AEINSE 10/21. Guía de buenas prácticas de ciberseguridad en proyectos de seguridad física

DICIEMBRE 2021

Contenido

1 La ciberseguridad en los sistemas de seguridad física 3
2 Afrontar proyectos de sistemas de seguridad física 5
3 El riesgo IT de los sistemas de seguridad física 7
3.1 Análisis y evaluación de riesgos de ciberseguridad en los sistemas de seguridad física 7
3.2 Activos 8
3.3 Las amenazas de los sistemas de seguridad 10
3.4 Vulnerabilidades 12
3.5 Impacto 13
4 Implementar una arquitectura segura: especificaciones de medidas de ciberseguridad 14
4.1 Medidas de ciberseguridad tradicionales de entornos IT 15
4.1.1 Ampliación de la política de seguridad con enfoque integral ciberfísico 15
4.1.2 Implicación de la alta dirección en la visión integral de la seguridad 16
4.1.3 Comunicación y aprovechamiento de las sinergias entre departamentos 16
4.1.4 Formación y concienciación en ciberseguridad del personal involucrado 17
4.1.5 Independencia de las redes de seguridad respecto a otros sistemas 17
4.1.6 Protección física de los sistemas informáticos 18
4.1.7 Utilización de equipos personales 19
4.1.8 Acceso remoto de personal propio o proveedores 19
4.1.9 Seguridad de la nube 20
4.2 Medidas de ciberseguridad específicas para sistemas de seguridad física 20
4.2.1 Tecnologías de identificación en sistemas de control de accesos 21
4.2.2 Protocolos de comunicación en sistemas de control de accesos 23
4.2.3 Control de acceso lógico en dispositivos IoT y sistemas 25
4.2.4 Control de acceso remoto en dispositivos IoT 27
4.2.5 Gestión de parches y vulnerabilidades en sistemas de seguridad física 27
5 Los nuevos servicios de seguridad necesarios 29
5.1 Ingeniería y consultoría de seguridad 29
5.2 Instalación de SSF 30
5.3 Mantenimiento de SSF 30
6 Bibliografía 32

Introducción

El presente documento es el primer resultado de las actividades del Grupo de Trabajo de AEINSE, “ciberseguridad aplicada a los Sistemas de Seguridad Física”.

Su objetivo es servir de Guía para los ingenieros que deban proyectar e instalar Sistemas de Seguridad Física (en adelante *SSF*), ya sea porque su desempeño se produzca en las empresas usuarias de los Sistemas, en empresas de ingeniería que deban realizar proyectos y supervisar las instalaciones, o en empresas de Seguridad dedicadas a instalación y mantenimiento de Sistemas de Seguridad.

La presente Guía tiene un objeto práctico de orientación para que:

- Se demanden las características necesarias de ciberseguridad en los SSF que las empresas necesitan instalar (empresas usuarias de Seguridad)
- Se proyecten y especifiquen las medidas de ciberseguridad necesarias a incorporar en los proyectos de instalación de SSF (empresas de ingeniería)
- Se oferten e instalen las medidas de ciberseguridad necesarias para los SSF (empresas de Seguridad de instalaciones y mantenimiento)

El desarrollo de esta Guía pretende presentar paso a paso todas las etapas a seguir, de forma que el resultado final permita disponer de unas medidas de ciberseguridad que protejan a los SSF de forma razonable y equilibrada ante los ciberataques.

Redacción:

- Raúl Aguilera Sares
- Raúl Porras Martín
- Álvaro Ubierna Alonso
- Alfonso Bilbao Iglesias

Revisión:

- Carlos Martínez Hernández
- Manuel Carpio Cámara

1 La ciberseguridad en los sistemas de seguridad física

Los sistemas de seguridad física, también denominados de seguridad electrónica, son "transversales" a todo tipo de infraestructuras y negocios. Desatender las ciberamenazas y no considerarlas en el diseño de las nuevas soluciones o no contemplarlas en los sistemas de seguridad existentes, puede provocar que éstos pierdan su funcionalidad principal que es la de proporcionar una protección física a las instalaciones de las organizaciones que las contemplan.

Si tomamos como ejemplo las infraestructuras críticas, veremos que todas las normativas y guías de buenas prácticas de seguridad, como el estándar IEC 62443-2-1, parte 2-1, punto 4.3.3, el NERC CIP-005-5, el NERC CIP-014-2 o incluso, y a pesar de no ser específica del entorno industrial, la ISO/IEC 27001:2013, puntos A.11.1, A.11.2 y A.11.4 recogen, de alguna forma, requerimientos de seguridad física.

Lograr la anulación de los sistemas de seguridad de una manera total o parcial, la inhibición de los sistemas de detección de incendios, llevar a cabo el borrado o alteración de las imágenes grabadas de los sistemas de circuito cerrado de televisión o la modificación de autorizaciones en los sistemas de control de accesos son sólo alguno de los ejemplos de ciberataques que podrían llevarse a cabo.

La guía de buenas prácticas NIST 800-82, recoge los atributos que deben considerarse a la hora de realizar una defensa en profundidad aplicada a la seguridad física, pero la implementación de éstos y, sobre todo, cómo gestionarlos dentro de la red de la propia infraestructura, no se encuentra definido.

Todos los beneficios que puede aportar la seguridad física pueden verse diluidos por una mala implementación o una incorrecta gestión dentro de la red, o incluso peor, suponer un riesgo adicional por una mala praxis.

Si bien el equipo humano de seguridad física de una organización puede estar muy familiarizado con los controles de seguridad física que se incluyen, es menos probable que esté familiarizado con las implicaciones de usar sistemas de IT (*Information Technology*) avanzados para entregar y administrar estas medidas, por no hablar de los controles que se requieren en los propios sistemas de IT. De hecho, cabe admitir que el proyectista o el instalador de sistemas de seguridad, en general, ha efectuado la transición a las instalaciones con equipos IP con poco conocimiento sobre este tipo de redes y sus riesgos. Ante la complejidad añadida de implementar seguridad lógica, en muchos casos se ha ignorado o implementado de manera muy básica.

Por el contrario, el equipo humano de seguridad de IT de una organización estará familiarizado con la protección de los sistemas de IT, pero muy probablemente no lo esté con las características de los sistemas que respaldan la seguridad física, conformados por dispositivos conectados entre sí que emplean en muchos casos protocolos diversos de comunicación específicos del mundo de seguridad física. Esto propicia que los conocimientos de seguridad empleados en los entornos IT no puedan ser extrapolados directamente para los sistemas de seguridad física ya que las medidas pueden ser intrusivas y afectar a la disponibilidad de los equipos. En el fondo, estos sistemas se

aproximan más al mundo OT (*Operational Technology*) que al IT, en el que resulta crucial un conocimiento profundo de los protocolos propietarios de comunicación entre los elementos de la red, servidores y los aplicativos que gestionan, supervisan y controlan estos sistemas.

