ESTUDIOS TOPOGRAFICOS, MECANICA DE SUELOS, AMBIENTALES, HIDROLOGICOS, JURIDICOS, FINANCIEROS, FERROVIARIOS, ELECTROMECANICOS Y MATERIAL RODANTE PARA LA ELABORACION DEL PROYECTO EJECUTIVO PARA LA CONSTRUCCIÓN DEL TREN INTERURBANO MEXICO – TOLUCA

MEMORIA DEL SES

Infraestructuras y Transportes

WWW.SENER.COM.MX

SENER

Control de firmas

Realizado	Revisado	Aprobado	Verificado
José Manuel Martín IRS	Enrique González Jordi Redó CE	Pablo Cruz Lorenzo Nogales DPE	David Madrid CAL
Agosto 2014	Agosto 2014	Agosto 2014	Agosto 2014

Aprobado electrónicamente mediante ruta

Información del Documento	
Título del documento	MEMORIA DEL SES
Número de documento	TITM-T4-ME-SRCTR-000-1486-001-108
Revisión	3
Contrato	DGTFM-09-14
Estimación	
Periodo de Estimación	
Referencia	Doc_01974313
Archivo digital	TITM-T4-ME-SRCTR-000-1486-001-108_02 Memoria del SES.docx

SENER

Registro de cambios

Rev	Fecha	Autor	Sección afectada	Cambios
00	Agosto 2014	José Manuel Martín	Todas	Edición Inicial
01	Agosto 2014	José Manuel Martín	Todas	Actualización del documento
02	Agosto 2014	José Manuel Martín	Todas	Correcciones
03	Agosto 2014		Todas	Correcciones

SENER

INDICE / TABLE OF CONTENTS

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

1 OBJETO

El objeto del presente documento consiste en definir las soluciones tecnológicas que satisfarán las funcionalidades requeridas para el subsistema de Securización (SES), así como describir el conjunto de elementos tecnológicos que apoyan la ejecución de la operación y el mantenimiento de dicho subsistema dentro de la futura línea ferroviaria de tren Interurbano México - Toluca.

Este documento expone y desarrolla las soluciones tecnológicas concretas escogidas para la implementación final del subsistema a partir de aquéllas que mejor se adaptan al caso de la futura línea ferroviaria de tren interurbano México - Toluca tanto a nivel conceptual como en clave de análisis de estado del arte de proyectos similares.

2 LISTADO DE ACRÓNIMOS

Acrónimo	*Significado*
ACL	Access Control List
API	Application Programming Interface
BCP	Business Continuity Plan
BDD	Base de Datos
BIT	Bitácora y Gestor Maestro
CA	Certification Authority
CCO	Centro de Control Operacional
CPU	Central Processing Unit
CTR	Centro de Control (elementos comunes)
DCS	Distributed Control System
DMZ	Desmilitarized Zone
DRP	Disaster Recovery Plan
ESB	Enterprise Service Bus
FIFO	First In, First Out
FTP	File Transfer Protocol
GUI	Graphical User Interface
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IHM	Interfaz Hombre Máquina

Acrónimo	*Significado*
ILS	Integrador de Sistemas de Línea
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol security
ISO	International Organization for Standardization
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NTP	Network Time Protocol
PC	Personal Computer
PCN	Plan de Continuidad del Negocio
PCZ	Puesto de Control Zonal
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PRD	Plan de Recuperación de Desastres
QoS	Quality of Service
RED	Red de Datos Multiservicio
RTU	Remote Terminal Unit
SAI	Sistema de Alimentación Ininterrumpida
SAN	Storage Area Network

Acrónimo	*Significado*
SCADA	Supervisory Control And Data Acquisition
SES	Securización de Subsistemas
SGBD	Sistema de Gestión de Bases de Datos
SGIA	Sistema de Gestión Integrado de Alarmas
SGSE	Sistema de Gestión y Supervisión de la Explotación
SIEM	Security Information and Event Management
SIM	Simulación
SNMP	Simple Network Management Protocol
SO	Sistema Operativo
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
SSO	Single Sign-On
SUGM	Sistema Unificado de Gestión y Mando
SUGPPU	Sistema Unificado de Gestión de Perfiles de Usuarios
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Tabla 1 Listado de acrónimos de la Memoria del Subsistema de Securización

3 DOCUMENTACIÓN DE REFERENCIA

Referencia	Documento
[1]	TITM-III-RQ-INT-000-0001-00 Requisitos Generales de la Línea
[2]	TITM-T4-ME-SRCTR-000-1486-003-107 Memoria Ejecutiva del Centro de Control

Tabla 2 Documentos de referencia

Referencia	Documento
[1]	ISO/IEC 27001:2013 Information security management systems — Requirements
[2]	ISO/IEC 27002:2013, Code of practice for information security management

Tabla 3 Estándares aplicables

4 INTRODUCCIÓN

Se define el subsistema de Securización de Subsistemas (SES) como el conjunto de todos los elementos hardware, software y de comunicaciones que permiten, como mínimo:

- Garantizar la integridad de los sistemas de información y evitar manipulaciones intencionadas o errores no intencionales (provenientes de la organización [internos] como de terceros [externos]).
- Proteger a los sistemas frente a ataques que puedan afectar a su disponibilidad y, por tanto, permitir a la red de datos operar de forma continua.
- Procurar la confidencialidad de los datos generados y almacenados por la red de datos y sus subsistemas, evitando que entes no autorizados puedan tener acceso a dichos datos.
- Una gestión sencilla de los parámetros y reglas de seguridad (que se deriven de lo estipulado en las políticas de seguridad) mediante las interfaces de gestión centralizada.
- Ofrecer un conocimiento en tiempo real, por parte de los operadores, del estado de los subsistemas (en términos de securización de los mismos) y realizar las acciones preventivas y correctivas que se definan.
- Disponer de mecanismos para realizar un plan de recuperación de datos y continuidad de negocio para, en caso de ser necesario, asegurar que la información vital para la operación se encuentre siempre disponible independientemente de los eventos o situaciones desastrosas que puedan ocurrir.

El buen funcionamiento de SES depende del correcto diseño, instalación y configuración de todos los elementos (hardware y software) que permiten la recogida de datos, la ejecución de las aplicaciones que constituyen la lógica del propio subsistema, el intercambio de información entre ellas, la correcta interacción final con los operadores del mismo y la buena disposición de éstos a la hora de cumplir con las políticas definidas y de seguir la buenas prácticas sugeridas (en términos de securización de subsistemas).

4.1 Alcance

SES abarca todo el equipamiento hardware y software que permite al operador/mantenedor de Securización ubicado en las salas de operaciones del Centro de Control Operacional (CCO) la supervisión (visualización del estado de las variables/alarmas), el control remoto (envío de órdenes) y el posible mantenimiento de los dispositivos relacionados con la securización de los subsistemas, redes e información que forman parte de la línea del tren interurbano México-Toluca.

El objetivo de la Securización (SES) es garantizar la Confidencialidad, Integridad y Disponibilidad de los subsistemas, redes y datos que conforman todo el sistema.

El alcance del Subsistema de Seguridad de Subsistemas (SES) comprende, entre otros, los siguientes módulos:

- Cortafuegos (firewalls)
- Solución Sistema de Detección de Intrusión (IDS)/Sistemas de Prevención de Intrusión (IPS)
- Sistemas para detección y bloqueo de código malicioso
- Licencias software de Gestión, Administración y Mantenimiento del Subsistema.
- Licencias Antivirus
- Trabajos de ingeniería de seguridad asociados al análisis de riesgos y vulnerabilidades.

- Cableado de alimentación eléctrica en baja tensión para alimentación de equipos.
- Latiguillos de interconexión de fibra óptica y cobre para la conexión de equipos a tomas de usuario o puertos de repartidor existentes.

4.2 Exclusiones

Cabe destacar que todo el equipamiento hardware del Centro de Control (Estaciones de Trabajo, servidores) restará fuera del alcance del subsistema, dado que su suministro formará parte del subsistema de Comunes del Centro de Control (CTR).

También queda fuera del alcance del subsistema SES el diseño y el hardware asociado a las distintas redes de comunicaciones que permiten el intercambio de datos entre los dispositivos de campo, los servidores de control, los puestos de operación, etc..

Se dotará de doble fuente de alimentación a los equipos críticos de SES; este estudio queda fuera del alcance de este subsistema

4.3 Conceptos generales de securización

El objetivo de la Securización (SES) proyectada es garantizar Confidencialidad, Integridad y Disponibilidad de los subsistemas, datos y redes que conforman todo el sistema de la línea ferroviaria del tren interurbano México - Toluca. Se define:

- Confidencialidad: la confidencialidad consiste en asegurar la accesibilidad de la información solamente a los usuarios que estén autorizados a tener acceso. El objetivo de la confidencialidad será, por tanto, prevenir la divulgación no autorizada de información.
- Integridad: la verificación de la integridad consiste en determinar si se han producido alteraciones o realizado modificaciones no autorizadas durante la operación (accidental o intencionadamente).
- Disponibilidad: el objetivo de la disponibilidad es garantizar el acceso a un servicio o a un recurso cuando esto sea necesario.

Ilustración 1. Principales principios de la seguridad

Desde el punto de vista funcional el sistema se diseñará para trabajar de manera continua; es decir, la disponibilidad del servicio y del sistema será la prioridad absoluta. Es por eso que SES considerará como factor crítico prioritario la disponibilidad del sistema, seguido de integridad de los datos y por último la confidencialidad de la información (ver figura).

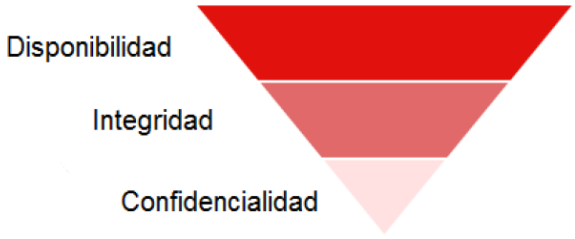


Ilustración 2. Comparativa de prioridades

Otros puntos a garantizar dentro del concepto de securización serían:

- Autenticación: consiste en la confirmación de la identidad de un usuario. Un control de acceso permite garantizar el acceso a los subsistemas y equipos relacionados únicamente a personas autorizadas.
- No repudio: evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas puede negar en el futuro una operación realizada por ella.

Para alcanzar dicho objetivo se deben plantear y definir los siguientes puntos:

- ¿Qué recursos se quieren proteger?
- ¿De qué amenazas se deben proteger?
- ¿En qué grado se necesita protegerlos?
- ¿Qué mecanismos y herramientas implantar para alcanzar un óptimo nivel de seguridad sin perder de vista la relación costo/beneficio?

Definidos estos puntos se podrán diseñar las políticas de seguridad adecuadas y tendentes a implementar y crear un perímetro de defensa que permita alcanzar el objetivo de Securización definido.

