PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

GUÍA PARA LA ELABORACIÓN DE PLANES DE SEGURIDAD DEL OPERADOR Y PLANES DE PROTECCIÓN ESPECÍFICA

AGRUPACIÓN EMPRESARIAL INNOVADORA PARA LA SEGURIDAD DE LAS REDES Y LOS SISTEMAS DE INFORMACIÓN

Título: *PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS: Guía para la elaboración de Planes de Seguridad del Operador y Planes de Protección Específica.*

ISBN: 978-84-615-5789-9
Impreso en España. AEI Seguridad.
Edita: AEI Seguridad.
Maqueta y diseño: AEI Seguridad.

Nota: AEI Seguridad no se hace responsable de las opiniones expresadas por los autores en esta obra.

Avda. José Aguado, 41 24005 León – Tel.: 987 87 71 89

info@aeiseguridad.es . www.aeiseguridad.es

INDICE

EQUIPO DE REDACCIÓN DE LA GUÍA

En la elaboración de la *Guía para la elaboración de PSO y PPE* han participado los siguientes profesionales de las distintas entidades que conforman la Agrupación Empresarial Innovadora para la Seguridad de las Redes y los Sistemas de la Información.

Coordinación: Antonio Ramos García (AEI-Seguridad) Félix Antonio Barrio Juárez (INTECO).	
Análisis de riesgos: • Antonio José Vázquez González • María Lourdes Belda Sánchez • Clarisa Lozano González • Eva Allende Barriocanal	
Medidas de seguridad: • Constantino Lázaro de la Osa • María Ángeles Díaz Robles • Anabel Vázquez Iglesias	
Medidas de seguridad: • Patricia Tejado (GMV Soluciones Globales Internet) • Enrique Martín Gómez (GMV Soluciones Globales Internet) • Jairo Montero Santos (GMV Soluciones Globales Internet) • Sergio Nistal Calvo (GMV Soluciones Globales Internet) • Miguel Montero Rodríguez (GMV Soluciones Globales Internet)	

Medidas de seguridad: • Natalia Potes Morante (Instituto Tecnológico de León, S.A.-Grupo Mnemo) • Fernando García Vicent (Instituto Tecnológico de León, S.A.-Grupo Mnemo) • Alejandro Gómez Bermejo (Instituto Tecnológico de León, S.A.-Grupo Mnemo) • Rocio Castrillo Ruiz de Castroviejo (Instituto Tecnológico de León, S.A.-Grupo Mnemo) • Jose Luis Jerez Guerrero (Instituto Tecnológico de León, S.A.-Grupo Mnemo)	
Medidas de seguridad: • Joaquín Ramírez (Tecnosylva) • Guillermo Marqués Rodríguez (Tecnosylva) • Víctor Arrimada de la Parra (Tecnosylva)	
Medidas de seguridad: • Javier García Beveride (Eme Multimedia) • Jesús Miguel Gimeno Pozuelo (Eme Multimedia) • María Eugenia Caballero Mateos (Eme Multimedia) • Oscar Prieto Blanco (Eme Multimedia) • Juan José Garrido González (Eme Multimedia) • Rebeca Blanco Beneítez (Eme Multimedia)	
Medidas de seguridad: • David Abril (B&A Consultores Estratégicos Analyza) • Ángel Fernández (B&A Consultores Estratégicos Analyza)	
Medidas de seguridad física: • Juan Carlos Díez Pérez (INDRA Sistemas) • Sira Zurdo Álvarez (INDRA Sistemas)	

• Fernando Aller Sánchez. (INDRA Sistemas)	
Seguridad en sistemas SCADA: • Susana Gonzalez García de Consuegra (TELVENT Global Services) • Victor Alejandro Luaces Bustabad (TELVENT Global Services) • Juan de las Casas Cámara (TELVENT Global Services)	TELVENT
Contribuciones especiales a la elaboración de la Guía: • Roberto Vidal • Javier García Álvarez • Esther Ortega Moro	XERIDIA
Contribuciones especiales a la elaboración de la Guía: • Koldo Peciña • Ricardo Estremera	S21sec
<u>Edición final y revisión:</u> Félix Antonio Barrio Juárez (INTECO) Luis Hidalgo Gutiérrez (Coordinación AEI Seguridad) Héctor René Suárez (INTECO)	aeiseguridad Agrupación Empresarial Innovadora para la seguridad de las redes y los sistemas de información INTECO Instituto Nacional de Tecnologías de la Comunicación