2 Afrontar proyectos de sistemas de seguridad física

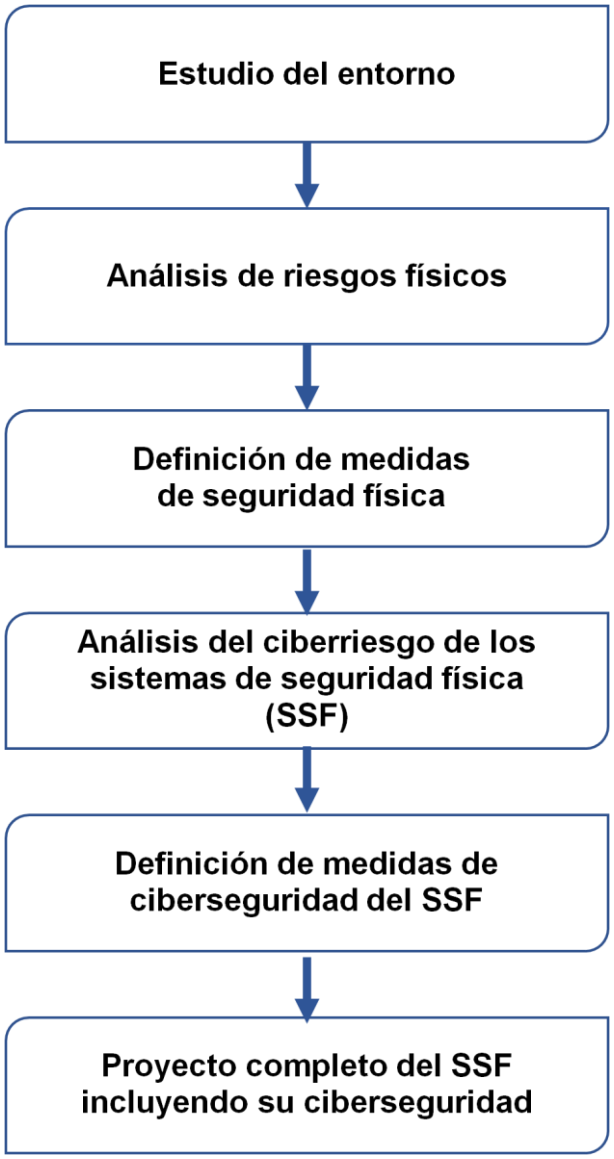
Una de las fases en el desarrollo de un plan integral de seguridad es la del análisis y evaluación de riesgos tras haber estudiado y analizado los entornos externo e interno de una organización. En esta fase, se identifican y clasifican los activos a proteger mediante medidas de protección activas (electrónicas), pasivas y de coordinación. Es entonces cuando se definen los elementos que conforman los diferentes subsistemas de seguridad (control de acceso, intrusión, anti-incendio, videovigilancia…). Dicho plan también incluye las medidas para proteger los activos susceptibles a las ciberamenazas.

Lo que habitualmente no tiene en cuenta el plan es que los propios elementos de los subsistemas de protección electrónica están expuestos a su vez a ciberamenazas que no estaban incluidas en el análisis de riesgos inicial, de forma que las medidas de ciberseguridad a implantar en la organización no las contemplan. Será necesario entonces llevar a cabo un nuevo análisis de riesgos IT para estos nuevos activos.

Idealmente, el análisis de riesgos IT debería llevarse a cabo después de haberse definido los subsistemas de seguridad electrónica, para que las medidas de ciberseguridad de la organización los incluyeran y fueran, por tanto, homogéneas. La realidad, en cambio, es que la implantación de la ciberseguridad y la de la seguridad física se desarrollan en paralelo y no se aplica a los sistemas de seguridad electrónicos.

En el momento en el que una organización requiera de los servicios de una empresa de seguridad para el diseño e implantación de los sistemas de seguridad, dicha empresa deberá de incorporar el análisis y evaluación de ciberriesgos de los sistemas de seguridad electrónica. En este caso los activos a proteger serán los activos que conforman los subsistemas de seguridad electrónica y las vulnerabilidades, amenazas y riesgos IT a los que estén expuestos. A la hora de medir el impacto, será necesario tener muy presente las dependencias entre los activos de los sistemas de seguridad y los activos a proteger. Se desarrollarán más estos conceptos en el apartado 3: El riesgo IT de los sistemas de seguridad física.

Las fases de desarrollo de un proyecto de seguridad física quedarán de la siguiente manera:


Estudio del entorno
Análisis de riesgos físicos
Definición de medidas de seguridad física
Análisis del ciberriesgo de los sistemas de seguridad física (SSF)
Definición de medidas de ciberseguridad del SSF
Proyecto completo del SSF incluyendo su ciberseguridad

3 El riesgo IT de los sistemas de seguridad física

3.1 Análisis y evaluación de riesgos de ciberseguridad en los sistemas de seguridad física

Los proyectos integrales de seguridad ya realizan un análisis de los riesgos a los que está expuesta una organización con el objetivo de establecer procedimientos y medios físicos y humanos que permitan mitigarlos y llevarlos a unos niveles aceptables para la dirección responsable de dicha organización. En ese sentido, el objetivo de la presente guía es el de advertir que es necesaria la ampliación del análisis de dichos riesgos para incluir la ciberseguridad de los medios de protección activos.

El análisis de riesgos es una herramienta que, al aplicarla, proporciona información acerca de los activos a proteger, la identificación de las potenciales amenazas que podrían afectar a los citados activos y la valoración del impacto que puede suponer la pérdida de los mismos. A partir del conocimiento de estos riesgos a los que se enfrenta la organización, se pueden identificar las oportunas medidas de seguridad que permitan el tratamiento de los riesgos.

Existe una amplia variedad de opciones a la hora de elegir una metodología para llevar a cabo un análisis de riesgos. En materia de seguridad de la información es más común utilizar la norma ISO 27001, o el método MAGERIT (incluido en el Esquema Nacional de Seguridad y con la herramienta PILAR para su implementación). De todas maneras, el resultado de cualquier análisis de riesgos es obtener un mapa de riesgos priorizados que permita identificar las medidas oportunas para su gestión.

Llegados a este punto, una consideración esencial es advertir que en el ámbito de la ciberseguridad se establecen tres dimensiones canónicas de la seguridad de las redes y sistemas de información:

- **Disponibilidad** de los servicios para ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio.
- **Integridad** o mantenimiento de las características de completitud y corrección de los datos. Si ésta se ve afectada, la información puede aparecer manipulada, corrupta o incompleta.
- **Confidencialidad** o que la información llegue solamente a las personas autorizadas. Si se ve comprometida pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en el departamento de seguridad (llevado al ámbito de la presente guía) que no es diligente en el mantenimiento del secreto y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

De esta manera, para evaluar los riesgos de ciberseguridad en los sistemas de seguridad físicos, se deberá determinar la probabilidad y el impacto que produciría la materialización de las amenazas que puedan afectar a la disponibilidad, integridad y confidencialidad de los activos que componen los diferentes subsistemas de seguridad.

3.2 Activos

El ámbito de la presente guía se limita a evaluar los activos de los sistemas de seguridad susceptibles de sufrir un ciberataque. En ese sentido, la definición de activo según la UNE 71504:2008 es adecuada:

"Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos".

Es necesario entonces elaborar un inventario de los activos que componen o compondrán el sistema de seguridad. Dependiendo del proyecto, puede que ya haya sistemas de seguridad electrónicos instalados desde hace tiempo y un conocimiento detallado de su funcionamiento y configuración no sea de fácil obtención. De todas maneras, esta información es necesaria y debe determinarse lo antes posible.

Al afrontar esta tarea, puede resultar de utilidad apoyarse en un catálogo general de activos de seguridad electrónica como el Catálogo de activos del documento CSF02/21 de AEINSE para adaptarlo al proyecto, eliminando aquellos activos que no apliquen y añadiendo aquellos que sean específicos de dicho proyecto.

Por otro lado, las siguientes cuestiones también pueden ayudar a generar el inventario:

- ¿Cuántas ubicaciones, sistemas y activos existen?

- ¿Qué sistemas hay en cada localización?
- ¿Cuáles son los sistemas más críticos para la protección de la organización en cada ubicación?
- ¿Cuáles son los activos críticos de los sistemas en las ubicaciones?
- ¿Están las ubicaciones sometidas a alguna regulación específica?
- ¿Quién es el responsable de los sistemas de seguridad?
- ¿Quiénes son los principales proveedores y colaboradores relacionados con los sistemas de seguridad?
- ¿Qué conexiones y datos entran y salen de los sistemas electrónicos de seguridad?
- ¿Hay algún problema conocido con los sistemas?
- ¿Cuáles son los proyectos en curso o programados?
- ¿Cuáles son los datos de contacto para el personal local y remoto y los proveedores?
- ¿Qué dependencias tiene la ubicación?
- ¿Hay resúmenes y diagramas detallados de los sistemas y la red?
- ¿Está protegida toda la documentación y se siguen procedimientos de gestión de cambios?

Las respuestas a estas preguntas permiten crear un inventario del sistema de seguridad electrónico. El inventario es un bloque fundamental para construir el marco de ciberseguridad del sistema y debe estar suficientemente detallado como para proporcionar una adecuada percepción del riesgo.