Gráficamente, podemos resumir la seguridad en:

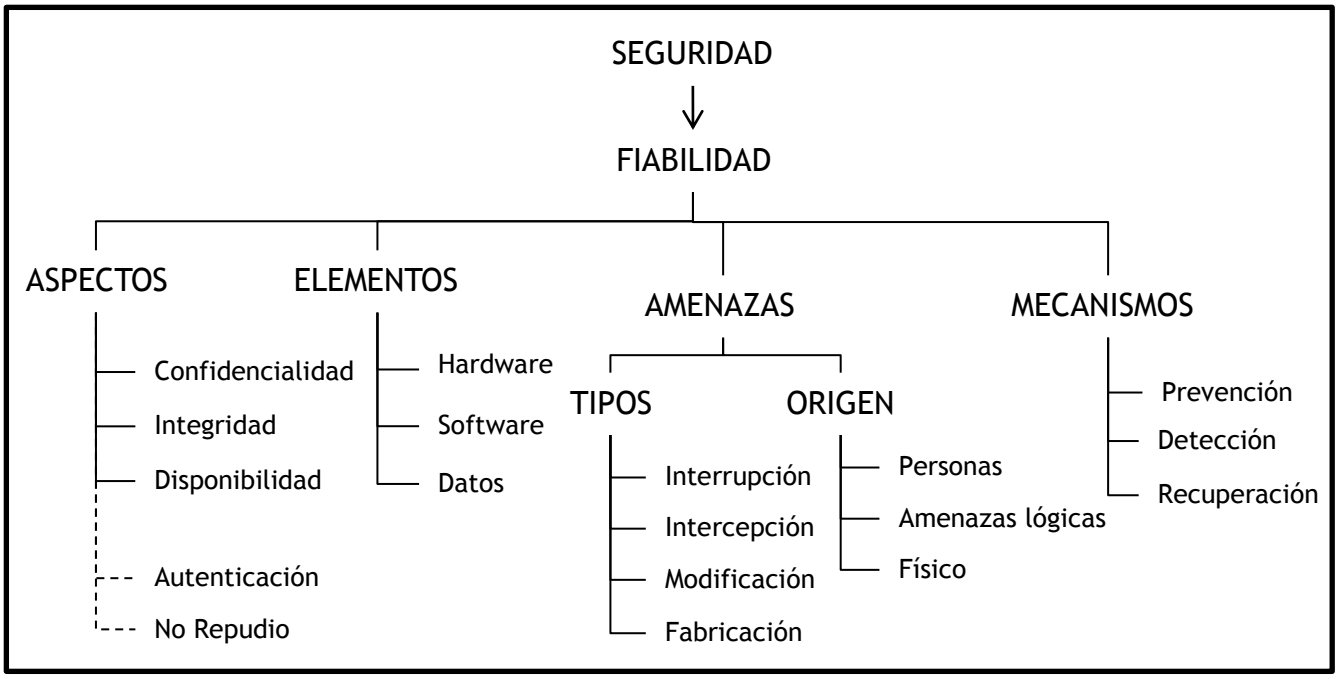


Ilustración 3. Esquema de conceptos de seguridad

4.3.1 Recursos a proteger

La determinación de los recursos que se debe proteger no está estandarizada; esta depende de cada organización y de los productos o servicios a los que la misma se dedique.

Generalizando, los recursos que deben ser protegidos se pueden dividir en:

- Hardware, que es el conjunto formado por todos los elementos físicos de un sistema, entre los cuales están los medios de procesamiento y almacenamiento.
- Software, que es el conjunto de programas lógicos que hacen funcional al hardware
- Datos, que es el conjunto de información lógica que maneja el software y el hardware.

Además, se debe tener en cuenta que cuando nos referimos a la seguridad en redes, el bien más preciado que debe protegerse es la "información" que circula por las mismas.

4.3.2 Amenazas

Se define amenaza como un evento que puede causar alteraciones en la información/sistemas de la organización ocasionándole pérdidas materiales, económicas, de información y de prestigio.

Se define impacto como la medición de las consecuencias al materializarse una amenaza.

Se define riesgo como la posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

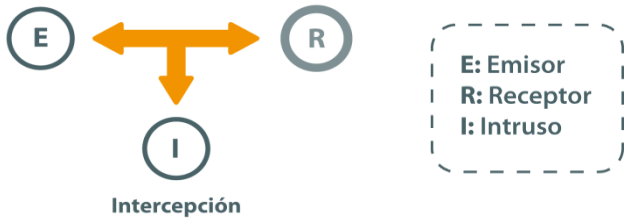
4.3.2.1 Tipos de amenazas

Para los tres elementos a proteger existen cuatro tipos de amenazas:

- ***Interrupción***, cuando un objeto del sistema se pierde, el sistema queda inutilizable o no disponible.

En este caso, no se puede garantizar la ***Disponibilidad*** ya que puede que la recepción no sea correcta.

- ***Interceptación***, cuando un elemento no autorizado consigue acceso a un determinado objeto del sistema.



En este caso, no se puede garantizar la ***Confidencialidad*** ya que es posible que alguien no autorizado acceda a la información.

- ***Modificación***, es cuando se altera algún objeto del sistema, una vez dentro del mismo.

En este caso, no se puede garantizar:

- ***Integridad***: los datos enviados pueden haber sido modificados de manera previa a la recepción de los mismos por parte del destinatario.
- ***Confidencialidad***: alguien no autorizado puede haber accedido a la información.

- ***Fabricación***, es cuando se falsea algún objeto del sistema mediante la creación de otro de aspecto igual al que podría haberse generado pero con un objetivo distinto.

Como en el caso anterior, no se puede garantizar:

- ***Integridad***: los datos enviados pueden haber sido modificados de manera previa a la recepción de los mismos por parte del destinatario.
- ***Confidencialidad***: alguien no autorizado puede haber accedido a la información.

4.3.2.2 Origen

La siguiente es una clasificación básica de amenazas según origen:

- ***Riesgos de origen físico:*** se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. Dentro de este tipo de amenazas encontramos:
  - Los desastres naturales tales como terremotos, tormentas eléctricas, e inundaciones.

- Los desastres del entorno: en esta categoría encontramos el sistema eléctrico, el ruido eléctrico, la humedad e incendios y humo.
- Amenazas hardware, tales como mal diseño, errores de fabricación, daños en discos duros o procesadores, errores de funcionamiento de la memoria,… Todas ellas hacen que la información o no esté accesible o no sea fiable en un momento determinado.

- ***Personas:*** son el factor de riesgo más importante que debe considerarse. Estas pueden o no tener intención, pero su efecto puede llegar a causar enormes pérdidas. El objetivo es buscar puntos débiles o vulnerables del sistema por donde las personas podrían ingresar a él y causar problemas.

  Hay dos tipos de atacantes: los pasivos, son aquellos que entran en el sistema pero no destruyen y los activos, que son aquellos que entran y alteran el sistema. Algunos de los posibles atacantes son:

  - *Personal:* se trata de cualquier empleado de la organización que, por error, desconocimiento o intencionalmente efectúe algún tipo de modificación que pueda ser considerada accidente.
  - *Ex empleados:* capaces de atacar el sistema puesto que lo conocen y saben cuáles son las debilidades del mismo, por dónde pueden ingresar virus, troyanos o demás amenazas lógicas.
  - *Hackers:* tienen como objetivo los entornos de seguridad media para curiosear, para utilizarlas como enlace hacia otras redes, para probar nuevas formas de ataques o por diversión. Suele tratarse de personas con distintos grados de conocimiento.
  - *Crackers:* se trata de cualquier persona que ataca al sistema para causar algún tipo de daño.
  - *Intrusos remunerados:* es el grupo de atacantes más peligroso ya que se trata de piratas informáticos con gran experiencia en problemas de seguridad y un posible amplio conocimiento del sistema, contratados por un tercero para robar secretos o para dañar la imagen de la empresa a la que atacan.

- ***Amenazas lógicas***. La seguridad lógica se refiere a la seguridad en el uso de software, la protección de los datos, procesos y programas. Las amenazas lógicas consisten en conjuntos de programas creados con alguna intención de dañar los sistemas informáticos o con esa capacidad debido a un error de programación. Entre ellos encontramos los siguientes:

  - *Software incorrecto*: se trata de errores cometidos por los programadores en forma involuntaria, los cuales se denominan *bugs*. A los programas que aprovechan estos errores e ingresan en el sistema se los llama *exploits*.
  - *Herramientas de seguridad*: estas son armas de doble filo ya que de la misma forma que el administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar deficiencias y atacar a través de las mismas.
  - *Puertas traseras*: también denominados atajos, son colocados en los programas para tener mayor velocidad en la detección y depuración de fallos durante la etapa de desarrollo de aplicaciones; si, en las versiones definitivas, estos atajos se mantienen pueden proporcionar a cualquier atacante un acceso global a datos a los que no debería poder acceder, suponiendo un grave peligro para la confidencialidad e integridad del sistema.

- *Bombas lógicas*: son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; a partir de ese momento tienen una función que no es la original sino una función dañina (que puede detectarse inmediatamente o con el paso del tiempo).
- *Canales cubiertos*: son canales de comunicación que permiten transferir información violando las políticas de seguridad del sistema.
- *Virus*: es un programa, desarrollado intencionalmente, para instalarse en una computadora sin el consentimiento del administrador. Se trata de un conjunto de instrucciones que alteran el funcionamiento de otros programas o sistemas operativos y también de los archivos (entre otras posibles funciones).
- *Gusanos*: son programas capaces de ejecutarse y propagarse por sí mismos a través de redes, en ocasiones portando virus o aprovechando *bugs* de los sistemas a los que se conectan para dañarlos. Estos tienen la característica de que son muy difíciles de programar, pero pueden causar mucho daño.
- *Caballo de Troya*: son instrucciones escondidas en un programa para que parezca que realizan las tareas que hipotéticamente les corresponderían, pero que, en realidad, ejecutan funciones ocultas sin el conocimiento del usuario u administrador.
- Spyware: son programas espía que recopilan información sobre una persona o una organización sin su conocimiento. Esta información puede ser luego cedida o vendida, por ejemplo, a empresas publicitarias. Pueden llegar a recopilar información del teclado de la víctima pudiendo así conocer contraseñas o nº de cuentas bancarias o pines.
- *Adware*: son programas que abren ventanas emergentes no deseadas mostrando publicidad de productos y servicios.
- *Spoofing*: son técnicas de suplantación de identidad con fines fraudulentos.
- *Phishing*: esta técnica intenta conseguir información confidencial de forma capciosa mediante suplantación de identidad.
- *Spam*: recepción de mensajes no solicitados que puede alcanzar (y en ocasiones tiene como fin último) la saturación del receptor.
- *Programas conejo o bacterias*: son programas cuya función es reproducirse hasta que el número de copias acaba con los recursos del sistema, produciendo una denegación de servicio.
- *Técnicas salami*: se trata del robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad de orígenes, lo cual hace dificultosa su detección.

4.3.3 Grado de protección

El grado de protección ha de estar acorde con la importancia del elemento dentro del funcionamiento del sistema, o sea que el costo no debe superar al del reemplazo o recuperación del elemento o disminuir a valores inaceptables la operatividad del elemento que se protege.

4.3.4 Mecanismos de protección

Para proteger el sistema hay que realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas o problemas legales que estas podrían generar de materializarse, y la probabilidad de su ocurrencia (análisis de riesgos); a partir de ese momento se comienza a diseñar ***una política de seguridad*** que defina responsabilidades y reglas que deben seguirse para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A los mecanismos utilizados para implementarla se les llama mecanismos de seguridad, los cuales son la parte más visible del sistema de seguridad, y se convierten en la herramienta básica para garantizar la protección de los subsistemas o de la propia red.

Esquemáticamente:

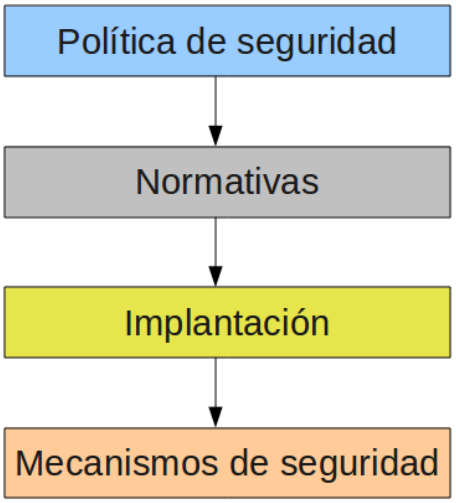


Ilustración 4. Jerarquía de seguridad

Hay tres tipos de mecanismos de seguridad:

- ***De prevención:*** son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo los acosos a la seguridad.
- ***De detección:*** son aquellos que se utilizan para detectar violaciones de seguridad o intentos de ello.
- ***De recuperación/correctivo:*** son aquellos que requieren que el objeto de evaluación reaccione en respuesta a cualquier posible anomalía, violación de seguridad o cualquier otro evento indeseable, con el objeto de preservar o regresar a un estado de seguridad o limitar cualquier posible daño.

4.3.4.1 Medidas preventivas

4.3.4.1.1 Restringir el acceso lógico entre redes

Uno de los principales focos de riesgo es la tendencia actual de interconexión entre redes. Por ello, es aconsejable controlar estas conexiones para que únicamente se lleven a cabo las realmente necesarias.

