# NIVELES DE SEGURIDAD

## Según el estándar ISA99/IEC6443

Apollocom

Tecnología conectada con la inteligencia

# NIVELES DE SEGURIDAD

## ¿QUÉ SON LOS NIVELES DE SEGURIDAD?

El estándar ISA99/IEC62443 define los niveles de seguridad de la siguiente manera:

“Los Niveles de Seguridad (SL, por sus siglas en idioma inglés) proveen una aproximación cualitativa para la Ciberseguridad de una determinada zona. Al ser un método cualitativo, la definición de niveles de seguridad sirve para comparar y gestionar la seguridad de diferentes zonas dentro de una organización.”

## TIPOS DE NIVELES DE SEGURIDAD

Según el estándar es necesaria la identificación de tres tipos diferentes de niveles de seguridad:

- Nivel de Seguridad Objetivo (SL-T): Es el nivel de seguridad deseado para un sistema particular. Es determinado usualmente a través de la realización de evaluaciones de riesgos las cuales determinan un nivel de seguridad particular para asegurar la correcta operación.

- Nivel de Seguridad Alcanzado (SL-A): Es el nivel de seguridad actual para un sistema particular. Éste es medido una vez que el diseño del sistema está disponible o cuando un sistema ya se encuentra instalado. Se utilizan para establecer si la seguridad de un sistema alcanza los niveles definidos según el SL-T.

- Nivel de Seguridad según Capacidad (SL-C): Son los niveles de seguridad que los componentes o sistemas pueden otorgar cuando son configurados apropiadamente. Estos niveles permiten saber si un determinado sistema es capaz de alcanzar el nivel de seguridad objetivo (SL-T) de forma nativa sin medidas compensatorias o contramedidas adicionales cuando es configurado e integrado apropiadamente.

## ¿CÓMO USAR LOS NIVELES DE SEGURIDAD?

Cuando se diseña un nuevo sistema o se analiza la ciberseguridad de uno existente, el primer paso es segmentar dicho sistema en diferentes zonas y definir los conductos que las vinculan.

Una vez establecido el modelo de zonas y conductos, se debe asignar a cada zona y conducto un SLT (nivel de seguridad objetivo). Una vez determinado el SL-T el sistema puede ser diseñado o rediseñado para alcanzar dicho nivel.

Durante el proceso de diseño o adecuación, es necesario evaluar las capacidades de seguridad de cada componente o subsistema. Los proveedores o integradores del producto deberán proveer dicha información como parte de sus tareas. Esta información es de suma utilidad ya que permite determinar si un componente o sistema es capaz de alcanzar el nivel de seguridad objetivo (SL-T) deseado. Es probable que en un diseño particular haya algunos componentes o sistemas que no pueden alcanzar el SL-T. En aquellos casos en que el nivel de seguridad según capacidad (SL-C) de estos es menor al deseado como SL-T, se deberán considerar medidas compensatorias o contramedidas para reducir esa brecha. Dichas contramedidas pueden requerir cambios en los diseños e incluso la selección de componentes adicionales. Cada vez que se realice una modificación en los sistemas industriales, su nivel de seguridad debe ser evaluado obteniéndose así el nivel de seguridad alcanzado (SL-A) y comparar el mismo con el SL-T).


***Figura 1.***

## VECTOR DE NIVELES DE SEGURIDAD

## REQUISITOS FUNDAMENTALES DE CIBERSEGURIDAD

Los Niveles de Seguridad se encuentran basados en los siete requisitos fundamentales definidos en el documento ISA- 62443-1-1.
Dichos requisitos son:
1. Controles de Identificación y Autenticación (IAC)
2. Control de Uso (UC)
3. Integridad del Sistema (SI)
4. Confidencialidad de los Datos (DC)
5. Flujo de Datos Restringido (RDF)
6. Tiempo de Respuesta a Eventos (TRE)
7. Disponibilidad de Recursos (RA)

En lugar de representar el nivel de seguridad asignado con un único valor, es posible utilizar un vector de niveles de seguridad el cual representa los niveles de seguridad definidos para cada uno de los siete requisitos fundamentales.

## DEFINICIÓN DE NIVELES DE SEGURIDAD

El estándar ISA99/IEC62443 define los niveles de seguridad dentro de una escala de cinco valores (0, 1, 2, 3 y 4), cada uno de los cuales representa un nivel incremental en cuanto a medidas de ciberseguridad.