Es esencial comprender cualquier dependencia entre sistemas y/o activos (en especial con los que están fuera del ámbito de esta guía). Un activo de un sistema de seguridad puede ser un lector de control de accesos o un sensor de presencia. El valor de dichos activos es relativamente bajo, pero el impacto resultante de un hackeo que produzca la anulación de alguno de ellos puede llevar a un ataque que permita a un delincuente entrar en una sala restringida con objetos de alto valor. La criticidad de los activos depende también de su dependencia con otros y en el caso de los activos de los sistemas de seguridad física, de forma habitual, será más relevante el valor del activo que protege que el del propio activo del sistema de seguridad.

Para simplificar los análisis de riesgos en los que participan un gran número de activos repetidos, una opción interesante será modelar los sistemas incluyendo un único representante por cada clase, aplicándose posteriormente las medidas resultantes a cada uno de los constituyentes de la clase. En estos casos hay que cerciorarse de que las dependencias son las mismas, y los entornos de operación también.

Cabe señalar que estos inventarios son una fuente de información sensible que puede ser muy útil para un atacante. En consecuencia, estos inventarios deben protegerse. El acceso a estos inventarios debe limitarse al mínimo número de personas que necesiten acceder a esta información.

3.3 Las amenazas de los sistemas de seguridad

Las amenazas a la ciberseguridad de los sistemas de seguridad electrónica pueden ser numerosas y surgir de diferentes fuentes.

Estas amenazas son genéricas, por lo que es útil aplicarlas en escenarios de ejemplo para que su impacto y las vulnerabilidades relacionadas puedan considerarse más específicamente, teniendo especial cuidado en garantizar que los escenarios escogidos son lo suficientemente amplios para incluir todas las amenazas. Las amenazas propuestas en el *Libro II - Catálogo de Elementos* de MAGERIT se agrupan, según su origen y/o motivación, en cuatro conjuntos que engloban tanto amenazas de carácter físico, como lógico:

- **Desastres Naturales [N]**: Eventos que pueden ocurrir sin ser causados, directa o indirectamente, por intervención humana.
- **De Origen Industrial [I]**: Eventos que pueden ocurrir accidentalmente a causa de una actividad humana de tipo industrial.
- **Errores y Fallos No Intencionados [E]**: Errores causados por personas sin intencionalidad.
- **Ataques Deliberados [A]**: Incidentes causados voluntariamente por atacantes malintencionados. Las amenazas son similares en número y naturaleza a las de los errores no intencionados, con la diferencia de que en el caso de los ataques hay alevosía.

En la presente guía, en el que nos centramos en las amenazas del entorno IT que puedan afectar a los activos de los sistemas de seguridad física, no tiene sentido evaluar las amenazas por desastres naturales que afecten a dichos activos ni las de origen industrial, así que solamente será necesario centrarse en aquellas correspondientes a **Errores y Fallos No Intencionados [E]** y **Ataques Deliberados [A].**

[E] Errores y fallos no intencionados
[E.1] Errores de los usuario
[E.2] Errores del administrador del sistema/de la seguridad
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia

[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento/actualización de programas (software)
[E.23] Errores de mantenimiento/actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A] Ataques deliberados
[A.3] Manipulación de los registros de actividad (log)
[A.4] Manipulación de los ficheros de configuración
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.13] Repudio (negación de actuaciones)
[A.14] Interceptación de información (escucha)
[A.15] Modificación de la información
[A.18] Destrucción de la información

[A.19] Revelación de información
[A.22] Manipulación de programas
[A.23] Manipulación del hardware
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)
[A.31] Distracción
[A.40] Incumplimiento (leyes, reglamentos, normas…)

3.4 Vulnerabilidades

Comprender las vulnerabilidades implica un examen detallado de todos los elementos del sistema de seguridad (incluyendo servidores, estaciones de trabajo, infraestructura de red, etc.), para determinar las vulnerabilidades que existen. Ejemplos de áreas donde se deberán identificar con especial atención cualesquiera vulnerabilidades incluyen, pero no están limitadas a:

- Conexiones a otros sistemas
- Acceso remoto
- Protección antivirus
- Control del acceso
- Contraseñas y cuentas
- Parcheados de seguridad
- Monitorización del sistema
- Resistencia y continuidad del sistema
- Terceros que acceden a los sistemas de seguridad

Al considerar la seguridad del sistema completo es importante recordar que un sistema entero está tan protegido como lo esté el eslabón más débil.

3.5 Impacto

Una vez que se han identificado las amenazas es mucho más fácil examinar el impacto que pueden causar. Hay que considerar cada escenario para cada centro, subsistema y considerar cuál sería el impacto en la vida real, no sólo en el sistema de seguridad electrónico, sino también para cualquier sistema del que dependan. Al determinar el impacto, hay que hacer referencia a los inventarios y a las dependencias ya identificadas.

Clasificación del impacto: es habitual en el estudio del riesgo cuantificar los posibles impactos o consecuencias de una amenaza en términos de valor monetario. Se da este caso particularmente al considerar el riesgo financiero. Sin embargo, al considerar el riesgo para la ciberseguridad de los sistemas de seguridad electrónica puede ser difícil determinar los impactos financieros exactos de los incidentes de seguridad. Esta cuantificación de las consecuencias financieras supone un campo completo de especialización por sí mismo y puede ser excesivo para estudiar los riesgos para la ciberseguridad de los sistemas de seguridad física.

Con el fin de evitar un esfuerzo excesivo en la determinación de los impactos de un riesgo, a menudo es posible expresar el impacto en términos de lenguaje de negocio en vez de como una cifra monetaria. Por ejemplo, ser capaz de comunicar el impacto de una posible amenaza a la que se enfrenta un sistema de seguridad física en términos del efecto que tendría en el sistema hace el riesgo mucho más comprensible. Algunos ejemplos podrían ser:

- Pérdida de confidencialidad de la información.
- Delitos o daños cometidos en la organización protegida
- Pérdida de la continuidad del negocio
- Daño a la reputación
- Incumplimiento de la legalidad vigente

Al considerar el impacto de una amenaza particular, es importante considerar cómo la amenaza puede variar con el tiempo. Por ejemplo, un incidente puede tener inicialmente un menor impacto, pero si se le permite que continúe un largo periodo de tiempo, la gravedad del impacto podría ser mayor. También debe ser considerado el efecto de impactos coincidentes o sucesivos, especialmente cuando pueden ser producidos por una causa común.

4 Implementar una arquitectura segura: especificaciones de medidas de ciberseguridad

Tal y como se comenta en la introducción de este documento, la necesidad de analizar los ciberriesgos de los SSF, al igual que en muchos otros aspectos de la vida diaria, aparece según madura el proceso de transformación digital de nuestra sociedad.

Es indudable que el avance de la transformación digital aporta innumerables ventajas, como son:

- La facilidad la interconexión de diferentes sistemas.
- La reducción de las tecnologías propietarias que complicaba la integración de sistemas.
- El abaratamiento de la tecnología.
- La generación de datos/información que permiten aprender de la experiencia y mejorar la forma de actuar.
- El acercamiento de la tecnología para uso y disfrute de la sociedad en general.
- Etc.

Pero también se ha de reconocer que este cambio conlleva sus connotaciones negativas, como son:

- La ampliación del perímetro de exposición de los sistemas al estar interconectados.
- El incremento de la complejidad de los sistemas.
- Las dependencias interdepartamentales dentro de las organizaciones,
- La necesidad de formación tecnológica digital a todos los usuarios.

Cualquier profesional que tenga una experiencia de más de 2 décadas en este sector recordará la simplicidad de concepto de aquellos sistemas de videovigilancia basadas en cámaras analógicas, cables coaxiales punto a punto, matrices analógicas y monitores con tubo de rayos catódicos. Aquellos sistemas, al no estar conectados con el exterior, no eran tan vulnerables a muchas de las amenazas actualmente existentes.