Para la aplicación de esta restricción se deberá implementar una arquitectura de red segura que incluya, al menos, los siguientes aspectos:

- ***Segmentación de redes***. No todos los usuarios tienen las mismas necesidades, ni todos los servicios los mismos requerimientos. Por ello, se recomienda realizar una segmentación de la red, de modo que cada subred tenga un propósito específico y ofrezca acceso controlado únicamente a aquellos usuarios que lo requieran. Además de incrementar la seguridad, la segmentación permite una gestión más eficiente de los recursos.
- ***Generación de DMZs***. Es un caso particular del apartado anterior. El objetivo y la finalidad de las DMZs consiste en ubicar en una red semi-confiable aquellos servicios y equipos que requieran visibilidad hacia otra red diferente y, que además necesiten conectividad con la red confiable.
- ***Instalación de elementos de seguridad***. Para completar la segmentación de red, es necesaria la instalación y configuración de elementos de seguridad, como pueden ser firewalls, IDS, routers con ACLs, IPS, correladores de eventos, etc… La elección de unos dispositivos u otros dependerá del alcance y la criticidad de la red que debe protegerse, aunque elementos como firewalls son imprescindibles en una red como la que se prevé en el sistema de tren interurbano México - Toluca. Algunos ejemplos de elementos de seguridad serían:
    - ***Firewalls***. Permite habilitar única y exclusivamente las conexiones necesarias, denegando todo el tráfico que no haya sido explícitamente autorizado. Asimismo, el firewall deberá contar con mecanismos de acceso y gestión remota robustos.
    - ***Routers con ACL***. Sirve para establecer listas de control de acceso que limiten en cada interfaz del router las direcciones IP de origen y destino, permitiendo solamente aquellas que sean necesarias y denegando el resto.
    - ***IDS en la red***. Desplegar sondas IDs para que se encarguen de enviar los eventos generados a un correlador de eventos que agregue y analice la información de todas las sondas, generando las correspondientes alarmas de securización.

4.3.4.1.2 Restringir el acceso físico a la red interna y a sus dispositivos

Se deberán establecer los mecanismos de protección físicos que se consideren necesarios, combinándolos con mediadas de protección lógica cuando sea posible.

El estudio de los mecanismos de protección físicos queda fuera del alcance de este documento.

4.3.4.1.3 Redundar componentes con disponibilidad esencial

Como ya se ha comentado, SES priorizará la disponibilidad de los sistemas; por ello, se deben redundar, ya sea física o lógicamente, aquellos componentes que se consideren críticos. El objetivo de esta redundancia es eliminar lo que se denominan puntos únicos (o singulares) de fallo, de modo que la funcionalidad quede garantizada en caso de que ocurra un fallo lógico o físico. Los elementos que se suelen redundar son:

- ***Dispositivos de red***, mediante pares redundados de dispositivos con configuración activo-activo, activo-pasivo o activo-standby. En el plano lógico, se recomienda configurar conexiones redundantes o implementar algoritmos que permitan recalcular caminos en caso de error en algún enlace.
- ***Servicios críticos***. En esta categoría se incluyen los elementos de procesamiento (por ejemplo, servidores).

4.3.4.1.4 Crear equipos multidisciplinares

Es recomendable que los equipos encargados de operar y mantener los sistemas y redes sean multidisciplinares; es decir, que los miembros de los equipos abarquen varios campos de conocimiento. Así se evitará la toma de decisiones en base a premisas incompletas por falta de conocimiento.

4.3.4.1.5 Definir roles y responsabilidades

Los empleados deben tener asignadas única y exclusivamente las funciones y responsabilidades propias de su puesto y, por tanto, contar únicamente con las credenciales de acceso a los sistemas y aplicaciones que les son necesarias.

Aplicando los roles y responsabilidades de forma adecuada, se minimiza la posibilidad de ocurrencia de errores humanos y de ataques internos. De igual manera, se facilita la trazabilidad de las acciones en caso de incidente.

4.3.4.1.6 Desarrollar e implantar adecuadamente políticas y procedimientos

Es necesario desarrollar e implantar un conjunto de políticas y procedimientos que deben seguirse. Este conjunto de documentos debe abarcar todos los aspectos que afectan a la securización de los sistemas.

Más información en el apartado 10.

4.3.4.1.7 Segregar entornos

Se debe valorar la existencia de un entorno de pruebas (preproducción) diferente del de producción donde poder probar los cambios que se deseen realizar en el entorno productivo y detectar posibles malfuncionamientos o errores derivados de su instalación o puesta en marcha.

4.3.4.1.8 Contratación del personal operador

Es recomendable solicitar referencias al personal susceptible de ser contratado y verificar las mismas.

4.3.4.1.9 Asegurar los accesos remotos

En los accesos remotos se recomienda establecer mecanismos de seguridad robustos que eviten accesos no autorizados. Es recomendable implementar, entre otras, las siguientes medidas:

- Cifrar las comunicaciones con algoritmos robustos

- Tunelizar (*tunneling*, ver **¡Error! No se encuentra el origen de la referencia.**) todo el tráfico
- Establecer un mecanismo que garantice que la máquina origen de la conexión cumple los requisitos mínimos de seguridad (antivirus, S.O.,…)
- Configurar un límite de tiempo de inactividad que implique la finalización de sesión

4.3.4.1.10 Utilizar preferentemente enlaces de comunicación físicos

Es recomendable utilizar enlaces de comunicación físicos, por su disponibilidad además de por seguridad lógica.

4.3.4.1.11 Concienciar y formar al personal

Es necesario fomentar una cultura de seguridad entre los usuarios y, paralelamente a esta concienciación, ofrecer periódicamente una serie de cursos de formación sobre seguridad de la información.

4.3.4.1.12 Realizar simulacros de forma periódica

Se recomienda realizar periódicamente simulacros en aspectos relativos a la disponibilidad funcional, violación de integridad, accesos no autorizados,….

4.3.4.1.13 Bastionar aplicaciones, sistemas operativos y equipos

Es decir, antes de realizar el despliegue de una aplicación, sistema operativo o equipo en el entorno de producción se debe configurar y securizar tanto como sea posible sin que se vea afectada su funcionalidad:

- Eliminación o desactivación de servicios innecesarios
- Sustitución de cuentas por defecto por cuentas personales y biunívocas.
- Modificación de la configuración por defecto.
- Activación de mecanismos y controles de seguridad
- Configuración de ejecución de actualizaciones automáticas para controlar su momento de lanzado, su ordenación y agrupamiento, anular las que no sean oportunas, …
- …

4.3.4.1.14 Mantener las firmas de los antivirus actualizadas

Se han de mantener las firmas de los antivirus actualizadas. Antes de cualquier instalación en el entorno de producción, es imprescindible aplicarlo en un entorno de pruebas para detectar posibles conflictos o malfuncionamiento.

4.3.4.1.15 Mantener el software actualizado

Se han de actualizar y aplicar los parches de seguridad críticos e importantes, en un plazo razonable de tiempo, de modo que las deficiencias de seguridad sean corregidas.

Antes de proceder con cualquier instalación en el entorno de producción, es imprescindible aplicarlo en un entorno de pruebas para detectar posibles conflictos o malfuncionamiento.

4.3.4.2 Medidas de detección

4.3.4.2.1 Auditorías periódicas de seguridad

Es recomendable realizar auditorías de seguridad periódicas tanto físicas como técnicas.

- Auditorías técnicas, realizando test de intrusión internos y externos, así como test de vulnerabilidades y análisis de la red. El resultado de éstos, debe ser la generación de un documento que refleje el nivel de seguridad y los planes correctivos.
- Auditorías físicas, realizando inspecciones físicas aleatorias de las instalaciones, comparando la seguridad existente con la prevista en la política de seguridad correspondiente.

4.3.4.2.2 Inventario de sistemas

Generar y mantener actualizado un inventario de equipos y sistemas, en el que para cada activo se recoja la información necesaria (finalidad, criticidad, responsable,…). Este inventario permitirá, entre otras cosas, la detección de equipos o elementos no autorizados.

4.3.4.3 Medidas correctivas

4.3.4.3.1 Plan de Continuidad de Negocio y Plan de Recuperación ante Desastres

Para garantizar la operatividad y disponibilidad de los sistemas, se recomienda definir y aprobar un Plan de Continuidad del Negocio (PCN) y un Plan de Recuperación ante Desastres (PRD).

En caso de incidente, estos planes contienen las pautas a seguir para mantener el funcionamiento el sistema y aplicar las medidas necesarias para volver a la normalidad.

4.3.4.3.2 Realización periódica de copias de seguridad.

Para garantizar la disponibilidad de los sistemas y la red en caso de ocurrir algún incidente relativo a datos, es imprescindible realizar copias de seguridad periódicas; este período dependerá de la criticidad del activo y la frecuencia con la que se realicen cambios sobre el mismo.

Las copias de respaldo disfrutarán de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. Se considerará la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Es recomendable asimismo realizar pruebas periódicas de restauración de copias de seguridad, con el fin de verificar que la información que contienen es íntegra y fiable, y que el proceso no reviste ningún riesgo añadido y es perfectamente asumible por el personal que debe llevarlo a la práctica.

4.4 Política de seguridad

Las políticas de seguridad de subsistemas trasladan los requerimientos de seguridad y fiabilidad de cada subsistema particular a una serie de procedimientos auditables, los cuales permiten salvaguardar la seguridad en su diseño, implementación, y posterior funcionamiento. El alcance de las políticas de seguridad es muy amplio: estas definen qué acciones pueden o no pueden ser realizadas por los diversos elementos físicos (por ejemplo, los operadores) y lógicos (por ejemplo, el subsistema de comunicaciones), los pasos a seguir durante las operaciones de mantenimiento y gestión de incidencias, además de la cadena de mando y las responsabilidades de cada uno de los miembros de la organización con respecto a la securización del subsistema.

La política de seguridad de subsistemas tiene como objetivo establecer las normas y requisitos de seguridad que permitan garantizar la confidencialidad, integridad y disponibilidad de los subsistemas de la empresa.

Los aspectos más importantes a tener en cuenta en la política de seguridad son, entre otros:

- Garantizar la confidencialidad, integridad y disponibilidad de los elementos (dispositivos, programas, herramientas,…) de los subsistemas
- Evaluar los riesgos para, valorando los activos, adecuar las políticas a la realidad de la organización
- Establecer la base para poder diseñar normas y procedimientos referidos a, por ejemplo:
    - Organización de la seguridad
    - Clasificación de datos
    - Seguridad de las personas
    - Seguridad física ambiental (este punto queda fuera del alcance de este documento)
    - Planes de contingencia
    - Prevención y detección de virus
    - Administración de los computadores
- Asignar responsabilidades de gestión de la seguridad
- Cumplir los requisitos legales aplicables en la empresa
- Gestionar las incidencias de seguridad de forma adecuada
- Disponer de un plan de contingencia frente a desastres o discontinuidad en la operación
- Formar a usuarios de las obligaciones y procedimientos con respecto a la seguridad de los sistemas
- Monitorear periódicamente los procedimientos y operaciones de la organización de tal forma que, ante cambios, las políticas puedan actualizarse oportunamente
- Evaluar los resultados de la aplicación de los procedimientos y operaciones de la organización con el objetivo de mejorarlos continuamente

A partir de las políticas se podrá comenzar a desarrollar, primero las normas, y luego los procedimientos de seguridad que serán la guía para la realización de las actividades.

Las políticas de seguridad deben considerar principalmente los siguientes elementos:

Característica	Descripción
Alcance	Alcance de la política incluyendo facilidades, sistemas y personal sobre la cual aplica
Objetivo(s)	Objetivos de la política, descripción clara de los elementos involucrados en su definición
Identificación de roles	Las partes involucradas en la política deben ser claramente identificadas
Responsabilidad	Deberes y responsabilidades de las partes identificadas deben ser definidos
Interacción	Describe la interacción apropiada entre las partes identificadas dentro de la política
Procedimientos	Procedimientos esenciales pueden ser llamados, pero no deben ser explicados en detalle dentro de la política
Relaciones	Identifica las relaciones entre la política, servicios y otras políticas existentes
Mantenimiento	Describe las responsabilidades y guías para el mantenimiento y actualización de la política
Sanciones	Definición de violaciones y sanciones por no cumplir las políticas

Tabla 4. Características de las políticas de seguridad

La política de seguridad es el conjunto de directrices de referencia que definen los objetivos de securización y las medidas que deben implementarse para tener la certeza de alcanzar estos objetivos.