Los niveles de seguridad definidos son los siguientes:

- SL 0: No fija requisitos específicos o no precisa protecciones de ciberseguridad.
- SL 1: Requiere protección contra violaciones casuales.
- SL 2: Requiere protección contra violaciones intencionales con bajos recursos, conocimientos generales y baja motivación.
- SL 3: Requiere protección contra violaciones intencionales con recursos sofisticados, conocimientos específicos de los Sistemas de Automatización y Control y una moderada motivación.
- SL 4: Requiere protección contra violaciones intencionales con recursos sofisticados, conocimientos avanzados de los Sistemas de Automatización y Control y una elevada motivación.

## FORMATO DEL VECTOR DE NIVELES DE SEGURIDAD

Un vector puede ser utilizado para representar los requisitos de ciberseguridad para una zona, conducto o sistema de forma más representativa que un único valor. Dicho vector contiene un valor específico para los niveles de seguridad definidos para cada uno de los requisitos fundamentales. (ver 3.4.1)

El formato utilizado es el siguiente:
SL-?([FR,]dominio) = { IAC UC SI DC RDF TRE RA }

Donde:

SL-? = (Requerido) Representa el tipo de SLs (ver 3.2). Los posibles valores son:

› SL-T = Nivel de Seguridad Objetivo
› SL-A = Nivel de Seguridad Alcanzado
› SL-C = Nivel de Seguridad según Capacidad

[FR,] = (Opcional) Campo que indica los requisitos fundamentales (FRs) que cada SL representa. Los FRs son representados de manera abreviada según las siglas mencionadas en el punto 3.4.1 para facilitar su interpretación.

dominio = (Requerido) Representa el dominio al cual los SLs son aplicados. Un dominio puede ser una determinada zona, un conducto, sistema de control o un determinado componente. Algunos ejemplos de diferentes dominios de la “Figura 6 - Modelo de alto nivel para procesos industriales” pueden ser: “SIS zone”, “BPCS zone”, “BPCS HMI”, “Plant DMZ” etc.

› Ejemplo 1 — SL-T(BPCS Zone) = { 2 2 0 1 3 1 3 }
› Ejemplo 2 — SL-C(SIS Zone) = { 3 3 2 3 0 0 1 }
› Ejemplo 3 — SL-C(RA, BPCS HMI) = 4

Nota: el ejemplo 3 define solamente un nivel de seguridad 4 para el requisito fundamenta RA (Disponibilidad de Recursos) en el BPCS HMI.

## GUÍA PARA LA DEFINICIÓN DE NIVELES DE SEGURIDAD

El estándar ISA99/IEC62443 establece una guía práctica de cómo implementar medidas de protección contra incidentes de ciberseguridad fundamentada en los niveles de seguridad previamente definidos para cada zona y/o conducto agrupados en siete requisitos “técnicos” fundamentales de ciberseguridad que como ya se ha mencionado son:

1. Controles de Identificación y Autenticación (IAC)
2. Control de Uso (UC)
3. Integridad del Sistema (SI)
4. Confidencialidad de los Datos (DC)
5. Flujo de Datos Restringido (RDF)
6. Tiempo de Respuesta a Eventos (TRE)
7. Disponibilidad de Recursos (DR)

Las siguientes siete tablas muestran los controles propuestos por el estándar para cada uno de los siete requisitos fundamentales de ciberseguridad. Las tablas están compuestas por “Requisitos del Sistema (SR)” y “Aumento de Requisitos (RE)”:

| SRs y REs | SL-1 | SL-2 | SL-3 | SL-4 |
|---|---|---|---|---|
| **FR 1 - CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN (IAC)** | | | | |
| SR 1.1 -Identificación y autenticación de usuarios humanos | ✓ | ✓ | ✓ | ✓ |
| RE (1) Identificación y autenticación única | | ✓ | ✓ | ✓ |
| RE (2) Múltiple factor de autenticación para redes no confiables | | | ✓ | ✓ |
| RE (3) Múltiple factor de autenticación para todas las redes | | | | ✓ |
| SR 1.2 - Identificación y autenticación de procesos de software y dispositivos | | ✓ | ✓ | ✓ |
| RE (1) identificación y autenticación única | | | ✓ | ✓ |
| SR 1.3 - Gestión de cuentas | ✓ | ✓ | ✓ | ✓ |
| RE (1) Gestión de cuentas unificada | | | ✓ | ✓ |
| SR 1.4 - identificación de gestión | ✓ | ✓ | ✓ | ✓ |
| SR 1.5 - Gestión de autenticación | ✓ | ✓ | ✓ | ✓ |
| RE (1) Hardware de seguridad para identificar credenciales mediante proceso de software | | | ✓ | ✓ |
| SR 1.6 - Gestión de acceso inalámbrico | ✓ | ✓ | ✓ | ✓ |
| RE (1) Identificador y autenticador único | | ✓ | ✓ | ✓ |
| SR 1.7 - Fortaleza de autenticación basada en contraseñas | ✓ | ✓ | ✓ | ✓ |
| RE (1) Generación de contraseñas y restricciones en tiempo de vida para usuarios humanos | | | ✓ | ✓ |
| RE (2) Restricciones en el tiempo de vida de contraseñas para todos los usuarios | | | | ✓ |
| SR 1.8 - Certificados de infraestructura de clave publica | | ✓ | ✓ | ✓ |
| SR 1.9 - Fuerte autenticación basada en clave publica | | ✓ | ✓ | ✓ |
| RE (1) Hardware de seguridad para autenticar claves publicas | | | ✓ | ✓ |
| SR 1.10 - Feedback de autenticador | ✓ | ✓ | ✓ | ✓ |
| SR 1.11 - Intentos de login fallidos | ✓ | ✓ | ✓ | ✓ |
| SR 1.12 - Notificaciones de uso de sistema | ✓ | ✓ | ✓ | ✓ |
| SR 1.13 - Acceso a través de redes no seguras | ✓ | ✓ | ✓ | ✓ |
| RE (1) Solicitud de aprobación de acceso explicita | | ✓ | ✓ | ✓ |