La transformación digital implica que los sistemas SSF (al igual que ocurre en los sistemas de gestión de un automóvil, un túnel o una lavadora) se soporten para su interconexión y gestión globalizada en una capa de tecnología digital estándar y basada en protocolos TCP/IP. Unos protocolos que fueron diseñados en los años 60 para interconectar unos pocos equipos, tales como grandes ordenadores de centros de investigación militar o universidades.

Esta tecnología basada en protocolos TCP/IP, comúnmente denominada tecnología IP, en unas pocas décadas se ha extendido en el corazón de la gestión de todos los sistemas complejos del mundo.

Como consecuencia los protocolos de comunicaciones que interconexionan las modernas cámaras de videovigilancia IP, los lectores de acceso, las centrales de

incendio, o los lectores de matrícula con los centros de control utilizan el mismo lenguaje de comunicación que un ordenador cuando consulta una página web.

Por detrás de estos servicios se encuentran unas redes de comunicaciones basadas en electrónica de red (conmutadores/switches, cortafuegos/firewalls y enrutadores/routers) enlazados mediante conexiones de cobre, de fibra óptica o por satélite, en los que se entremezcla la información de las conversaciones telefónicas con los datos de la mensajería instantánea de los móviles, y éstos con las imágenes de las cámaras de videovigilancia y la información de los sistemas de control de un edificio.

Ante la tentación simplista de alegrarse por la fácil interconexión de sistemas y pensar en conectarlos todos en un mismo "totum-revolutum", el responsable de seguridad que actualmente diseña o gestiona un SSF debe ser conocedor de los principios básicos de esta tecnología para saber cómo minimizar las vulnerabilidades y amenazas que le acechan.

En los siguientes apartados se describen las principales vulnerabilidades que el mundo IT "contagia" a nuestros anteriormente robustos y seguros SSF y ciertos enfoques de cómo combatirlas. Es importante recalcar que no se trata solo de adoptar soluciones técnicas, sino que se ha de empezar por adoptar medidas a nivel de política de seguridad y de organización de los recursos.

4.1 Medidas de ciberseguridad tradicionales de entornos IT

4.1.1 Ampliación de la política de seguridad con enfoque integral ciberfísico

Tradicionalmente ha sido habitual que, en gran parte de las organizaciones, las responsabilidades de la seguridad a nivel físico y a nivel de sistemas de la información han recaído en personas diferentes. Sería recomendable seguir el principio de "unidad de mando", concepto bien conocido en toda organización defensiva para unificar objetivos, criterios y diseño organizativo.

Posiblemente uno de los mayores logros de la ley de Protección de Infraestructuras Críticas o Ley PIC (Ley 8/2011) fue el impulsar la concepción de una seguridad integral en las organizaciones públicas y privadas donde cada vez es más complicado aislar las amenazas físicas de las cibernéticas en las instalaciones.

En las últimas décadas ha sido notorio el incremento en la consciencia de la necesidad de la ciberseguridad en las organizaciones, y esto ha promovido la adopción de medidas tan concretas como la certificación ISO 27001 en los sistemas de información más sensibles.

Cualquier organización moderna y con visión de perdurar en el tiempo debe plantearse disponer de una Política de Seguridad Integral que unifique ambos enfoques

de manera convergente y adecuadamente alineada con el negocio/misión de la organización, y dotada de los recursos suficientes para su cumplimiento.

4.1.2 Implicación de la alta dirección en la visión integral de la seguridad

Siguiendo con el punto anterior, es obvio que para que una política de seguridad integral tenga sentido y se lleve a cabo coherentemente es vital la implicación de la alta dirección con este objetivo.

Esta implicación se ha de demostrar en varios aspectos:

- La alineación de la política de seguridad con los objetivos del negocio.
- La participación del responsable de la política de seguridad integral en los órganos de dirección de la organización.
- La dedicación de suficientes recursos técnicos humanos y económicos en su consecución, y
- El esfuerzo en la diseminación de la cultura de la seguridad en toda la organización.

Es importante recalcar que la clasificación tradicional de los activos de una organización (personas y bienes), se amplió hace ya unas décadas con una tercera categoría, la información, a los cuales hay que añadir un cuarto enfoque que es la reputación.

4.1.3 Comunicación y aprovechamiento de las sinergias entre departamentos

El hecho de que la tecnología IP sea la base de los sistemas IT de las organizaciones, junto con el de que la concienciación por la ciberseguridad de los sistemas de la información ha cogido gran importancia en las últimas décadas, ha propiciado que muchas organizaciones fomenten la estandarización de procedimientos en sus departamentos de informática o IT, incluso llegando a la creación de estándares de certificación como la ISO 27001.

La ventaja principal del proceso de obtener una certificación es que, más allá del hecho de obtener el deseado certificado final, la organización se ha de replantear honestamente sus necesidades, la priorización de sus activos y la elaboración de los procedimientos oportunos que le ayuden a asegurar la continuidad del negocio ya que los sistemas de información son básicos para el mismo.

Muchas de las medidas técnicas que se han de adoptar en los SSF por las vulnerabilidades que la tecnología IT aporta al entorno son muy similares, cuando no idénticas, a las que aplica el departamento de IT en su día a día.

Por ello es muy conveniente que los procedimientos y medidas que se adopten en el entorno de los SSF se basen y coordinen con los existentes en el resto de las instalaciones IT de la organización.

Como se ha dicho, la implicación de la alta dirección en estos asuntos es imprescindible para evitar la estanqueidad de la información y propiciar la colaboración y el aprovechamiento de las sinergias.

Los beneficios de este enfoque son múltiples siendo los más claros, por ejemplo:

- La reducción del tiempo de elaboración de nuevos procedimientos desde cero.
- La adquisición conjunta de sistemas y licencias.
- La dedicación compartida de recursos de personal en las labores de implantación y/o mantenimiento.
- La monitorización de amenazas híbridas (físico-lógicas).
- Etc.

4.1.4 Formación y concienciación en ciberseguridad del personal involucrado

Uno de los principios básicos de la seguridad es que un sistema es tan vulnerable como lo sea el más débil de los eslabones que lo conforman.

La realidad confirma en el día a día que el factor humano, dotado de sus grandes cualidades difícilmente reemplazables por una máquina, también es mucho más propenso a cometer errores que los sistemas electrónicos.

Es por ello indispensable que las personas involucradas en el diseño, implantación y mantenimiento de los SSF reciban la adecuada formación para estar al día en un mundo tan cambiante como es el entorno digital actual.

Por otro lado, de nada vale tener los sistemas más avanzados y caros del mercado si el personal que trabaja con ellos no está adecuadamente motivado y concienciado frente a la ciberseguridad.

Cualquier presupuesto de implantación o adaptación de un SSF debe dotarse de una partida presupuestaria para la formación periódica y las campañas continuas de concienciación.

4.1.5 Independencia de las redes de seguridad respecto a otros sistemas

El hecho de que hoy en día la mayoría de los sistemas modernos existentes (ya sean de seguridad, de gestión de las instalaciones de un edificio, de alumbrado, de información, etc.) estén interconectados mediante tecnología IP obliga a prestar especial atención a la interconexión de los sistemas para evitar extracción indebida de la información, o accesos no deseados a los sistemas de seguridad.

Desde hace décadas es habitual que los edificios y grandes instalaciones se doten de sistemas de comunicaciones basados en estándares como el cableado estructurado que permitan la conexión de equipos electrónicos de muy diversa naturaleza y propósito.

Generalmente estos sistemas se componen, a grandes rasgos, de los siguientes elementos:

- Uno o varios cuartos de sistemas que alojan los armarios o racks de comunicaciones, a los cuales llega el cableado tanto del exterior de la instalación como de las áreas interiores y donde se alojan los equipos de electrónica que interconexionan elementos de todo tipo;
- Un cableado de comunicaciones bien sea de cobre con pares trenzados tipo UTP o de fibra de óptica, tendido horizontal o verticalmente por la instalación; y
- Unos puntos de acceso donde se conectan los elementos finales (cámaras de vigilancia, monitores de información, ordenadores de puestos de trabajo, teléfonos, máquinas de vending, puntos de acceso wifi, controladores de iluminación, etc.).