La política de seguridad define un número de reglas, procedimientos y prácticas óptimas que han de asegurar un nivel de securización que esté a la altura de las necesidades de la organización.

Este documento se debe presentar como un proyecto que incluya a todos, desde los usuarios hasta el rango más alto de la jerarquía, para ser aceptado por todos. Una vez redactada la política de seguridad, se deben enviar a los empleados las cláusulas que los impliquen para que la política de seguridad tenga el mayor grado de cumplimiento posible.

Nota: Más información en el apartado 10

4.5 Buenas prácticas

Es un compendio de directrices de securización de sistemas adaptadas a las necesidades particulares de la línea del tren interurbano México-Toluca.

Desde SES se ofrecerá soporte para la resolución de consultas en relación a las buenas prácticas de seguridad.

Nota: Más información en el apartado 11

5 REQUERIMIENTOS FUNCIONALES

El subsistema de Securización suministrará los controles y buenas prácticas necesarias para que los servicios de la línea ferroviaria del tren interurbano México - Toluca puedan operar de forma continua y segura.

El subsistema contará con los mecanismos destinados al control de la actividad de las infraestructuras del sistema con los objetivos de:

- Vigilar el cumplimiento de las políticas de seguridad definidas.

  Las políticas de seguridad son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus subsistemas después de evaluar el valor de sus activos y los riesgos a los que estos están expuestos. También puede referirse al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información.

- Garantizar la seguridad perimetral

  El perímetro está formado, en términos generales, por las máquinas y dispositivos que se sitúan en la frontera de la red, donde ésta interactúa con el exterior, con otras redes. La seguridad perimetral vigila las comunicaciones para evitar accesos no autorizados, salida de datos desde el interior y ataques desde el exterior mediante, por ejemplo:

  - Implementación de mecanismos de seguridad para evitar accesos no autorizados e independizar tráficos de los distintos subsistemas o servicios
  - Aislamientos de usuarios y servicios en redes independientes mediante Zonas Desmilitarizadas (DMZ).

- Asegurar la disponibilidad de las infraestructuras de comunicaciones y uso adecuado de los recursos

Para realizar estos objetivos de una manera óptima SES dispondrá, como mínimo, de las siguientes funcionalidades.

5.1 Requerimientos funcionales de tiempo real

Las capacidades y funcionalidades del subsistema son (debido a su criticidad) aquellas que se enmarcan dentro del entorno de tiempo real. Estas funcionalidades deben poder ser desempeñadas con un tiempo de respuesta lo suficientemente pequeño como para considerarse despreciable.

5.1.1 Servidor de seguridad

Un servidor de seguridad es un mecanismo (hardware y/o software) para controlar el flujo de datos entre dos partes de una red con distintos niveles de confianza. SES dispondrá de un servidor de seguridad con, como mínimo, las siguientes funcionalidades:

- Implantación de normas de control de acceso entre dos o más redes
- Filtrado de las comunicaciones a nivel de:
  - Protocolo utilizado
  - Direcciones IP origen y destino
  - Puertos de origen y destino

    - Aplicación
- Control del flujo de información
- Registro de tráfico denegado

Un servidor de seguridad tiene software especializado para detener intrusiones maliciosas, antivirus, antispyware, antimalware, además de contar con cortafuegos redundantes de diversos niveles y/o capas para evitar ataques.

5.1.2 Plataforma unificada

El subsistema dispondrá de una plataforma unificada que permitirá una gestión sencilla de los parámetros y reglas de seguridad mediante las interfaces de gestión centralizada.

Asimismo permitirá, a los operadores de SES, conocer en tiempo real el estado del todos los subsistemas (en lo que a securización de redes y de la información se refiere) y poder llevar a cabo acciones preventivas o correctivas cuando así se requiera.

Permitirá, del mismo modo, la instalación de nuevos equipos o la configuración de los equipos que ya forman parte del subsistema de SES por parte de usuarios autorizados mediante herramientas software.

Tendrá capacidad para el almacenamiento centralizado o distribuido de todas las tablas y software de los equipos de la red.

Las siguientes funcionalidades también estarán disponibles de manera centralizada:

- Gestión de reglas/versiones de firewall, IPS/IDS y antivirus
- Despliegue de nuevas versiones de firmware y/o software
- Análisis en tiempo real de las alertas de seguridad detectadas

5.1.3 Control de acceso

El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso pueda (o no) acceder a un recurso del sistema para realizar una determinada acción.

En todo control de acceso se requerirá lo siguiente:

- Que todo acceso esté prohibido, salvo concesión expresa (estrategia restrictiva)
- Que la entidad quede identificada singularmente
- Que la utilización de los recursos esté protegida
- Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización
- Que la identidad de la entidad quede suficientemente autenticada
- Que se controle tanto el acceso local como el acceso remoto

Con el cumplimiento de estas medidas se garantizará que nadie accederá a recursos sin autorización.

El subsistema garantizará el acceso a los recursos de información de la red a todos los usuarios, programas, procesos y sistemas autorizados.

El subsistema dispondrá de mecanismos que permitan gestionar, de manera centralizada:

- Usuarios y sus datos de identificación
- Asociar roles, perfiles y políticas de seguridad
- Controlar el acceso a los recursos
- …

Para más información sobre estos puntos, consultar el apartado correspondiente del documento [2].

5.1.4 Control de tráfico

El subsistema permitirá controlar el tráfico generado y recibido mediante el empleo de elementos que recolectan información en tiempo real de los elementos de la red, realizando también un análisis de los datos recogidos para detectar situaciones que están fuera de los parámetros normales de operación.

Con la tecnología de control de tráfico (Firewall, IDS/IPS, …) los operadores de SES podrán bloquear la actividad de red peligrosa y detectar cualquier penetración en la red interna. Esta tecnología permitirá, entre otras:

- Bloquear conexiones entrantes y salientes, según ciertos criterios (puerto, protocolo,…)
- Generar análisis estadísticos del tráfico (flujo de red) en busca de anomalías
- Recolectar tráfico de red sospechoso para análisis posterior
- Detectar y bloquear:
    - Instrucciones salientes
    - Descargas de archivos sospechosos
    - Transmisión de información confidencial

5.1.5 IPS/IDS

Son herramientas utilizadas para detectar y prevenir/bloquear las posibles violaciones a la seguridad; es decir, intrusiones (ataques externos a la organización) a un equipo o a una red y el uso indebido desde dentro de la organización (amenazas internas).

5.1.5.1 IDS

Un IDS (Intrusion Detection System) o Sistema para Detección de Intrusos es una herramienta o sistema de seguridad que monitorea el tráfico en una red y los eventos ocurridos en un determinado subsistema, para así poder identificar los intentos de ataque o amenaza que puedan comprometer la seguridad y la operativa de dicho subsistema. El desempeño de los IDS se basa en la búsqueda y análisis de patrones previamente definidos que implique cualquier tipo de actividad sospechosa o maliciosa sobre una red o host.

No están diseñados para detener un ataque, aunque sí pueden generar ciertos tipos de respuesta ante éstos.

Los IDS aportan a la seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa; incrementan la seguridad del subsistema o red vigilando el tráfico y examinando los paquetes en busca de datos sospechosos que puedan afectar a los distintos elementos.

5.1.5.2 IPS

Un IPS (Intrusion Prevention System) o Sistema de Prevención contra Intrusos se define como un dispositivo que ejerce el control de acceso en una red para proteger a los subsistemas o equipos de posibles ataques. Los IPS cuentan con la capacidad de tomar decisiones de control de acceso basadas en los contenidos del tráfico, como por ejemplo las direcciones IP fuente y destino o los puertos de acceso.

En cuanto a su funcionamiento, un IPS al igual que un IDS, funciona ante la detección de intrusos, pero la diferencia es que el IDS alerta ante la detección de un posible intruso, mientras que un IPS establece e implementa políticas de seguridad para proteger el equipo o la red de un ataque.

Las principales funcionalidades del IPS son:

- Identificación de actividad maliciosa
- Registro de información sobre cualquier actividad maliciosa
- Intento de bloqueo/paro de la actividad maliciosa
- Informe de actividades maliciosas

Los requisitos mínimos que debe cumplir un sistema IPS son:

- Debe ser estable (confiable), sino las aplicaciones pueden no correr correctamente
- No debe impactar negativamente en el rendimiento del sistema
- No debe bloquear actividades o tráfico legítimo (no producirá "falsos positivos").

Durante la marcha en vacío (pruebas SAT y de Producción) se deben activar todas las reglas de bloqueo (IPS) y los primeros meses de la misma servirán para desactivar todas las reglas que causen falsos positivos y/o problemas con la latencia (afinando por tanto el rendimiento y funcionamiento del IPS).

5.1.6 Filtrado de contenido

SES dispondrá de los mecanismos necesarios que filtrarán el contenido inapropiado o inseguro tanto de entrada como de salida del sistema, ya que este suele ser un factor de riesgo de la seguridad de la red y un motivo de consumo innecesario del ancho de banda.

Los sistemas de filtrado analizan el contenido que circula por la red comparándolo con patrones previamente definidos en la búsqueda de virus, spam, o simplemente contenido no recomendable.

Existen muchas tecnologías aplicadas a los filtros, siendo actualmente los más usados en el filtrado de contenidos los de tipo semántico (búsqueda de cadenas de texto) y los de categorías, basadas en listas clasificadas de sitios Web en función de sus propios contenidos; resumiendo, los filtros de contenidos actúan básicamente de dos formas:

- Por palabras clave. Se restringe el acceso a todas las páginas que contengan las palabras que hayamos seleccionado.

- Por listas "negras" o "blancas". Las listas negras son una recopilación de webs de contenido inadecuado que son bloqueadas. Las listas blancas son sitios de internet por los que puede navegar (y solo por esos sitios).

5.1.7 Detección de código malicioso y virus

Código malicioso (Malware) es un término que hace referencia a cualquier conjunto de códigos (software), especialmente sentencias de programación, que tiene un fin malicioso.

Algunos de los tipos de código malicioso más conocidos son los siguientes:

- **Virus**. Tal y como se ha comentado **son programas capaces de crear copias de sí mismos**, de forma que anexan estas copias a otros programas legítimos o en zonas especiales de soportes de almacenamiento, como en el caso de los discos duros. Los virus suelen diseñarse para producir todo tipo de problemas en un ordenador, como volverlo más lento, bloquearlo o impedir el acceso a la información.
- **Gusanos**. Los gusanos son un tipo de código malicioso que **se diseñó originalmente para su propagación a través de redes de comunicaciones**, mediante el uso de servicios como el correo electrónico. En la actualidad, son capaces de propagarse a través de servicios de mensajería instantánea o de redes de intercambio de ficheros (P2P) y su velocidad de propagación es muy alta en comparación con los virus, alcanzando además, zonas geográficas muy amplias. En realidad las técnicas de propagación de los gusanos comienzan a ser usadas por otros tipos de código malicioso.
- **Troyanos**. Son programas diseñados para **acompañar o ser incorporados a programas legítimos**. Su propagación es, a diferencia de los virus o los gusanos, “manual”, en el sentido de que es el usuario el que, mediante la distribución del programa que contiene el troyano facilita su propagación.
- **Spyware**. Son programas destinados a la **recolección de información sobre la actividad de un usuario**. Están diseñados para pasar inadvertidos, de forma que el usuario no perciba ningún tipo de actividad fuera de lo normal. Cuanto más tiempo pasen sin ser detectados, más información serán capaces de recopilar (datos que luego son enviados a servidores o direcciones de correo que los recogen y los usan para todo tipo de fines).
- **Adware**. Son programas diseñados para **mostrar publicidad al usuario**. Suelen ser instalados junto con otros programas legítimos. Estos programas pueden recopilar información sobre la actividad del usuario con objeto de mostrar publicidad dirigida y específica. En general este tipo de aplicaciones son más bien una molestia, pero su instalación puede suponer un peor funcionamiento del ordenador y también, el acceso a sitios y páginas web que pueden contener a su vez código malicioso.

