientos de verificación, fueron realizados en base a la integración del estándar NERC CIP-007-6 (Seguridad cibernética - Gestión de seguridad del sistema) y la norma ISO/IEC 27002:2013 (Dominio Seguridad en las Telecomunicaciones).

La integración del estándar NERC CIP V.5 (que es específico para el sector eléctrico) y la norma ISO/IEC 27002:2013 (que es general para cualquier organización) se realizó considerando la norma PAS99:2012, la cual da los lineamientos a ser considerados para realizar la integración de varios estándares.

VII. Referencias

[1] L. E. Chavarría, "SCADA SYSTEM´S & TELEMETRY," Atlantic International University, Mexico, Oct 2007.

[2] J. L. Miguel, "PAS99: Especificación de los requisitos comunes del sistema de gestión como marco para la integración," INNOVACION/ARTÍCULO, pp. 11-12, Mar 2013.

[3] CIP-002-5.1a (Cyber Security — BES Cyber System Categorization), NERC-CIP Standard Version 5, 2014.

[4] CIP-003-6 (Cyber Security - Security Management Controls), NERC-CIP Standard Version 5, 2014.

[5] CIP-004-6 (Cyber Security - Personnel & Training), NERC-CIP Standard Version 5, 2014.

[6] CIP-005-5 (Cyber Security - Electronic Security Perimeter(s)), NERC-CIP Standard Version 5, 2014.
[7] CIP-006-6 (Cyber Security - Physical Security of BES Cyber Systems), NERC-CIP Standard Version 5, 2014.
[8] CIP-007-6 (Cyber Security - System Security Management), NERC-CIP Standard Version 5, 2014.
[9] CIP-008-5 (Cyber Security - Incident Reporting and Response Planning), NERC-CIP Standard Version 5, 2014.
[10] CIP-009-6 (Cyber Security - Recovery Plans for BES Cyber Systems), NERC-CIP Standard Version 5, 2014.
[11] CIP-010-2 (Cyber Security - Configuration Change Management and Vulnerability Assessments), NERC-CIP Standard Version 5, 2014.
[12] CIP-011-2 (Cyber Security - Information Protection), NERC-CIP Standard Version 5, 2014.
[13] CIP-014-2 (Physical Security), NERC-CIP Standard Version 5, 2014.
[14] "5. Políticas Seguridad". [Online]. Available: http://www.iso27000.es/iso27002_5.html. [Accessed: 03-Sep-2017].
[15] "6. Aspectos Organizativos". [Online]. Available: http://www.iso27000.es/iso27002_6.html. [Accessed: 03-Sep-2017].
[16] "7. Seguridad Ligada a los recursos humanos". [Online]. Available: http://www.iso27000.es/iso27002_7.html. [Accessed: 03-Sep-2017].
[17] "8. Gestión Activos". [Online]. Available: http://www.iso27000.es/iso27002_8.html. [Accessed: 03-Sep-2017].
[18] "9. Control de Accesos". [Online]. Available: http://www.iso27000.es/iso27002_9.html. [Accessed: 03-Sep-2017].
[19] "10. Cifrado". [Online]. Available: http://www.iso27000.es/iso27002_10.html [Accessed: 03-Sep-2017].
[20] "11. Seguridad física y Ambiental". [Online].Available: ttp://www.iso27000.es/iso27002_11.html [Accessed: 03-Sep-2017].
[21] "12. Seguridad en la Operativa". [Online].Available:http://www.iso27000.es/iso27002_12.html [Accessed: 03-Sep-2017].
[22] "13. Seguridad en las Telecomunicaciones". [Online]. Available: http://www.iso27000.es/iso27002_13.html. [Accessed: 03-Sep-2017].
[23] "14. Adquisición, desarrollo y Mantenimiento de los sistemas de información". [Online]. Available: http://www.iso27000.es/iso27002_14.html. [Accessed: 03-Sep-2017].
[24] "15. Relaciones con Suministradores". [Online]. Available: http://www.iso27000.es/iso27002_15.html. [Accessed: 03-Sep-2017].
[25] "16. Gestión de Incidentes". [Online]. Available: http://www.iso27000.es/iso27002_16.html. [Accessed: 03-Sep-2017].
[26] "17. Aspectos de la SI en la Gestión de la Continuidad de Negocio". [Online]Available:http://www.iso27000.es/iso27002_17.html. [Accessed: 03-Sep-2017].
[27] "18. Cumplimiento". [Online]. Available: http://www.iso27000.es/iso27002_18.html. [Accessed: 03-Sep-2017].
[28] ISACA, COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. © 2012 ISACA, pp. 45.

VIII. BIOGRAFÍA

Christian Marcelo Gallardo Yanchapaxi.- Ingeniero en Electrónica y Telecomunicaciones de la Escuela Politécnica Nacional, Magíster en Conectividad y Redes de Telecomunicaciones de la Escuela Politécnica Nacional, Certificado en "Cisco Certified Network Associate Routing & Switching" (CCNA), Instructor oficial de "Cisco Certified Network Associate Routing & Switching", Entrenamiento en redes SCADA otorgado por la empresa ABB en Houston Texas. Actualmente se desempeña como parte del Área SCADA de CELEC EP – TRANSELECTRIC encargado de la red de datos del sistema SCADA/EMS. (cga.gallardo@gmail.com).

Gabriel Roberto López Fonseca.- Ingeniero en Redes de la Información, Escuela Politécnica Nacional, 2010. Master en Seguridad de Sistemas, Sheffield Hallam University, UK, 2015. Magister en Gestión de las Comunicaciones y Tecnologías de la Información, Escuela Politécnica Nacional, 2017. Actualmente se desempeña como docente investigador de la Escuela Politécnica Nacional en Quito.

Franklin Leonel Sánchez Catota.- Obtuvo el título de Ingeniero en Electrónica y Telecomunicaciones por la Escuela Politécnica Nacional y posteriormente el Máster Interuniversitario en Ingeniería Telemática por la Universidad Carlos III de Madrid y la Universidad Politécnica de Catalunya. Actualmente es docente a tiempo completo de la Escuela Politécnica Nacional.