El esquema descrito permite que, con los equipos y los conocimientos adecuados, se puedan interconectar todos los elementos distribuidos por la instalación, y dotarlos del adecuado acceso hacia el exterior.

Uno de los pilares de diseño de la red de comunicaciones que soporte un SSF es que ésta esté lo más aislada posible del resto de las instalaciones.

El grado máximo de aislamiento posible que otorgara el mayor nivel de seguridad sería, obviamente, que no existiese interacción física entre la red de comunicaciones y los entornos exteriores de la instalación u otros sistemas internos de la misma que tengan diferente objetivo.

Pero este nivel de aislamiento no siempre es factible dado que, en muchas ocasiones, los puestos de gestión de la seguridad no se ubican en el mismo sitio o se requiere que la información sea transferida y compartida con sistemas remotos.

En este caso el diseño debe incluir una serie de elementos cortafuegos (firewall) o zonas desmilitarizadas (DMZ) que permitan ser configuradas adecuadamente para permitir únicamente ciertos accesos y en ciertos momentos.

Más allá de la utilización de diferentes equipos de comunicaciones para la red de seguridad frente al resto de sistemas es importante una adecuada política de segmentación de redes que mantenga controlado el nivel de riesgo de los accesos indebidos.

4.1.6 Protección física de los sistemas informáticos

Se da la peculiar paradoja de que para proteger los sistemas IT que dan servicio a una entidad es necesario dotarlos de elementos de seguridad física.

Es el caso de los controles de acceso y las cámaras de vigilancia de los centros de procesos de datos, los cuartos técnicos y los racks de comunicaciones.

Una vez más, la superposición de las diferentes medidas de seguridad en capas física-lógica-física hace necesaria la coordinación entre los diferentes departamentos de la organización y la existencia de unos procedimientos detallados y que se cumplan.

4.1.7 Utilización de equipos personales

Desde hace ya décadas es habitual que en las organizaciones parte del personal comparta dispositivos electrónicos para su uso particular y para el uso profesional, tales como teléfonos inteligentes, tabletas y ordenadores. A esta práctica se le conoce como BYOD (*Bring Your Own Device*)

Es una realidad que hay que tener en cuenta y que debe ser adecuadamente regulada y, en caso de ser autorizada, se deben implementar los medios adecuados de protección tales como control remoto de los dispositivos, antivirus centralizado, establecer una política para la gestión de dispositivos BYOD, etc.

4.1.8 Acceso remoto de personal propio o proveedores

Uno de los riesgos más importantes que se han introducido en los sistemas en los últimos años por la convergencia del mundo IP, es la costumbre (o necesidad) de permitir el acceso remoto de personas a los sistemas de la organización.

Además, cada vez hay más organizaciones que posibilitan a sus plantillas la posibilidad de compaginar trabajo presencial con teletrabajo.

Estas prácticas deben ser adecuadamente analizadas y reguladas. Es imprescindible tanto –analizar su necesidad, como acotar las personas que tengan acceso a la misma, procedimentar las formas de acceso, implementar las medidas de control correspondientes, etc.

Este es uno de los casos en que es más clara las sinergias con el resto de los sistemas IT de la organización.

Adicionalmente cada vez está más extendido que muchos servicios de mantenimiento y actualización de sistemas se traten de realizar en remoto por los proveedores, motivado sobre todo por la reducción de costes y la inmediatez de las intervenciones.

De nuevo es una práctica que debe ser cuidadosamente analizada y, en caso de ser necesaria, hay que adoptar medidas técnicas como la implementación de una máquina de salto adecuadamente controlada por el personal de la organización que no permita el acceso directo de ningún agente externo no deseado.

4.1.9 Seguridad de la nube

En la última década la nube ha invadido indudablemente todos los aspectos del día a día.. Actualmente es prácticamente imposible vivir sin ser usuario de banca online, ocio con vídeo bajo demanda, almacenamiento en la nube, etc.

No obstante, el sector de la seguridad, posiblemente por la criticidad de su visión, pero también por su desconfianza ante los elementos que no controla, es uno de los más reticentes a migrar a la nube.

Posiblemente cualquier profesional de la seguridad estará tranquilo sabiendo que los equipos que gestionan sus sistemas de seguridad están alojados en su CPD, bajo la atenta mirada de sus cámaras, las puertas controladas con sus controles de acceso, y dentro de edificios supervisados por sus vigilantes de seguridad.

Pero también es cierto que los servicios en la nube ofrecen ventajas como la replicación de los sistemas que albergan la información, facilitan el acceso desde cualquier entorno, y aseguran un nivel de visibilidad mayor que el de un CPD privado.

Obviamente la nube no es una solución válida para cualquier tipo de instalación, pero sí es una opción que ha de tenerse en cuenta y valorar adecuadamente.

La inclusión de una plataforma basada en nube que de soporte a un sistema de seguridad debe definir aspectos tales como:

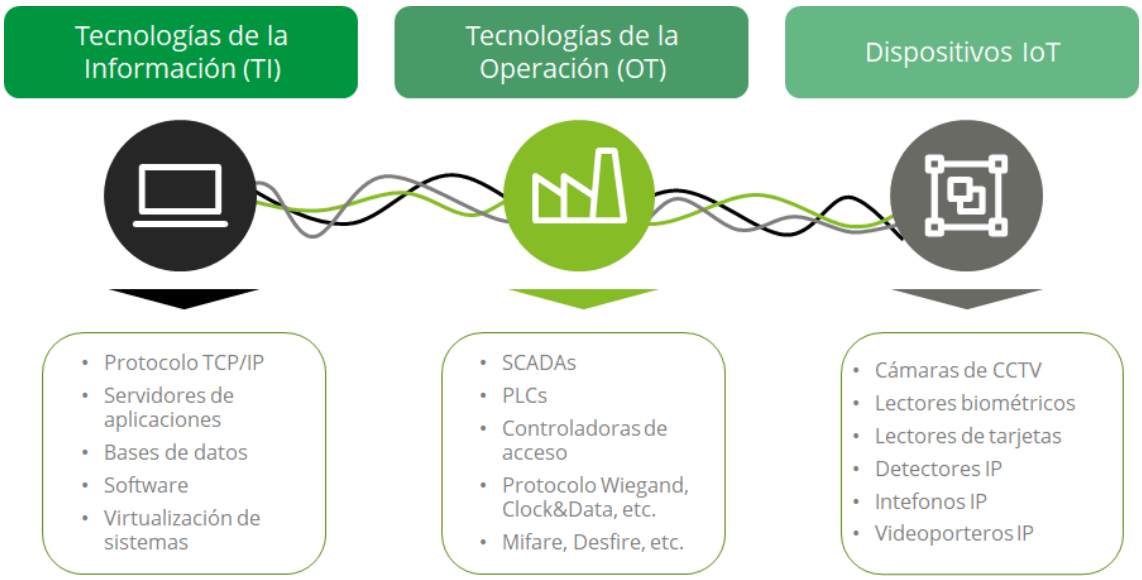
- Acuerdo de nivel de servicio (SLA) con proveedores externos, (tanto de la nube como de sus comunicaciones).
- Modelos de nube.
- Definición de requisitos de seguridad en nube.
- Establecimiento de política de uso.
- Replicación y disponibilidad del almacenamiento.
- Cumplimiento del Reglamento General de Protección de Datos europeo.
- Etc.

4.2 Medidas de ciberseguridad específicas para sistemas de seguridad física

Tal y como se ha descrito anteriormente, los sistemas de seguridad física presentan numerosos desafíos frente a las ciberamenazas. Se distinguen tres grandes bloques dentro de estos sistemas:

- Sistemas y protocolos propios de los entornos de Tecnologías de la Información: redes TCP/IP, servidores de aplicaciones, bases de datos, software, virtualización de sistemas, etc.
- Sistemas y protocolos propios de los entornos de Tecnologías de la Operación: sistemas y protocolos propios empleados en los sistemas de seguridad física como Mifare, Wiegand, controladoras de acceso, PLCs, etc.