Los códigos maliciosos pueden tener múltiples objetivos, tales como:

- Extenderse por la computadora, otras computadoras en una red o por internet.
- Robar información y claves.
- Eliminar archivos e incluso formatear el disco duro.
- Mostrar publicidad invasiva.

Utilizaremos el término genérico ***virus*** para designar cualquier tipo de código malicioso.

SES proporcionará los mecanismos para detectar y bloquear código malicioso que pudiera afectar a las estaciones de trabajo y servidores de la red.

Las principales características de estos mecanismos de detección serán, como mínimo:

- Precisión y facilidad de uso
- Compatibilidad con los sistemas operativos y aplicaciones principales de cada subsistema de la línea.
- Actualizaciones frecuentes y respuesta rápida a nuevos virus
- Análisis automático o bajo demanda
- Protección en tiempo real
- Alertas de detección al usuario
- Posibilidad de herramientas de reparación de elementos infectados o en cuarentena.

Se requerirá implementar mecanismos de tipo antivirus en todas las estaciones, servidores o equipos de procesado cuyo riesgo al código malicioso se determine como alto en el análisis de riesgos preliminar.

5.1.7.1 Antivirus/Protección frente a código malicioso

Las principales vías de infección suelen ser descargas y navegación en Internet, correos electrónicos, ficheros compartidos, discos duros portátiles y memorias USB.

Las etapas de protección incluyen:

- Prevención, haciendo copias de seguridad del software original y ficheros de datos, empleando una computadora en cuarentena para probar nuevas instalaciones,…
- Detección, con programas de rastreo que deben ser actualizados periódicamente para resultar eficaces.
- Contención, aislando inmediatamente el sistema afectado de la red
- Recuperación, mediante la eliminación del virus en el sistema afectado o bien, eliminando el elemento afectado y sustituyéndolo por su copia de seguridad limpia

El sistema antivirus:

- Proporcionará historial de actualizaciones frecuentes y una respuesta rápida a nuevos virus
- Deberá ser configurable de manera que las actualizaciones de definición de virus se puedan descargar en un sistema central dentro de la organización; el resto de usuarios deberán adquirir sus actualizaciones sólo desde ese host central
- Deberá ser capaz de realizar análisis automáticos o bajo demanda de las máquinas en busca de virus
- Deberá tener la capacidad de integración con aplicaciones que puedan integrar código malicioso, tales como correo electrónico, Web, FTP,…
- Deberá ser capaz de analizar cualquier tipo de archivo

- Deberá informar al usuario cuando se detecte un virus e interrogar al usuario/administrador sobre la acción a realizar (eliminar archivo infectado, eliminar virus del archivo,…)
- Deberá ofrecer una función de reparación de archivos infectados o en cuarentena
- Deberá ser capaz de proporcionar protección en tiempo real, analizando archivos abiertos, descargados o creados
- Deberá ser capaz de proteger el registro de inicio, y los elementos esenciales mediante “escudos”

El subsistema contará con:

- Un servidor antivirus/actualizaciones en el que se almacenarán las últimas versiones de firmas de virus y software del antivirus (así como del SO, aplicaciones varias, etc…)
- Servidor de seguridad con capacidad de antivirus
- Puntos finales: software que actúa sobre cada equipo analizándolo y protegiéndolo.

El sistema antivirus escogido no deberá entorpecer la operación normal del usuario ni ralentizar las operaciones habituales del equipo y permitirá configurar excepciones para evitar posibles falsos positivos e incompatibilidades con otras herramientas de trabajo.

5.2 Requerimientos funcionales de tiempo no real

Se listan a continuación las funcionalidades de SES no pertenecientes al entorno de ejecución en tiempo real del mismo.

5.2.1 Backups y recuperación de datos

SES proporcionará mecanismos que permitan realizar copias de seguridad de datos, programas, configuraciones y sistemas operativos,… planificando su frecuencia, configurando sus características (total, incremental, parcial,…) y su ciclo de vida.

Estos mecanismos facilitarán la recuperación de datos y sistemas en caso de pérdida accidental o intencionada.

SES implementará el sistema de backup de dos modos distintos:

- Almacenaje directo: guardado de datos a corto plazo (por un período de 30 días) con tal de facilitar y agilizar la consulta de datos recientes en el tiempo.
- Almacenaje de respaldo: volcado de datos hacia el lugar de almacenamiento permanente, en el cual estarán disponibles a largo plazo. El sistema de almacenaje de respaldo estará basado en un robot de cintas y opcionalmente con una Storage Area Network (SAN) compartida con el resto de subsistemas que requieran grabación permanente de datos.

Para más información sobre estos puntos, consultar el apartado correspondiente del documento [2].

5.2.2 Gestión de riesgos

El licitante tendrá que desarrollar un análisis de riesgo preliminar del sistema que habrá de ser aceptado por los interesados.

El objeto de este estudio es identificar los riesgos a los que están expuestos los sistemas de información y control, que se prevé formen parte de la infraestructura de la red y que pueden verse afectados por diversas amenazas.

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

En general contiene cuatro fases:

- *Análisis*: Determina los componentes de un sistema que requieren protección, las vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo
- *Clasificación*: Determina si los riesgos encontrados y los riesgos restantes son aceptables
- *Reducción*: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas
- *Control*: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento

Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales que forman el marco operativo del proceso con el propósito de:

- Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo
- Orientar el funcionamiento organizativo y hacerlo tendente a implantar la funcionalidad de SES
- Garantizar comportamiento homogéneo
- Garantizar corrección de conductas o prácticas que nos hacen vulnerables
- Conducir a la coherencia entre lo que pensamos, decimos y hacemos

Una buena Gestión de Riesgos no es una tarea única, sino un proceso dinámico y permanente que tiene que estar integrado en los procesos (cotidianos) de la estructura institucional, que debe incluir a todos (desde los usuarios hasta el rango más alto de la jerarquía) y que requiere su reconocimiento y apoyo.

6 CRITERIOS DE DISEÑO PARTICULARES

El presente capítulo pretende hacer un resumen sobre los criterios de diseño particulares que debe implementar SES para llevar a cabo adecuadamente su finalidad principal: garantizar la Confidencialidad, Integridad y Disponibilidad de los subsistemas, redes y datos que conforman todo el sistema de la línea ferroviaria del tren Interurbano México - Toluca. Nótese que los criterios de diseño generales (compartidos por todos) que complementan este apartado se nombran en el apartado “Criterios de diseño particulares” de la Memoria Ejecutiva del Centro de Control [2].

Para gestionar las funcionalidades propias de las consolas de administración de SES, el Centro de Control contará con entornos virtuales donde se ejecutarán las máquinas virtuales que SES solicite.

Sin embargo, para mayor seguridad se debe dotar al sistema de diferentes modos de operación sobre los elementos monitorizados. Dicho en otras palabras, debe ser posible el control desde distintos emplazamientos con la intención de asegurar el control total de la línea en situaciones degradadas. Para ello se definen dos niveles de operación distintos:

- **Nivel 1 (centralizado)** – control desde uno de los Puestos de Operación de SES del Centro de Control.
- **Nivel 2 (zonal)** – control desde el Puesto de Control Zonal

En ningún caso se permitirá que se esté controlando un elemento desde diferentes niveles al mismo tiempo para evitar solapamientos entre órdenes.

7 ARQUITECTURA DEL SISTEMA

Se presenta en este capítulo la estructura general del sistema, detallando su arquitectura (tanto hardware como software), describiendo asimismo los elementos que lo componen y los criterios de configuración empleados en su diseño.

7.1 Arquitectura Hardware

SES hará uso de la Red de Datos Multiservicio (RED) de la Línea de Tren Interurbano México - Toluca para el intercambio de información entre el Centro de Control Operacional y los elementos de campo.

La arquitectura propuesta para SES se muestra en la figura siguiente:

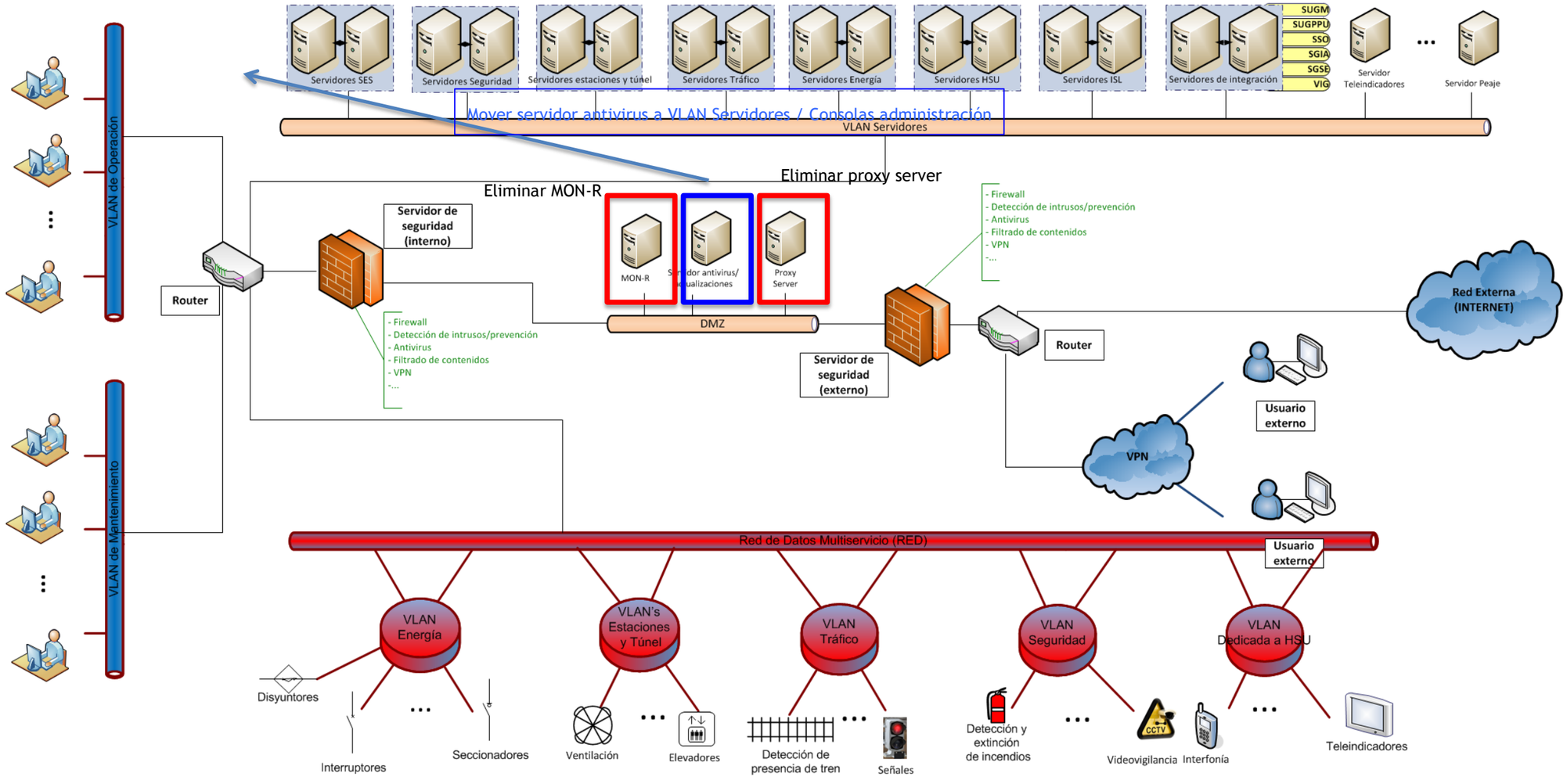


Ilustración 5 Arquitectura SES

Para mantener un buen esquema de seguridad es recomendable el uso de sistemas cortafuegos (firewall) y sistemas de detección/prevención de intrusos (IDS/IPS). Además se debe permitir la cantidad mínima de conexiones iniciadas desde la red interna hacia el exterior y no se debe permitir desde el exterior hacia la red interna propia del centro de control (operadores, servidores, mantenedores,…) a excepción de conexiones VPN, y todas aquellas permitidas deben estar debidamente documentadas y justificadas.