| FR 2 - CONTROL DE USO (UC) | | | | |
|---|---|---|---|---|
| SR 2.1 - Aplicación de autorización | ✓ | ✓ | ✓ | ✓ |
| RE (1) Aplicación de autorización para todos los usuarios | | ✓ | ✓ | ✓ |
| RE (2) Mapeo de permisos a roles | | ✓ | ✓ | ✓ |
| RE (3) Anular supervisor | | | ✓ | ✓ |
| RE (4) Doble Aprobación | | | | ✓ |
| SR 2.2 - Control de uso inalámbrico | ✓ | ✓ | ✓ | ✓ |
| RE (1) Identificar y reportar dispositivos inalámbricos no autorizados | | | ✓ | ✓ |
| SR 2.3 - Control de uso para dispositivos portátiles y mobile | ✓ | ✓ | ✓ | ✓ |
| RE (1) Aplicación del estado de seguridad de dispositivos portátiles y mobile | | | ✓ | ✓ |
| SR 2.4 - Código mobile | ✓ | ✓ | ✓ | ✓ |
| RE (1) Chequeo de integridad de código mobile | | | ✓ | ✓ |
| SR 2.5 - Bloqueo de sesión | ✓ | ✓ | ✓ | ✓ |
| SR 2.6 - Terminación de sesiones remotas | | ✓ | ✓ | ✓ |
| SR 2.7 - Control de sesiones concurrentes | | | ✓ | ✓ |
| SR 2.8 - Eventos auditables | ✓ | ✓ | ✓ | ✓ |
| RE (1) Pistas de auditoria de sistemas con gestión centralizada | | | ✓ | ✓ |
| SR 2.9 - Auditar capacidad de almacenamiento | ✓ | ✓ | ✓ | ✓ |
| RE (1) Advertir cuando se haya alcanzado el umbral de capacidad en los registros de auditoría | | | ✓ | ✓ |
| SR 2.10 - Responder a fallas en el proceso de auditoria | ✓ | ✓ | ✓ | ✓ |
| SR 2.11 - Marcas de tiempo | | ✓ | ✓ | ✓ |
| RE (1) Sincronización interna de tiempo | | | ✓ | ✓ |
| RE (2) Protección en la integridad de la fuente de tiempo | | | | ✓ |
| SR 2.12 - No repudio | | | ✓ | ✓ |
| RE (1) No repudio para todos los usuarios | | | | ✓ |
| **FR 3 - INTEGRIDAD DEL SISTEMA (SI)** | | | | |
| SR 3.1 - Integridad en las comunicaciones | ✓ | ✓ | ✓ | ✓ |
| RE (1) Usar criptografía para proteger la integridad | | | ✓ | ✓ |
| SR 3.2 - Protección contra código malicioso | ✓ | ✓ | ✓ | ✓ |
| RE (1) Protección contra código malicioso en los puntos de entrada y salida | | ✓ | ✓ | ✓ |
| RE (2) Gestión centralizada para protección contra código malicioso | | | ✓ | ✓ |
| SR 3.3 - Verificación de funcionalidades de seguridad | ✓ | ✓ | ✓ | ✓ |
| RE (1) Mecanismos automáticos para verificar funcionalidades de seguridad | | | ✓ | ✓ |
| RE (2) Verificaciones de funcionalidades de seguridad durante la operación normal | | | | ✓ |
| SR 3.4 - Integridad del software e información | | ✓ | ✓ | ✓ |
| RE (1) Notificaciones automáticas sobre violaciones de integridad | | | ✓ | ✓ |
| SR 3.5 - Validación de entradas | ✓ | ✓ | ✓ | ✓ |
| SR 3.6 - Salidas Determinísticas | ✓ | ✓ | ✓ | ✓ |
| SR 3.7 - Manejo de errores | | ✓ | ✓ | ✓ |
| SR 3.8 - Integridad de sesiones | | ✓ | ✓ | ✓ |
| RE (1) Invalidar IDs de sesión una vez que la sesión fue terminada | | | ✓ | ✓ |
| RE (2) Generación de IDs únicos de sesión | | | ✓ | ✓ |
| RE (3) Aleatoriedad de IDs de sesión | | | | ✓ |