- Dispositivos IoT conectados:
  - Subsistema de intrusión: centrales de intrusión, expansores de zonas, detectores, etc.
  - Subsistema de control de accesos: lectores, controladoras, etc.
  - Subsistema de circuito cerrado de televisión: cámaras, videograbadores, etc.
  - Subsistema de interfonía: interfonos, videoporteros, centrales de interfonía, etc.



Los múltiples sistemas y protocolos disponibles de los distintos entornos de IT, OT e IoT incorporan mayores dificultades para proporcionar sistemas de seguridad física ciberseguros al no ser posible la extrapolación directa de las medidas de ciberseguridad tradicionales a estos entornos. Se hace necesario incorporar tratamientos específicos a las vulnerabilidades propias existentes en los sistemas de seguridad física, así como proporcionar medidas de ciberseguridad tradicionales de los entornos propios de IT.

En este apartado, se describen las vulnerabilidades más importantes y específicas que afectan y están presentes en los sistemas de seguridad física que los responsables de seguridad de una organización deben conocer, contemplar y mitigar para evitar mantener sistemas de seguridad vulnerables.

4.2.1 Tecnologías de identificación en sistemas de control de accesos

Gran parte de las organizaciones emplean métodos de control de acceso por identificación mediante tarjeta de proximidad en sus diversas instalaciones. Estos sistemas presentan vulnerabilidades que tienen que ser analizadas y mitigadas de manera adecuada.

Los sistemas de control de acceso que utilizan la identificación por medio de tarjetas electrónicas de proximidad permiten llevar a cabo el proceso de autenticación e identificación de dos maneras:

- Lectura del Card Serial Number (CSN) o ID de la tarjeta.
- Identificador (ID) almacenando en un sector de memoria de la tarjeta protegido mediante uso de criptografía.

Tanto la identificación por medio del uso del CSN como algunos de los protocolos y tecnologías empleados para la protección del ID en uno de los sectores de memoria de la tarjeta presentan vulnerabilidades que los responsables de seguridad de una organización deben conocer, evitar o mitigar en su caso.

4.2.1.1 Uso del CSN como medio de identificación en tarjetas

Necesidad:

El CSN o Card Serial Number es un número que se graba en la memoria de las tarjetas durante el proceso de fabricación. El problema de utilizar este medio como modo de identificación es que en la actualidad es muy sencillo llevar a cabo la clonación de estos identificadores. Esto representa una vulnerabilidad si los lectores hacen uso únicamente de este número para identificarse en el sistema.

El UID o CSN no debe emplearse como mecanismo seguro de identificación en control de accesos (es transmitido sin cifrar, en texto plano) ya que puede ser leído por cualquier lector que cumpla con los protocolos de la ISO 14443 y clonado.

Adicionalmente, en muchos casos, estos identificadores no son únicos y podrían ser empleados en distintas organizaciones sin conocimiento alguno generando una brecha de seguridad adicional.

Solución:

Debe evitarse el uso del CSN como identificador de accesos para no generar una brecha de seguridad en las instalaciones de una organización y que pueda ser explotada por atacantes con conocimientos específicos en estos sistemas.

4.2.1.2 Identificación por medio de ID almacenado en sector de memoria

Necesidad:

El modo de funcionamiento más seguro de identificación por medio de tarjetas electrónicas en un sistema de control de accesos es almacenar las credenciales en forma de datos sobre los sectores de memoria de las tarjetas, protegidos mediante claves cifradas almacenadas tanto en la tarjeta como en los lectores de control de acceso, de modo que se permita una autenticación e identificación seguras de las tarjetas contra los lectores y viceversa.

Las consideraciones a tener en cuenta en este método de identificación y autenticación radican en los algoritmos de cifrado que se emplean en las comunicaciones entre la tarjeta y el lector. Algunos de los sistemas comúnmente utilizados para llevar a cabo la identificación de los usuarios por tarjetas electrónicas emplean algoritmos cuyos sistemas de cifrado son vulnerables como Mifare Classic.

Según la normativa EN-60839 de referencia para sistemas de control de accesos, los sistemas que almacenan las credenciales sobre los sectores de memoria de las tarjetas cumplen con un grado de seguridad 4. Sin embargo, esta normativa no tiene en cuenta ni analiza las vulnerabilidades que presentan alguno de los algoritmos existentes en el mercado.

Algunas tecnologías emplean algoritmos de cifrado propietarios que dificultan en mayor medida la capacidad de llevar a cabo las actualizaciones y evoluciones necesarias, por las limitaciones de las empresas que los desarrollan, para poder subsanar las vulnerabilidades que son detectadas en dichos algoritmos.

Solución:

Es necesario el empleo de protocolos y algoritmos seguros y se recomienda que los mismos sean protocolos abiertos que sigan los estándares internacionales de demostrada eficacia ya que se trata de normas que son revisadas y verificadas de forma regular por los organismos correspondientes, con el objetivo de ofrecer los niveles de seguridad más transparentes posibles.

Por tanto, se ha de evitar el uso del CSN de las tarjetas y emplear el método de almacenamiento de las credenciales cifradas en los sectores de memoria de las mismas considerando algoritmos de encriptación que no presenten vulnerabilidades y hayan sido comprometidos.

4.2.2 Protocolos de comunicación en sistemas de control de accesos

Necesidad:

Al margen de los ataques para vulnerar las credenciales de las tarjetas, los sistemas de control de acceso presentan vulnerabilidades adicionales en los protocolos de comunicación estandarizados para las comunicaciones entre los lectores y las controladoras de acceso intermedias.

La gran mayoría de sistemas de control de acceso emplean en las comunicaciones entre lector y controlador protocolos de comunicación que no son seguros, como Wiegand o Clock&Data. Estos protocolos emplean comunicaciones sin cifrar (en texto plano) por lo que las transacciones pueden ser capturadas, analizadas y reproducidas por un atacante.

Para llevar a cabo un ataque sobre las comunicaciones entre lector y controlador de accesos que emplean protocolos de comunicación sin cifrar, un atacante únicamente necesitaría acceder a las líneas de comunicación. Para ello, podría manipular directamente el lector de control de accesos desmontando el mismo, que se encuentra

ubicado en el lado no seguro del control de acceso (ya que es el medio de identificación encargado de controlar el acceso), para poder acceder a las comunicaciones entre el lector y el controlador.

Una vez con acceso a las líneas de comunicación, el atacante podría llevar a cabo un ataque "man-in-the-middle" con la finalidad de monitorizar todo el tráfico entre los dispositivos y capturar credenciales con acceso permitido en el punto de control de accesos en cuestión. Este ataque consistiría en colocar un dispositivo intermedio en medio de la línea que permita captar los datos del usuario que se transmiten desde el lector al controlador. El dispositivo sería capaz de almacenar estos datos y transmitirlos hasta el atacante. Además de poder llevarse a cabo la captura de datos para poder realizar una clonación de tarjetas, otros patrones relevantes podrían ser utilizados por el atacante como patrones de comportamiento de usuarios (horarios, turnos, utilización de los puntos de control, etc.).

Solución:

Es necesario que las organizaciones mitiguen las vulnerabilidades presentes en los protocolos de comunicación de control de acceso tradicionales por medio de la supervisión del estado de la línea en las comunicaciones y el cifrado de los datos que se transmiten en la misma.

En algunos casos, los lectores disponen de un contacto (tamper) en la carcasa del dispositivo que genera una señal de alarma si se lleva a cabo cualquier tipo de manipulación sobre el equipo. Esta medida de protección auxiliar, aunque no permitiría proteger directamente las comunicaciones entre lector y controlador de acceso, sí que permitiría alertar a los responsables de seguridad de la organización de cualquier manipulación en el lector. Por tanto, es necesario que esta señal de tamper se cablee y configure adecuadamente.

Adicionalmente, es necesario implementar protocolos de comunicación entre lector y controlador que utilicen comunicaciones cifradas como, por ejemplo, OSDP (Open Supervised Device Protocol). Este tipo de protocolos proporcionan protección frente a los ataques "man-in-the-middle" al utilizar criptografía sobre el canal de comunicación.