Con las zonas desmilitarizadas, presentes en la figura anterior, se busca mantener a hosts o servidores que pueden ser accedidos por usuarios externos y que puedan acceder a una red externa (Internet) fuera de la red principal (en nuestro caso, VLANs y RED), de tal manera que los equipos que estén ubicados en estas zonas no podrán iniciar la comunicación con ninguno de los equipos que están dentro de la red principal, pero sí habrá flujo de información en sentido contrario, así que lo equipos que se encuentren en las DMZs estarán disponibles para las distintas redes.

Será necesario identificar y gestionar todas aquellas conexiones abiertas entre redes mediantes mecanismos especializados y restrictivos, tales como: firewalls, IDS (Intrusion Detection System), IPS (Intrusion Prevention System), antivirus, protocolos VPN (Virtual Private Network),… Cada uno de estos componentes debe estar bien configurado y distribuido estratégicamente por todo el sistema con el fin de alcanzar una protección fuerte y garantizar una defensa en profundidad.

La solución propuesta incluye la utilización de, como mínimo:

- Servidores de seguridad: firewalls con tecnología UTM/XTM (Gestión Unificada de Amenazas) integrando sistemas cortafuegos, IDS/IPS, gestión VPN, … (ver 7.2.2)
- Sistemas antivirus, instalados en todos los dispositivos críticos que forman parte del sistema (servidores, puestos de trabajo,…) (ver 5.1.7.1)
- Utilización de DMZ, donde inicialmente no se instalará ningún servicio aunque estará disponible para futuras necesidades.
- Matriz de discos NAS, para ampliaciones de memoria

7.2 Elementos del sistema

Se realiza a continuación una descripción de los elementos mostrados en el capítulo “Arquitectura Hardware” (ver 7.1), que define el diseño de SES.

La descripción se centra en el equipamiento particular de este subsistema que se prevé para el correcto funcionamiento del mismo, tal y como se describe en este documento. Para aquellos elementos que pertenezcan a la parte del Centro de Control y sean destinados a su utilización de forma común con el resto de subsistemas y telemandos, la descripción se realiza de forma detallada en la Memoria Ejecutiva del Centro de Control [2].

7.2.1 Equipamiento en el Centro de Control

Parte del equipamiento asociado a SES que deberá ser incluido en el Centro de Control se encuentra debidamente detallada en la Memoria Ejecutiva del Centro de Control [2]; como ejemplo de este equipamiento:

- Clúster de dos servidores de datos configurados con balanceo de carga

- Servidor de actualizaciones (aplicaciones, antivirus, S.O., etc …)
- 4 Puestos de Operación de Seguridad (será desde este puesto de operación desde donde se supervise el subsistema SES), presentando cada uno de ellos el siguiente nivel de equipamiento (en lo que exclusivamente a SES se refiere):
    - 1 Terminal de Trabajo para la ejecución de la parte cliente de la aplicación de supervisión nativa de SES
    - 1 pantalla para la visualización de la aplicación nativa de Securización de Subsistemas
- Etc…

Para más información sobre estos puntos, consultar el apartado correspondiente del documento [2].

7.2.2 Servidor de seguridad

En fase de diseño se determinarán los puntos donde se deben ubicar los servidores de seguridad (firewalls con tecnología UTM-XTM [Gestión Unificada de Amenazas]) y su arquitectura específica. Los equipos se tendrán que adaptar a las interfaces de red existentes en los puntos de instalación escogidos.

Estos servidores de seguridad integrarán funciones de seguridad en un único dispositivo, combinando, como mínimo:

- Firewall
- Protocolo de capa de conexión segura de VPN (Virtual Private Network)
- Sistema de prevención/detección de intrusiones (IPS/IDS)

Estos servidores de seguridad deberán garantizar las siguientes funciones básicas, como mínimo:

- Prevención y detección de intrusiones en la red centrada en el bloqueo de ataques contra PC y servidores
- Detección y bloqueo de antivirus y antimalware
- Filtrado de contenidos
- Filtrado de paquetes (a nivel de protocolo, origen, destino y aplicación)
- Funciones habituales de firewall (cortafuegos)
- Acceso remoto con soporte VPN
- Realización de tareas NAT/PAT
- Soporte de características MPLS
- Alta disponibilidad

Algunas de las prestaciones que brindará la utilización de firewalls serán:

- Prevenir al acceso a la red interna de usuarios no autorizados

- Acceso transparente hacia el exterior de usuarios habilitados
- Transferencia de datos privados de forma segura por la red pública
- Proveer de un sistema de alarmas advirtiendo de intentos de intromisión en la red interna

Los equipos empleados proporcionarán una baja latencia1 así como una redundancia de camino ante la caída de cualquier elemento.

La capacidad máxima será suficiente para transportar y distribuir toda la información con origen y/o destino a los dispositivos con los que está interconectado, dimensionándose con capacidad sobrante (con un margen mínimo al alza sin necesidad de ampliaciones hardware, firmware o software).

7.2.3 Redes privadas virtuales

Una red privada virtual (VPN, Virtual Private Network) consiste en un conjunto de sistemas o dispositivos interconectados a través de canales seguros, sobre una red pública, permitiendo el acceso remoto de los recursos y servicios de la red de forma transparente y segura como si los usuarios estuvieran conectados a la red de forma local.

El sistema SES permitirá la creación de redes VPN mediante conexiones VPN extremo a extremo.

Estas VPN proporcionarán el máximo nivel de seguridad posible a través de IPsec (Seguridad IP cifrada) o túneles VPN Secure Sockets Layer (SSL) y tecnologías de autenticación. Estas tecnologías protegen los datos que pasan por la red privada virtual contra accesos no autorizados.

Las conexiones VPN garantizan la confidencialidad y la integridad de la información que por ellas se transmita y proporcionan comunicaciones seguras con derechos de acceso adaptados a usuarios individuales.

Una solución VPN debe ofrecer los siguientes requerimientos:

- Autenticación de usuarios
- Control de acceso
- Administración de direcciones
- Cifrado de datos
- Administración de claves
- Soporte a protocolos múltiples
- Ancho de banda reservado

[1] ***Nota**: Latencia es la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.*

7.2.3.1 Autenticación de usuarios

La autenticación es uno de los requerimientos más importantes en una VPN. Cada entidad participante en una VPN debe identificarse a sí misma ante otros y viceversa. La autenticación es el proceso que permite a los diversos integrantes de la VPN verificar las identidades de todos.

Existen muchos mecanismos de autenticación pero el más popular de todos ellos es la Infraestructura de Claves Públicas (PKI, Public Key Infraestructure), el cual es un sistema basado en la autenticación por medio de certificados.

7.2.3.2 Control de acceso

El control de acceso en una red está definido como el conjunto de políticas y técnicas que rigen el acceso a los recursos privados de una red por parte de usuarios autorizados. Una vez que un usuario ha sido autenticado, se debe definir a qué recursos de la red puede tener acceso dicho usuario. Los diferentes tipos de VPN, ya sea de firewalls, sistemas operativos, etc; son responsables de gestionar el estado de la conexión del usuario. La VPN debe administrar el inicio de una sesión, permitir el acceso a ciertos recursos, continuar una sesión, impedir el acceso de recursos y terminar una sesión.

El conjunto de reglas y acciones que definen el control de acceso se denomina políticas de control de acceso.

7.2.3.3 Administración de direcciones

Un servidor VPN debe asignar una dirección IP al cliente VPN y asegurarse de que dicha dirección permanezca privada. Las direcciones deben ser protegidas con fuertes mecanismos de seguridad, esto es, deben usarse técnicas que permitan la ocultación de la dirección privada dentro de una red pública.

La tecnología más utilizada para ocultar la información es el tunneling. El tunneling es una técnica que encapsula los datos (incluyendo la dirección destino privada) dentro de otro conjunto de datos. Así, el contenido de los paquetes encapsulados se vuelve invisible para una red pública.

Un ejemplo de protocolo tunelizado es MPLS, donde se hace uso de un sistema de etiquetas para transmitir información. MPLS es una tecnología que proporciona mejoras significativas en los métodos de enrutamiento y en la creación de “túneles”.

7.2.3.4 Cifrado de datos

Cifrar o encriptar los datos es una tarea esencial de una VPN. Aunque se puedan encapsular los datos dentro de un túnel, estos todavía pueden ser leídos si no se implementan fuertes mecanismos de cifrado de la información. Antes de enviar la información, el servidor VPN cifra la información convirtiéndolo en texto cifrado. El receptor de la información descifra la información y la convierte en texto nativo.

7.2.3.5 Administración de claves

En una VPN, es importante la administración de claves. Para asegurar la integridad de una clave pública, ésta es publicada junto con un certificado. Un certificado es una estructura de datos firmada digitalmente por una organización conocida como autoridad de certificación (CA) en la cual todos confían. Una CA firma su certificado

con su clave privada. Un usuario que utiliza la clave pública de la CA podrá comprobar que el certificado pertenece a dicha CA y por lo tanto, la clave pública es válida y confiable.

7.2.3.6 Soporte a protocolos múltiples

Para que una solución VPN sea viable, es necesario también que ésta pueda ofrecer soporte a múltiples protocolos.

7.2.4 VLAN

Una VLAN (Red de Área Local Virtual) es una agrupación lógica de dispositivos o servicios de red, en base a funciones, equipos de trabajo, aplicaciones,…, sin considerar la localización física o conexiones de red.

La función de las VLAN's es una segmentación lógica de la red en diferentes dominios de broadcast; es decir, los paquetes de información son solamente conmutados entre puertos que han sido asignados a la misma VLAN.

Las VLAN's proveen flexibilidad, escalabilidad, seguridad, facilidad de administración y mejor desempeño de la red:

- Incrementan el desempeño de la red agrupando estaciones de trabajo, recursos y/o servidores, según su función, sin importar si ellos se encuentran en el mismo segmento físico LAN.
- Facilidad de administración de adición, movimiento y cambio de recursos en la red (flexibilidad, escalabilidad)
- Mejoran la seguridad de la red, porque solamente las estaciones de trabajo que pertenezcan a la misma VLAN podrán comunicarse directamente.
- Facilitan el control de flujo de tráfico, porque permiten controlar la cantidad y tamaño de los dominios de broadcast, debido a que éstos, por defecto, son filtrados desde todos los puertos que no son miembros de la misma VLAN.

7.2.5 DMZ

Una zona desmilitarizada (DMZ, Demilitarized Zone) es una pequeña red que se sitúa entre la red interna (LAN) de la organización y la red externa o Internet, la cual ofrece fiabilidad en el intercambio de la información y permite reducir los efectos de ataques maliciosos en la red interna.

DMZ proporciona un nivel de protección adicional en la red de datos.

El objetivo de una DMZ es controlar los accesos que provienen del exterior de la red hacia el interior de la red de la organización y proteger la confidencialidad de los datos manejados a través de esta; las conexiones desde la red interna (VLANs) y la externa a la DMZ están permitidas, mientras que, en general, las conexiones iniciadas desde la DMZ solo se permitan hacia la red externa. Los equipos en la DMZ no pueden iniciar comunicación con la red interna.

En la DMZ, los servidores de acceso público (con conexión a internet) se colocan en un segmento separado, aislado de la red interna.

El firewall es relevante en la implementación de DMZ, ya que es responsable de garantizar que las políticas adecuadas para proteger a las redes locales de la DMZ se encuentren habilitadas, mientras que se mantiene la accesibilidad a la zona desmilitarizada (DMZ).

La arquitectura propuesta incluye dos servidores de seguridad (firewalls UTM/XTM) en alta disponibilidad. La comunicación entre los servidores de la DMZ y las máquinas que se encuentran en la empresa sólo tiene lugar bajo condiciones estrictamente controladas.

8 MODOS DE OPERACIÓN

SES permitirá los modos de operación centralizado y zonal. La naturaleza y características generales de estos modos de operación se describen en el capítulo correspondiente de la Memoria Ejecutiva del Centro de Control [2] . El presente capítulo concretiza las funciones que cada uno de los modos permitirá desempeñar en SES.

8.1 Centralizado

En el modo centralizado, el operador de SES situado en la sala de operación del CCP tendrá el control de los dispositivos supervisados por SES. El control centralizado es el modo habitual de operación sobre dichos dispositivos.