1. INTRODUCCIÓN

La presente Guía ha sido elaborada por **aeiseguridad** en respuesta a una necesidad de mercado existente dada la reciente publicación de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (en adelante, LPIC).

La LPIC y su desarrollo reglamentario publicado mediante el Real Decreto 704/2011 de 21 de mayo (en adelante, RDPIC) establecen, entre otras, la necesidad de que los que sean designados como operadores críticos elaboren dos documentos:

- Un Plan de Seguridad del Operador (PSO)
- Un Plan de Protección Específico (PPE) para cada una de las infraestructuras que haya sido identificada como crítica por el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)

Estos documentos deben reunir una serie de características, que **aeiseguridad** conoce de primera mano, gracias a su colaboración en el Grupo de trabajo Informal sobre Protección de Infraestructuras Críticas en el que a participado como experto para el desarrollo de las guías que publicará el CNPIC para la redacción de dichos planes.

Dado que las guías que publicará el CNPIC solo incluirán los contenidos mínimos y dado el perfil y conocimientos de los componentes de **aeiseguridad**, la Agrupación ha creído interesante desarrollar esta guía que ahonda en cómo abordar la implantación de las medidas que se deben implantar y más tarde reflejar en dichos Planes.

Por tanto, esta Guía recoge, en base a mejores prácticas nacionales e internacionales un resumen de recomendaciones para implantar las medidas de seguridad identificadas en los PSO y en los PPE que consideramos que será de gran interés para aquellas organizaciones interesados en al protección de las infraestructuras críticas y, en especial de los operadores críticos.

Finalmente, dada la importancia que tienen los sistemas SCADA en este tipo de entornos, se ha incluido un anexo especial dedicado específicamente al aseguramiento de dicho tipo de sistemas.

2. CONTENIDO DE LA GUÍA

Para la confección de este documento se ha recopilado la información de los estándares o normativas más relevantes en cada uno de los temas tratados. Concretamente se han considerado la familia de las normas ISO27000, el Esquema Nacional de Seguridad (ENS) y las guías publicadas por el NIST y el NERC.

- Las ISO27000 porque es el referente de seguridad internacional y son las guías de buenas prácticas en seguridad en las que se apoya el estándar de Seguridad ISO27001
- ENS porque son los requerimientos de seguridad de las administraciones públicas españolas que, hoy por hoy, son un referente y están completamente alineadas con la ISO y particularizadas para los casos de administración electrónica en España.
- NIST porque es la Organización más conocida en elaboración de guías de seguridad específicas para el gobierno de los Estados Unidos, que también está completamente alineada con ISO, con una trayectoria de un gran número de años.
- En el caso del NERC, se han incluido estas guías por estar pensadas específicamente para la protección del sector eléctrico, como infraestructura crítica.

De este modo se consigue tener una visión general de los puntos de seguridad generales a considerar (dados por ISO y NIST), una visión más particular que se está aplicando en las administraciones públicas españolas (dadas por ENS) y finalmente una visión más enfocada en infraestructuras críticas (proporcionada por las guías del NERC).

La Guía cuenta con dos grandes apartados alineados con la estructura de los PSO y PPE:

- Por una parte, todo un capítulo dedicado al análisis de riesgos que es uno de los aspectos principales de los mencionados planes.
- Por otra, dos capítulos dedicados a recoger las medidas de seguridad lógicas y físicas que se deberán implantar en las infraestructuras críticas para mejorar los niveles de protección integrales.