Por otro lado, es recomendable que los protocolos de comunicación cifrados que se empleen sean protocolos abiertos que permitan interoperabilidad y sean empleados por la mayoría de fabricantes de control de accesos.

Por tanto, es necesario que sobre nuevos proyectos de seguridad física o migraciones de sistemas existentes se tengan en cuenta estas vulnerabilidades y sean tratadas desde el diseño o durante el ciclo de vida de los activos.

4.2.3 Control de acceso lógico en dispositivos IoT y sistemas

4.2.3.1 Gestión de identificadores y contraseñas en dispositivos IoT

Necesidad:

Los fabricantes de sistemas de seguridad física incorporan contraseñas por defecto en todos los dispositivos IoT que comercializan (cámaras, lectores biométricos, interfonos, etc.). En muchos casos, estas contraseñas no requieren ser reemplazadas durante el proceso de instalación de los equipos de seguridad física proporcionando una puerta abierta a usuarios no legítimos.

Las contraseñas por defecto que incluyen los dispositivos IoT de seguridad física normalmente son contraseñas poco robustas que no incluyen combinaciones de letras, números, así como uso de mayúsculas, minúsculas y caracteres especiales. Adicionalmente, en muchos casos, tanto los identificadores como las contraseñas por defecto de acceso a los dispositivos IoT son siempre las mismas para los equipos de la misma gama fabricante y pueden incluso encontrarse de manera pública en Internet.

Por tanto, no gestionar adecuadamente los identificadores y contraseñas de los dispositivos IoT de seguridad física incorpora una brecha de seguridad en estos sistemas que puede ser explotada por atacantes y utilizarlos como puntos de entrada a los sistemas internos de una organización.

Estas vulnerabilidades presentes en los equipos de seguridad pueden provocar que un atacante comprometa los datos confidenciales almacenados por los equipos, llevar a cabo cambios en las configuraciones de los sistemas e incluso enviar o relevar la información disponible en los equipos, pudiendo derivar, incluso, en sanciones para las organizaciones debido a incumplimiento de la legislación vigente de privacidad de datos.

Solución:

Para evitar que los atacantes puedan explotar estas vulnerabilidades es necesario:

- Aplicar y hacer cumplir una política de contraseñas para todos los dispositivos IoT de seguridad física que incluya contraseñas fuertes y tiempos de caducidad. Se recomienda que las contraseñas sean cambiadas con frecuencia, pero cuando no sea posible o práctico, se deberían considerar alternativas apropiadas.
- Revisar periódicamente todos los derechos de acceso.
- Modificar las contraseñas por defecto en el momento de la instalación de los dispositivos IoT.
- Aplicar técnicas que se basen en las reglas de necesidad de conocer.

Obligar a proveedores externos (por ejemplo, instaladores o mantenedores de sistemas de seguridad física) a firmar acuerdos de confidencialidad.

4.2.3.2 Gestión de contraseñas de administrador en sistemas de seguridad física

Necesidad:

Los fabricantes de sistemas de seguridad física incorporan en sus sistemas contraseñas de administrador, denominadas también maestras o root, que permiten completo acceso a las parametrizaciones y configuraciones globales de los sistemas. Adicionalmente, en muchos casos, los instaladores, mantenedores o integradores de sistemas de seguridad física incorporan a los sistemas contraseñas maestras que ni siquiera son comunicadas a los responsables de seguridad de la organización, permitiéndoles un acceso y control total a dispositivos y sistemas.

Las contraseñas root que incluyen los sistemas de seguridad física permiten el acceso global a los sistemas y normalmente son contraseñas poco robustas que no incluyen combinaciones de letras, números, así como uso de mayúsculas, minúsculas y caracteres especiales. Adicionalmente, en muchos casos, se mantienen por defecto, por lo que es habitual el empleo de las mismas contraseñas en sistemas de distintas organizaciones.

Por otro lado, estas contraseñas root son conocidas por personal externo a la organización el cual, normalmente, no dispone de los mismos procesos de gobierno y control que los que se realizan sobre el personal propio.

Por tanto, una gestión inadecuada de las contraseñas root puede dejar abierta una nueva brecha de seguridad en estos sistemas que puede ser empleada por los atacantes.

Solución:

Para solventar y mitigar estas vulnerabilidades presentes en los sistemas de gestión de seguridad física es necesario:

- Aplicar y hacer cumplir una política de contraseñas root para todos los sistemas de seguridad física. Se recomienda sustituir los usuarios “administrador” por otros con el mismo nivel de acceso, o en su defecto al menos incluir contraseñas fuertes y con tiempos de caducidad.
- En caso de permitir el uso de contraseñas root es necesario modificar las contraseñas por defecto de los sistemas en el momento de la instalación de las medidas de seguridad física.
- Revisar periódicamente todos los derechos de acceso.
- Aplicar técnicas que se basen en las reglas de necesidad de conocer.
- Obligar a proveedores externos (por ejemplo, instaladores o mantenedores de sistemas de seguridad física) a firmar acuerdos de confidencialidad.

4.2.4 Control de acceso remoto en dispositivos IoT

Necesidad:

Los dispositivos IoT de seguridad física permiten en muchos casos el acceso remoto a los mismos (por ejemplo, para dar mantenimiento a los equipos). Disponen de backdoors (puertas traseras) que pueden ser explotadas por hackers o usuarios maliciosos para tomar el control de los dispositivos y ser el punto de acceso a los sistemas de una organización.

Estos puntos de acceso remoto, sin un control adecuado, pueden permitir que un atacante acceda a la información de los dispositivos (por ejemplo, imágenes de cámaras de circuito cerrado de televisión) o modificar sus perfiles de configuración o acceso. Además, las organizaciones pueden verse expuestas a sanciones derivadas de incumplimientos en la legislación vigente, por ejemplo, ante el incumplimiento de las leyes de privacidad.

Solución:

Para evitar que los atacantes puedan explotar estas vulnerabilidades presentes en los sistemas IoT de seguridad física es necesario:

- Realizar análisis de vulnerabilidades y/o test de penetración en los dispositivos IoT antes de la puesta en marcha de los equipos con la finalidad de detectar puntos de acceso remoto a los equipos no autorizados.
- Deshabilitar las backdoors que son detectadas en los dispositivos o configurar las mismas de manera que sólo usuarios legítimos puedan acceder de manera remota a los equipos de seguridad.
- Llevar a cabo análisis de vulnerabilidades y/o test de penetración de manera periódica a lo largo del ciclo de vida de los dispositivos IoT para asegurar que no se habiliten puntos de acceso remoto no autorizados por la organización.

4.2.5 Gestión de parches y vulnerabilidades en sistemas de seguridad física

Necesidad:

En muchos casos, las organizaciones disponen de una gran variedad de equipos de sistemas de seguridad física de diferentes fabricantes. Es muy común que incluso equipos que son empleados para una misma función (por ejemplo, controlar puertas de acceso en el interior de una instalación o supervisar áreas de interés mediante cámaras de circuito cerrado de televisión) no sean homogéneos en todos los puntos y se incluyan dispositivos con diferentes características e incluso de fabricantes diferentes.

La falta de homogeneidad de equipos en las instalaciones de una organización, la infinidad de fabricantes en el mercado y el continuo avance en las tecnologías y dispositivos de seguridad física, dificulta una gestión adecuada de las actualizaciones o parches de seguridad de sistemas y dispositivos de seguridad.

Una gran parte de los dispositivos IoT o sistemas de seguridad física no permiten la gestión automatizada de las actualizaciones o parches de seguridad dificultando aún más su gestión eficaz. Adicionalmente, no suelen existir mecanismos de comunicación claros y precisos entre los responsables de seguridad de una organización y los proveedores o fabricantes de los equipos instalados en sus instalaciones, lo que imposibilita que nuevas actualizaciones en los dispositivos y sistemas sean transmitidas de manera rápida y adecuada a los responsables de la organización.