En caso de que un dispositivo se encuentre bajo el modo de operación zonal, los operadores de SES no tendrán control sobre él y deberán realizar una solicitud de toma de mando, esperando a que el personal de la Línea que se encuentra gobernando el dispositivo desde el Puesto de Control Zonal correspondiente lo devuelva al modo centralizado.

En el modo de control centralizado, el conjunto de operaciones que es posible realizar incluyen las siguientes:

- Supervisión y visualización instantánea en tiempo real del estado de los subsistemas (en términos de securización de los mismos)
- Realización de acciones preventivas y correctivas
- Envío de órdenes al conjunto de elementos de SES
- Etc…

8.2 Zonal

Los Puestos de Control Zonales (PCZ) ubicados en la Línea tendrán sobre los dispositivos de SES las mismas capacidades y atribuciones que el operador de SES situado en la sala de operaciones del CCP.

En caso de producirse una interrupción en las operaciones de la Sala de Operación del CCP, el PCZ tendrá tanto software de control como de supervisión, pudiendo continuar operando con total normalidad el subsistema de SES.

9 INTERFACES DEL SISTEMA

El subsistema de Securización, por su naturaleza dispone de un amplio número de interfaces con el resto de subsistemas que conforman la línea ferroviaria del tren interurbano México-Toluca. Estas interfaces deberán ser resueltas de forma satisfactoria independientemente de los adjudicatarios de los diferentes contratos.

SES garantizará la confidencialidad, integridad y disponibilidad de la información en tiempo real transmitida por/para cada uno de los subsistemas que forman parte de la línea ferroviaria del tren interurbano México-Toluca sobre la red de datos multiservicio y su recepción segura en los puestos de trabajo destinados a este subsistema.

La información a intercambiar entre SES y los diferentes subsistemas con el fin de cumplir este requisito será confirmada por el contratista del sistema en la fase de obra, esto es, los interfaces declarados en la siguiente lista (propuesta de proyecto que deberá ser evaluada y ampliada según nuevas necesidades detectadas) serán definidos técnicamente por el adjudicatario quien los someterá a aprobación por parte del responsable facultativo de la obra, proceso tras el cual dicho contratista adjudicatario procederá a su resolución.

En la siguiente lista se presenta el conjunto de interfaces identificadas:

- Interfaces Securización con Energía, como mínimo:
    - Alta y Media Tensión (AMT)
    - Tracción (TRA)
    - Subestación de Alumbrado y Fuerza (SAF)

- Interfaces Securización con Electromecánicas, como mínimo:
    - Elevadores (ELV)
    - Escaleras (ESC)
    - Instalaciones Hidráulicas (INH)
    - Instalaciones Sanitarias (INS)
    - Protección contra Incendios (PCI)
    - Ventilación (VEN)
    - Clima (CLI)

- Interfaces Securización con Señalización, como mínimo:
    - Señalización (SEN)
    - Control Automático del Tren (ATC)
    - Detección Auxiliar (DAU)

- Interfaces Securización con Material Rodante, como mínimo:
    - Material Rodante (ROD)

- Interfaces Securización con Telecomunicaciones, como mínimo:
    - Radiocomunicaciones (RAD)
    - Radiocomunicaciones de Banda Ancha (RBA)
    - Videovigilancia (VID)
    - Telefonía (TEL)
    - Grabación de Audio (REC)
    - Interfonía (INF)
    - Sonorización y Voceo (SON)
    - Teleindicadores (TLI)
    - Red de Datos Multiservicios (RED)
    - Red de Nivel Físico (FIS)
    - Cronometría (CRO)
    - Bitácora y Gestor Maestro (BIT)
    - Peaje (PJE)
    - Control de Accesos (ACC)

- Interfaces Securización con Centro de Control, como mínimo:
    - Equipos Comunes (CTR)
    - Telemando de Tráfico (TTR)
    - Telemando de Estaciones y Túnel (TES)
    - Telemando de Energía (TEN)
    - Telemando de Seguridad (TSG)
    - Herramientas de Servicio al Usuario (HSU)
    - Integración Subsistemas de la Línea (ISL)

10 POLÍTICAS DE SEGURIDAD Y PROCEDIMIENTOS

Se deberá generar, como mínimo, las siguientes políticas/procedimientos (con el propósito de incrementar el nivel de disponibilidad, confidencialidad e integridad de los sistemas y administrar los riesgos asociados):

- Política de seguridad

  Define de manera general los requisitos de seguridad aplicables al entorno operativo.

- Política de seguridad física y ambiental

  Define los requisitos de seguridad física que deben cumplir todos los elementos que forman parte del sistema. También incluye los requisitos ambientales que se deben dar para el correcto mantenimiento de los equipos desplegados.

  Esta política queda fuera del alcance de este documento.

- Procedimientos de gestión de cambios

  Recoge los pasos a seguir a la hora de afrontar cambios en los activos de información, incluyendo la especificación del responsable/ejecutor del cambio y las pruebas de validación realizadas antes de aplicarlo en el entorno productivo.

- Procedimientos de gestión de usuarios

  Establece y define los pasos y requisitos a seguir para la gestión de alta, baja o modificación de usuarios. Debe incluir un responsable autorizador de las acciones descritas y la asignación de permisos/roles a cada usuario en función de sus necesidades operativas.

- Procedimientos de aplicación de parches y firmas

  Establece los requisitos y pasos a seguir para la aplicación de seguridad y firmas de antivirus contemplando al menos los siguientes aspectos: alcance de los sistemas afectados, definición de políticas de actualización de los sistemas, periodicidad y horario de despliegue de parches y firmas, realización de pruebas controladas previas al despliegue y despliegue y aplicación de las firmas y parches de seguridad.

- Procedimiento de gestión de copias de seguridad

  Define, como mínimo, los períodos de realización de las copias de seguridad, almacenamiento físico de los dispositivos que contienen las copias, testeo de las copias, personal responsable y mecanismo de destrucción segura.

- Procedimiento de gestión y administración de activos

  Recoge la gestión y la administración de todos los activos de información que forman parte del sistema. Para cada activo, se deberá incluir al menos: responsable, finalidad y uso y una referencia al análisis de riesgos del activo.

- Procedimiento de control de accesos físicos

  Establece, al menos, los requisitos para conceder acceso físico a las instalaciones, registro de datos del personal, identificación del personal, personal que autoriza el acceso y período temporal de validez de la autorización.

11 BUENAS PRÁCTICAS

El diseño e implementación de un sistema de gestión de la seguridad de una organización está influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados, el tamaño, las características operativas y la estructura de la organización.

La aplicación de buenas prácticas en los esquemas de seguridad de las organizaciones permite responder de una mejor manera frente a los incidentes, ya que se contemplan las mejores experiencias para cada caso.

11.1 Buenas prácticas de seguridad en redes/sistemas

Las buenas prácticas a seguir para garantizar un nivel adecuado en las redes/sistemas son, entre otras:

- Contar con políticas de seguridad basadas en estándares
- Realizar planes de contingencia en caso de incidentes: DRP (Plan de recuperación del negocio), BCP (Plan de continuidad del negocio)
- Dar a conocer la importancia de la seguridad a todos los trabajadores de la organización
- Ejecutar frecuentes auto-evaluaciones de seguridad de la información
- Manejar canales seguros de comunicación
- Cifrar comunicaciones y datos durante el transporte y el almacenamiento
- Hacer un uso adecuado de las contraseñas
- Realizar backups de la información
- Establecer planes de contingencia ante un incidente de seguridad
- Contar con un inventario detallado de los equipos que integran la red
- Proteger las redes a través de diferentes mecanismos
- Delimitar tanto el acceso lógico como físico a los sistemas
- Utilizar firewalls, sistemas detectores de intrusos, antivirus.
- Controlar y regular las cuentas de usuarios
- Evaluar los impactos frente a pérdidas de algún activo
- Asegurar física y lógicamente los equipos que integran la red
- Auditar firewalls, sistemas o cualquier dispositivo que se considere necesario
- Implementar un sistema de gestión de vulnerabilidades para garantizar que éstas sean mínimas.
- Identificar equipos críticos
- Implementar políticas de uso de la red
- Siempre que sea posible, llevar a cabo pruebas de seguridad. Las pruebas deberían poder hacerse en entornos de prueba dedicados.
- Realizar pruebas de estrés y penetración (más información, capítulo 12)

11.1.1 Firewalls

Más detalladamente, respecto a firewalls:

- Implementar firewalls con reglas ajustadas y autoajustables
- Revisar la configuración de los firewalls periódicamente.
- Gestionar, bajo el mismo estricto procedimiento de control de cambios que el resto de los subsistemas tecnológicos, los cambios en los cortafuegos,
- Establecer procesos adecuados de gestión y supervisión de los cortafuegos
- Gestionar los cortafuegos por administradores con la adecuada formación
- Gestionar y supervisar los cortafuegos en régimen 24/7

11.1.2 Acceso remoto

Más detalladamente, respecto a acceso remoto:

- Mantener un histórico de todas las conexiones de acceso remoto y sus tipos
- Implementar mecanismos de autenticación adecuados
- Implementar procesos y mecanismos para habilitar y deshabilitar las conexiones de acceso remoto
- Restringir acceso remoto a máquinas específicas y determinados usuarios y, si es posible, en determinados momentos.
- Revisar periódicamente los terceros que tienen acceso remoto a los sistemas
- Garantizar que los equipos usados para acceso remoto están debidamente protegidos

11.1.3 Antivirus

Más detalladamente, respecto a antivirus:

- Proteger los sistemas con software antivirus en las estaciones de trabajo y los servidores
- Obtener las características de los diferentes subsistemas antes del despliegue del software
- Actualizar periódicamente antivirus y las licencias oportunas.

11.1.4 Securización del sistema

Más detalladamente, respecto a securización de los sistemas:

- Investigar qué puertos están abiertos y qué protocolos y servicios están en uso (por ejemplo, mediante un escaneo de puertos).
- Eliminar o desactivar puertos sin utilizar en los sistemas operativos y las aplicaciones para evitar el uso no autorizado.
- Garantizar que todos los sistemas de seguridad incorporados están habilitados.

- Restringir el uso de los dispositivos extraíbles y, si es posible, no utilizarlos. Cuando sean estrictamente necesarios, aplicar, antes de su uso, procedimientos que garanticen que no contienen malware.

11.1.5 Monitorización de sistemas

Más detalladamente, respecto a monitorización de sistemas:

- Vigilar en tiempo real los sistemas para determinar un comportamiento inusual. Una variedad de parámetros debe estar definida y supervisada en tiempo real y compararse con unos valores base para un funcionamiento normal para proporcionar una indicación de comportamiento no usual.
- Usar sistemas de detección y prevención de intrusiones para proporcionar una visión más detallada de la actividad de la red.

11.1.6 Actualizaciones de seguridad

Más detalladamente, respecto a actualizaciones de seguridad:

- Implementar procedimientos para el despliegue de parches de seguridad y nuevas versiones a los sistemas.
- Tener en cuenta la certificación de los proveedores de estos parches, las pruebas de las actualizaciones antes de su aplicación y un proceso de despliegue que minimice el riesgo de interrupción durante el cambio.

11.1.7 Altas y bajas de usuarios

Más detalladamente, respecto a altas y bajas de usuarios:

- Implementar los procedimientos necesarios para garantizar que los nuevos usuarios reciben las cuentas correspondientes, los niveles de autorización y capacitación en materia de seguridad.
- Implementar los procedimientos para garantizar la recuperación de la información y documentación confidencial, la desactivación de las cuentas y el cambio de contraseñas cuando se dé de baja un usuario o bien cuando los usuarios cambien de roles y responsabilidades

11.1.8 Conexión de dispositivos

Más detalladamente, respecto a conexión de dispositivos externos:

- Establecer un procedimiento para verificar que los productos estén libres de virus y gusanos antes de conectarlos a la red.

11.1.9 Documentación

Más detalladamente, respecto a documentación:

- Documentar un inventario completo de los sistemas y sus componentes.
- Documentar el marco que proporciona la seguridad para los sistemas de control y revisarlo y actualizarlo periódicamente para reflejar las amenazas actuales. Este documento debe incluir detalles de los estudios del riesgo, asunciones hechas, vulnerabilidades conocidas y medidas de protección aplicadas.
- Garantizar que toda la documentación de los sistemas está segura y su acceso está limitado al personal autorizado.