| FR 4 - CONFIDENCIALIDAD DE LOS DATOS (DC) | | | | |
|---|---|---|---|---|
| SR 4.1 - Confidencialidad de la información | ✓ | ✓ | ✓ | ✓ |
| RE (1) Protección de la confidencialidad de la información alojada o en tránsito por redes no confiables | | ✓ | ✓ | ✓ |
| RE (2) Protección de la confidencialidad a través de los límites de las zonas | | | | ✓ |
| SR 4.2 - Persistencia de la información | | ✓ | ✓ | ✓ |
| RE (1) Purga de recursos de memoria compartida | | | ✓ | ✓ |
| SR 4.3 - Uso de criptografía | ✓ | ✓ | ✓ | ✓ |
| **FR 5 - FLUJO DE DATOS RESTRINGIDO (RDF)** | | | | |
| SR 5.1 - Segmentación de redes | ✓ | ✓ | ✓ | ✓ |
| RE (1) Segmentación física de redes | | ✓ | ✓ | ✓ |
| RE (2) Independencia de redes sin sistemas de control | | | ✓ | ✓ |
| RE (3) Aislamiento lógico y físico de redes criticas | | | | ✓ |
| SR 5.2 - Protección de límites de zonas | ✓ | ✓ | ✓ | ✓ |
| RE (1) Denegar por defecto, permitir por excepción | | ✓ | ✓ | ✓ |
| RE (2) Modo isla | | | ✓ | ✓ |
| RE (3) Cierre ante falla | | | ✓ | ✓ |
| SR 5.3 - Restricción en comunicaciones persona a persona de propósitos generales | ✓ | ✓ | ✓ | ✓ |
| RE (1) Prohibir todas las comunicaciones persona a persona de propósitos generales | | | ✓ | ✓ |
| SR 5.4 - Particionamiento de aplicaciones | ✓ | ✓ | ✓ | ✓ |
| **FR 6 - TIEMPO DE RESPUESTA A EVENTOS (TRE)** | | | | |
| SR 6.1 - Auditar accesibilidad a logs | ✓ | ✓ | ✓ | ✓ |
| RE (1) Acceso programado a logs de auditoria | | | ✓ | ✓ |
| SR 6.2 - Monitoreo continuo | | ✓ | ✓ | ✓ |
| **FR 7 - DISPONIBILIDAD DE RECURSOS (RA)** | | | | |
| SR 7.1 - Protección contra denegación de servicio | ✓ | ✓ | ✓ | ✓ |
| RE (1) Gestionar la carga en las comunicaciones | | ✓ | ✓ | ✓ |
| RE (1) Limitar los efectos de una denegación de servicio a otros sistemas o redes | | | ✓ | ✓ |
| SR 7.2 - Gestión de recursos | ✓ | ✓ | ✓ | ✓ |
| SR 7.3 - Control de backup del sistema | ✓ | ✓ | ✓ | ✓ |
| RE (1) Verificación de backup | | ✓ | ✓ | ✓ |
| RE (2) Automatización de backup | | | ✓ | ✓ |
| SR 7.4 - Restauración y reconstitución del sistema de control | ✓ | ✓ | ✓ | ✓ |
| SR 7.5 - Energía de emergencia | ✓ | ✓ | ✓ | ✓ |
| SR 7.6 - Ajustes de redes y configuraciones de seguridad | | | ✓ | ✓ |
| RE (1) Reportes de ajustes de seguridad actuales legibles desde una maquina | | | ✓ | ✓ |
| SR 7.7 - Menos funcionalidades | ✓ | ✓ | ✓ | ✓ |
| SR 7.8 - Inventario de componentes de sistemas de control | | ✓ | ✓ | ✓ |

**Fuente: Centro de Ciberseguridad Industrial**