Solución:

Es necesario establecer un proceso eficaz de gestión de parches y vulnerabilidades de los dispositivos IoT y sistemas de seguridad que permita detectar, distribuir y aplicar actualizaciones de firmware a cada uno de los equipos de seguridad física instalados. Es recomendable, también, disponer de suscripciones con los fabricantes de los sistemas instalados que permitan proporcionar una comunicación rápida y eficaz de las nuevas actualizaciones de seguridad.

Los procesos deben tener en cuenta la certificación de los proveedores de parches, las pruebas de las actualizaciones antes de su aplicación y un proceso de despliegue que minimice el riesgo de interrupción durante el cambio. Este proceso debe contar con las siguientes actividades:

- Detección e inventariado de equipos: Se requiere inventariar los sistemas y dispositivos IoT de seguridad física instalados en cada una de las instalaciones de la organización, así como las versiones de firmware desplegadas en los equipos.
- Investigación: Establecer un proceso de análisis continuo para identificar vulnerabilidades a lo largo del ciclo de vida de los sistemas.
- Valoración: Evaluación del riesgo de las vulnerabilidades detectadas en el proceso de análisis a partir de la determinación del impacto y probabilidad de la amenaza.
- Priorización de vulnerabilidades: Proceso de priorización de remediar las vulnerabilidades en base a la valoración de riesgo realizada.
- Prueba de actualizaciones: Antes del despliegue de las actualizaciones, es necesario llevar a cabo pruebas de las actualizaciones de sistemas y dispositivos IoT para confirmar que las mismas no afectan a la operatividad continua.
- Despliegue: El último paso consiste en el proceso de control y gestión en la distribución y aplicación de los parches en los dispositivos IoT.

Cuando durante el proceso de análisis o prueba se detecte que los parches de seguridad no puedan ser aplicados, será necesario considerar medidas alternativas apropiadas de protección que permitan mitigar los riesgos identificados.

5 Los nuevos servicios de seguridad necesarios

La necesidad ineludible de dotar de medidas de ciberseguridad a los Sistemas de Seguridad Físicos (SSF) genera a su vez una importante transformación de los servicios de Seguridad relacionados con los Sistemas de Seguridad "tradicionales", aunque la reglamentación actual no los contemple (ni los prohíba).

A pesar de que no haya legislación específica que cubra estas cuestiones, se hace imprescindible que estos aspectos se tengan en cuenta a la hora de realizar un proyecto de seguridad y no solo apelando al buen hacer y al deseo propio de la excelencia profesional, sino por ser bien conocedores del riesgo que supone plantear o mantener una instalación con puntos débiles.

Estos servicios se pueden concretar en tres categorías:

- Ingeniería y Consultoría de Seguridad
- Instalación de SSF
- Mantenimiento de SSF

Todos ellos deben completarse en sus prestaciones actuales con las que se describen a continuación, lo cual también incluye una oportunidad nueva de negocio para las empresas proveedoras de estos servicios.

5.1 Ingeniería y consultoría de seguridad

Estos servicios, no siempre existentes de forma separada a los de Instalación del SSF, deben tener en cuenta que:

- Los Análisis de Riesgos han de seguir el ciclo expuesto en esta guía, de forma que incluyan los riesgos correspondientes a las vulnerabilidades del SSF.
- La propuesta de medidas de Seguridad debe incluir las medidas de ciberseguridad aplicables a los SSF.
- La elección de las tecnologías a utilizar en el SSF debe tener en cuenta qué elementos disponen de las características intrínsecas de ciberseguridad necesarias y, en su caso, de las certificaciones aplicables.
- La descripción de las tareas de formación, pruebas y puesta en marcha, mantenimiento y administración del SSF incluidas en el proyecto deben tener en cuenta todo lo expuesto en esta Guía en lo que respecta a las necesidades derivadas de la ciberseguridad de los SSF.
- Los procedimientos de operación propuestos deben tener en cuenta los correspondientes a la administración del SSF desde la perspectiva de la ciberseguridad del mismo, incluso, en su caso, la interacción con el responsable de seguridad del Departamento de IT del usuario final.

5.2 Instalación de SSF

En esta actividad puede haberse incluido o no el proyecto del SSF:

- Si se había incluido, deberá aplicarse lo expuesto en el apartado anterior.
- Si no se había incluido, es posible que la empresa instaladora se encuentre con que el SSF había sido proyectado por otra empresa. En este caso, se debe analizar si lo expuesto en el punto 5.1 se encuentra incluido en el proyecto a seguir y, si fuera necesario, relacionar los incumplimientos o carencias encontradas para proponerlas como parte de su oferta de instalación, ya que de otra manera se puede encontrar frente al riesgo de que haya carencias de ciberseguridad en el diseño inicial que le perjudiquen en su proceso de instalación y/o posterior mantenimiento.

En cuanto al servicio concreto de la instalación ha de tener en cuenta:

- La instalación de los elementos del SSF deben seguir las indicaciones de ciberseguridad inherentes descritas por los fabricantes.
- La parametrización de los elementos ha de realizarse teniendo en cuenta las vulnerabilidades de ciberseguridad (por ejemplo, el cambio de claves por defecto).
- Se dispondrán todas las medidas de ciberseguridad genéricas de IT (apartado 4.1 de esta Guía) y las específicas de SSF (apartado 4.2).
- Las pruebas y puesta en servicio se harán teniendo en cuenta las medidas de ciberseguridad dispuestas.
- La documentación “as built” (fin de obra) deberá incluir todos los esquemas, tablas y manuales correspondientes a las medidas de ciberseguridad dispuestas.

5.3 Mantenimiento de SSF

El mantenimiento de un SSF se ve afectado ineludiblemente por la incorporación al Sistema de sus propias medidas de ciberseguridad.

Es posible que esta ampliación de las tareas de mantenimiento no se contrate con la empresa de mantenimiento de Seguridad “tradicional”, sino que se haga cargo del mismo otra empresa especializada de ciberseguridad o el propio Departamento de ciberseguridad del usuario.

Sea la empresa de Mantenimiento del SSF, una empresa especializada de ciberseguridad o el propio Departamento de ciberseguridad del usuario los que se hagan cargo de gestionar, monitorizar y mantener las medidas de ciberseguridad en los SSF, será necesario que en los servicios de mantenimiento se incluyan las tareas correspondientes a:

- Evaluación periódica de los niveles de riesgo y gestión de los mismos a partir de indicadores, métricas y reporte.
- Gestión de activos (inventario, riesgos en el ciclo de vida en la cadena de suministros, etc.).

- Evaluación y actualización de los requisitos de seguridad, verificación del cumplimiento en las políticas de seguridad de la organización y acuerdos de nivel de servicio para sistemas en la nube.
- Verificación y actualización del bastionado de sistemas y configuraciones seguras.
- Revisión de políticas y sistemas de protección frente al malware.
- Revisión de la seguridad de red (control de acceso a la red, mail, segmentación, etc.).
- Revisión de las políticas de control de acceso lógico y gestión del ciclo de vida de las identidades.
- Gestión de incidentes de ciberseguridad.
- Evaluación de la resiliencia de los sistemas.
- Gestión de parches y vulnerabilidades.

Estos servicios han de estar apoyados en un marco normativo conformado por políticas, normas y procedimientos que permitan establecer un gobierno de la ciberseguridad en los SSF. El marco normativo podrá ser desarrollado por personal interno o externo de la organización, pero la responsabilidad de su aprobación, seguimiento, control en la adherencia y cumplimiento recaerá siempre en la propia organización.

6 Bibliografía

(1) Guías CCN-STIC-480 de Seguridad en el control de procesos y SCADA, publicado por el CCN-CERT (Centro Criptológico Nacional – Computer Emergency Response Team)

(2) MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Libro II – Catálogo de Elementos, publicado por el CCN-CERT (Centro Criptológico Nacional – Computer Emergency Response Team)

(3) ***El punto en el que la seguridad y la ciberseguridad convergen*** - Publicado el 17/04/2019, por INCIBE https://www.incibe-cert.es/blog/el-punto-el-seguridad-y-ciberseguridad-convergen