11.2 Respaldo de la información

Dentro de las políticas de seguridad se debe contemplar y recalcar la importancia de realizar respaldos de la información.

A continuación se muestra un listado del tipo de información que debería respaldarse:

- En caso de máquinas virtuales, una copia idéntica de la VM y de los archivos que la conforman
- Bases de datos
    - Estructura e información
- Documentos
    - Texto
    - Audio
    - Video
    - Archivos de configuración
    - Bitácoras
    - Políticas de seguridad
    - Inventario de equipos
- Cuentas de usuarios
    - Archivos
- Cualquier otro tipo de información que se considere importante, como informes de trabajo, facturas,…

Los respaldos deberán estar almacenados en distintos medios que deberán estar seguros físicamente y en caso extremo, cifrados.

El acceso a esta información deberá estar restringido y sólo personal autorizado tendrá los privilegios para realizar dichos respaldos con el fin de evitar fuga de información, pérdida o alteración de la misma.

11.2.1 Copias de seguridad y recuperación

Más detalladamente, respecto a copias de seguridad y recuperación:

- Garantizar que los procedimientos de copia de seguridad y restauración están preparados y son apropiados para las amenazas identificadas
- Revisar y probar periódicamente los procedimientos
- Probar regularmente la integridad de las copias de seguridad a través de una restauración completa.
- Guardar las copias de seguridad tanto localmente como en centros remotos.

11.3 Seguridad en aplicaciones

La seguridad en las aplicaciones deberá cubrir los aspectos principales de la securización: disponibilidad, confidencialidad e integridad.

A la hora de analizar las aplicaciones, se deberán considerar entre otros:

- Distribución libre o comercial
- Tipo de tecnología utilizada
- Compatibilidad
- Soporte

11.4 Seguridad en sistemas operativos

Entre las buenas prácticas de seguridad se recomienda asegurar tanto los sistemas operativos como los distintos elementos que los integran (programas y servicios), manteniéndolos siempre actualizados. Se aconseja preparar políticas de gestión de actualizaciones claras que permitan coordinar y administrar parches de seguridad y actualizaciones.

Así mismo, deberán existir políticas de configuración de los distintos equipos que integran una red con la finalidad de minimizar el riesgo.

11.5 Buenas prácticas en servidores

Las recomendaciones respecto a servidores son, entre otras:

- Tratar de utilizar versiones SW lo más estables posibles
- Reconocimiento de los procesos que están corriendo en el equipo
- Eliminar componentes de software extraños
- Implementar un adecuado control de usuarios y privilegios
- Habilitar la auditoría en el servidor
- Realizar auditorías periódicas de:
    - Intentos de acceso
    - Acceso y permiso a archivos y directorios
    - Cambios no autorizados

- Sistemas más vulnerables a ataques
- Tráfico de red sospechoso o no autorizado

- Identificar puertos válidos según los servicios a proveer por cada servidor

11.5.1 Contraseñas y cuentas

Más detalladamente, respecto a contraseñas y cuentas:

- Aplicar y hacer cumplir una política de contraseñas para todos los sistemas (servidores y estaciones de trabajo) que incluya contraseñas fuertes y tiempos de caducidad.
- Cambiar las contraseñas con frecuencia.
- Revisar periódicamente todos los derechos de acceso y borrado de cuentas viejas
- Cambiar las contraseñas por defecto.
- Evitar las contraseñas no necesarias
- Estudiar la posible implementación de métodos de autenticación más fuertes para funciones críticas.

Esta práctica es extrapolable para el uso de contraseñas y cuentas en los accesos a cualquier aplicación/sistema/equipo.

11.5.2 Infraestructura e instalaciones

Más detalladamente, respecto a infraestructuras e instalaciones:

- Instalar los sistemas utilizando una infraestructura adecuada, como redes redundantes.
- Situar el equipamiento en zonas de ambiente controlado y con condiciones ambientales adecuadas.

12 PRUEBAS DE PENETRACIÓN

Una vez implementado el esquema de seguridad con todos los mecanismos necesarios para implementar la securización, éstos deberán ser sometidos a pruebas de intrusión o penetración (a través de ataques controlados desde dentro o fuera del sistema) haciendo uso de las mismas herramientas que diversos tipos de intruso utilizarían para intentar burlar la seguridad, con la finalidad de hallar vulnerabilidades o encontrar algunas cuestiones que no se hayan tomado en cuenta y poder corregirlas antes de que algún intruso lo haga.

No deberá confundirse una prueba de penetración con un ataque real, puesto que un ataque pone en riesgo información, mientras que una prueba se realizará con la finalidad de reforzar, crear o modificar los mecanismos de seguridad.

Para realizar un proceso de penetración deberá especificarse el ámbito donde se aplicará la prueba y debe incluirse una lista específica de las pruebas a realizar o incluso se debe proporcionar una descripción amplia de los procedimientos a realizar.

También es importante establecer límites, ya que en algunas ocasiones existe información con un alto grado de sensibilidad, la cual, bajo ningún concepto, deberá darse a conocer.

Se debe establecer una planificación y coordinación exacta para realizar la prueba, con la finalidad de evitar confusiones con las personas encargadas de la seguridad.

Una vez concluidas las pruebas se deberá realizar un reporte ejecutivo con los resultados de las pruebas realizadas, además de un reporte técnico donde se incluyan de manera detallada:

- Los resultados ordenados por prioridad
- Riesgos a los que está expuesta la organización
- Requerimientos para disminuir las amenazas
- Recomendaciones y acciones a realizar

Una vez generado el reporte, uno de los pasos finales es evaluar los resultados para mejorar las políticas de seguridad de la organización.

Algunas consideraciones importantes que deben tomarse durante las pruebas de penetración, es la comprensión de las razones o motivos por las que un atacante decidiría irrumpir en el sistema y violar la seguridad, esto es actuar como si se tratase del propio atacante, pensar como un atacante.

Como se mencionó anteriormente, la importancia de las pruebas de penetración reside en que permite revelar vulnerabilidades que pueden ser solucionadas de diferentes maneras, por ejemplo:

- Actualizando el sistema afectado
- Reconfigurando el firewall u otros dispositivos de seguridad
- Modificando los controles de acceso de aplicaciones y sistemas operativos

Aunque se realicen pruebas de penetración para determinar fallas técnicas, también es necesario verificar cuestiones de seguridad física, además de realizar un análisis de las políticas establecidas para determinar si éstas son suficientes para garantizar la seguridad.

13 PLAN DE MEJORA CONTINUA

Para establecer y gestionar un sistema de gestión de la securización se utilizará el ciclo PDCA. El **Ciclo PDCA** constituye una **estrategia de mejora continua** en cuatro pasos:

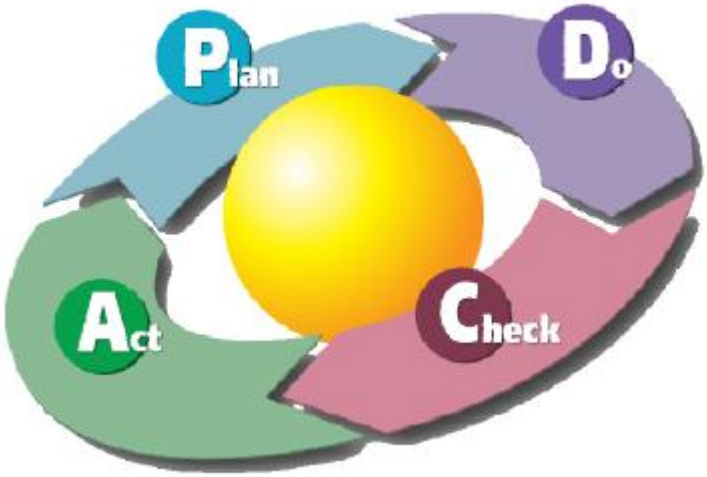


Ilustración 6. Ciclo PDCA

La interpretación de este ciclo es muy sencilla: cuando se busca obtener algo, lo primero que hay que hacer es planificar cómo conseguirlo (Plan), después se procede a realizar las acciones planificadas (Do), a continuación se comprueba qué tal se ha hecho (Check) y finalmente se implementan los cambios pertinentes para no volver a incurrir en los mismos errores (Act). Nuevamente se empieza el ciclo planificando su ejecución pero introduciendo las mejoras provenientes de la experiencia anterior (ciclo de vida continuo).

Adaptando ese ciclo a la gestión de la securización:

- **Plan** (planificar): establecer el sistema de gestión de securización
- **Do** (hacer): implementar y utilizar el sistema de gestión de securización
- **Check** (verificar): monitorizar y revisar el sistema de gestión de securización
- **Act** (actuar): mantener y mejorar el sistema de gestión de securización

Cualquier sistema de gestión exitoso depende del compromiso de todos los niveles y funciones de la organización. Un sistema de gestión permite a una organización desarrollar políticas, establecer objetivos y procesos, y tomar las acciones necesarias para mejorar su rendimiento.

13.1 PLANIFICAR (Plan)

Las principales operaciones que se llevan a cabo en este proceso son:

- Definir el alcance del sistema de gestión en términos de negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una política de seguridad
- Definir una metodología de evaluación del riesgo apropiada para el sistema de gestión y los requisitos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo más importante de esta metodología es que los resultados obtenidos sean comparables y repetibles.
- Identificar los riesgos:
    - Identificar los activos que están dentro del alcance del sistema de gestión de securización y a sus responsables directos
    - Identificar las amenazas en relación a los activos
    - Identificar las vulnerabilidades que pueden ser aprovechadas por dichas amenazas
    - Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos
- Analizar y evaluar los riesgos:
    - Evaluar el impacto de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo
    - Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados
    - Estimar los niveles de riesgo
    - Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado
- Identificar y evaluar las distintas opciones de tratamientos de los riesgos para:
    - Aplicar controles adecuados
    - Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos
    - Evitar el riesgo (por ejemplo, mediante el cese de las actividades que lo originan)
    - Transferir el riesgo a terceros (por ejemplo, compañías aseguradoras o proveedores de outsorcing)
- Seleccionar los objetivos de control y controles para el tratamiento del riesgo que cumplan con los requisitos identificados en el proceso de evaluación del riesgo
- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del sistema de gestión de securización
- Definir una declaración de aplicabilidad que incluya:
    - Los objetivos de control y controles seleccionados y los motivos para su elección
    - Los objetivos de control y controles que, en ese momento, ya están implementados

- Los objetivos de control y controles excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias

En relación a controles de seguridad, existe el estándar ISO 27002 que proporciona una completa guía de implantación que contiene 114 controles, según 35 objetivos de control agrupados en 14 dominios.

13.2 HACER (Do)

Las principales operaciones que se llevan a cabo en este proceso son:

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de securización.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles
- Procurar programas de formación y concienciación en relación a la securización a todo el personal
- Gestionar las operaciones del sistema de gestión
- Gestionar los recursos necesarios asignados al sistema de gestión para el mantenimiento de la seguridad
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad

13.3 VERIFICAR (Check)

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
  - Detectar a tiempo los errores en los resultados generados
  - Identificar brechas e incidentes de seguridad
  - Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad se desarrollan según lo previsto
  - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores
  - Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas
- Revisar regularmente la efectividad del sistema de gestión, atendiendo al cumplimiento de la política y objetivos del mismo, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas
- Medir la efectividad de los controles para verificar que se cumplen todos los requisitos de seguridad

- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados, etc…
- Realizar periódicamente auditorías internas del sistema de gestión en intervalos planificados
- Revisar el sistema de gestión, por parte de la dirección, periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del mismo son evidentes
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del sistema de gestión

13.4 ACTUAR (Act)

La organización deberá regularmente:

- Implantar en el sistema de gestión las mejoras identificadas
- Realizar las acciones preventivas y correctivas adecuadas en relación a las lecciones aprendidas de las experiencias propias y de otras fuentes
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder
- Asegurarse de que las mejoras introducidas alcanzan los objetivos previstos.