Finalmente, la Guía incluye un anexo dedicado a la securización de los sistemas SCADA, dada su relevancia en este tipo de infraestructuras, así como un apartado en el que se recogen, de manera exhaustiva las referencias utilizadas.

3. ANÁLISIS DE RIESGOS

3.1. OBJETIVOS

El análisis de riesgos no es un fin en sí mismo, sino que forma parte del proceso de gestión de la seguridad, en concreto, de la planificación estratégica para la elaboración y seguimiento del plan de seguridad que las organizaciones deben implantar para proteger las infraestructuras críticas que operan respecto de la amenaza de origen terrorista.

Conocer el tipo de riesgos al que está sometida una organización y en qué medida pueden afectar a las infraestructuras, hace del plan de seguridad una herramienta indispensable en la gestión integral de la seguridad de las organizaciones.

Entendiéndose por seguridad, la capacidad de las infraestructuras (tanto sus elementos físicos como sus redes o sus sistemas de información) para resistir, con un determinado nivel de confianza, las acciones ilícitas o malintencionadas que comprometan el normal funcionamiento de las mismas, y entendiéndose el riesgo como la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a las infraestructuras organizativas, se entenderá por qué el hecho de realizar un buen análisis de riesgos hace que la gestión de los mismos sea eficaz, ya que mediante esta gestión, la organización conoce, previene, impide, reduce o controla los riesgos que conoce.

Una particularidad importante que se ha de tener en cuenta, además, para la realización de estos análisis de riesgos para la protección de las infraestructuras críticas es que deberán tener un enfoque integral de la seguridad, considerando tanto sus elementos lógicos como físicos y las medidas de ambos tipos.

El análisis de riesgos es una herramienta de gestión que permite tomar decisiones: desde decisiones sobre inversión, pasando por las decisiones de adquisición de salvaguardas técnicas o la selección y capacitación del personal.

Llevar a cabo un análisis de riesgos es laborioso. Establecer un mapa de activos y valorarlos requiere la colaboración de muchos perfiles dentro de la Organización. Además, lograr una uniformidad de criterio entre todos es imprescindible ya que, si es importante cuantificar/valorar los riesgos, más importante aún es relativizarlos.

Establecer una metodología para realizar un buen análisis de riesgo no es nada fácil. Precisamente por eso, este es el objetivo del documento: proporcionar pautas para la definición de una metodología de gestión de riesgos válida para cualquier organización que opere infraestructuras críticas, para la identificación y evaluación de sus riesgos, identificar medidas de protección con un enfoque integral de la seguridad y que aporte a la organización el conocimiento, la prevención, la reducción y control de los riesgos.

3.2. DESCRIPCIÓN

Las pautas incluidas en el presente documento parten de la experiencia de la realización de análisis de riesgos e incorpora los enfoques de diferentes métodos existentes (como *Magerit, Mosler u otros métodos cuantitativos mixtos*).

El esquema de la metodología propuesta en el presente documento es el que se representa en la siguiente figura:

Figura 1: Fases de la metodología

Los diferentes elementos del análisis de riesgos se relacionan entre sí normalmente según se ilustra a continuación:

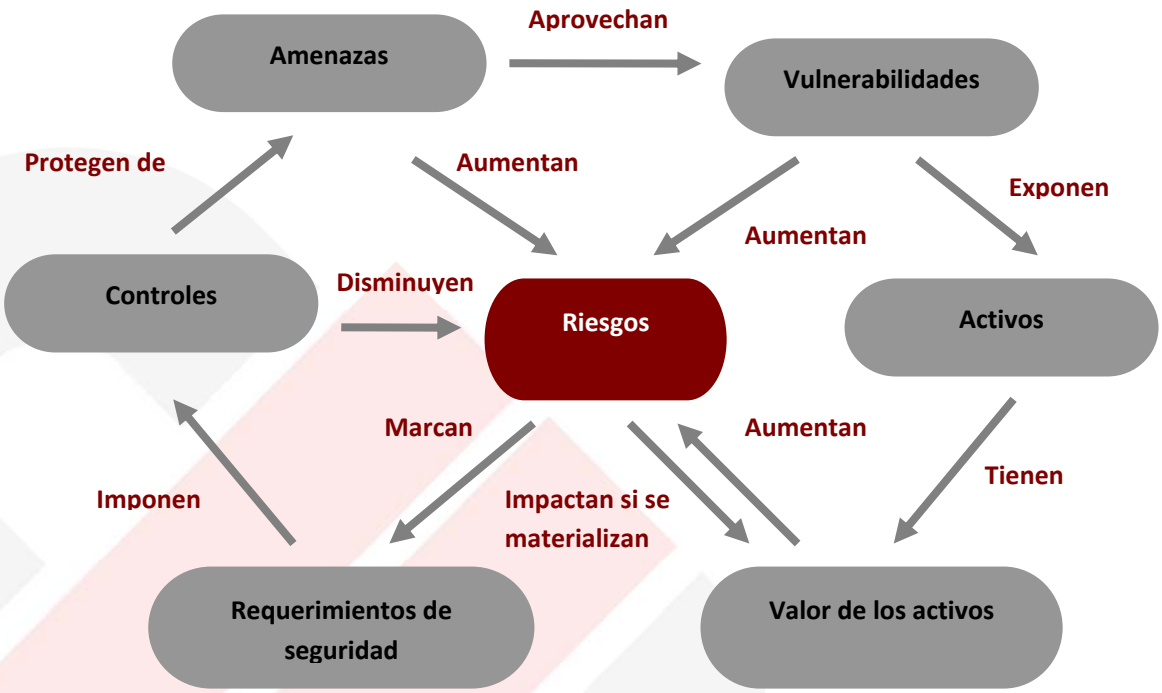

Figura 2: Elementos de un análisis de riesgos

3.3. MEJORES PRÁCTICAS

3.3.1. Fase I: Identificación de activos

El proceso de realizar un inventario de los activos de una organización es uno de los aspectos fundamentales del análisis de riesgos. Teniendo en cuenta que, además, el análisis de riesgos ha de permitir conocer la evaluación de riesgos a distintos niveles de agrupación (organización, servicio esencial e infraestructura crítica concreta, como mínimo), el inventario de activos ha de tenerlo en consideración para permitir, al menos, dichos niveles de agregación.

Se entienden por activos, aquellos recursos necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su Dirección.

Uno de los activos esenciales es la información que maneja el sistema, es decir, los datos. Además, se pueden identificar otros activos como son:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las instalaciones, incluidas las que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.

La *dependencia* entre activos es un concepto que se debe tener en cuenta a la hora de asignar valor a un activo, dado que en sí un activo puede tener un valor pequeño pero puede acumular un valor considerable si se considera el valor de todos los activos que dependen de su correcto funcionamiento (ejemplo típico de un activo de uso compartido: centralita telefónica, router de salida a Internet, servidor de ficheros, etc.).

Se entiende por tanto como dependencia de activos, la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior. Se dice, por tanto, que un "activo superior" depende de otro "activo inferior" cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior.

No todos los activos dentro de una organización son activos críticos de los que se deba gestionar los riesgos a los que están sometidos. La identificación de activos críticos se desarrolla en la fase siguiente (Fase II: Valoración de activos).

3.3.1.1. Etapa I: Identificación de procesos.

El análisis de procesos de cada línea de actividad de una organización es un paso clave para la correcta identificación de activos.

Se trata de realizar un análisis exhaustivo de todos los pasos que se siguen en la organización, teniendo en cuenta la información de un proceso a otro, los canales de información y los recursos para poder canalizar la información.

Ejemplo: Empresa que se dedica a: "Venta, Instalación y Servicio Técnico de telefonía incluida la venta y reparación de tendidos y cableados, montaje de centralitas, venta de equipos informáticos y terminales móviles".

Etapa I: Para esta empresa se identifica un único cliente: cliente al que se le instala un sistema de telefonía, por lo que se identifica una única línea de negocio.

Se representan a continuación mediante diagrama de flujo los procesos de la organización.

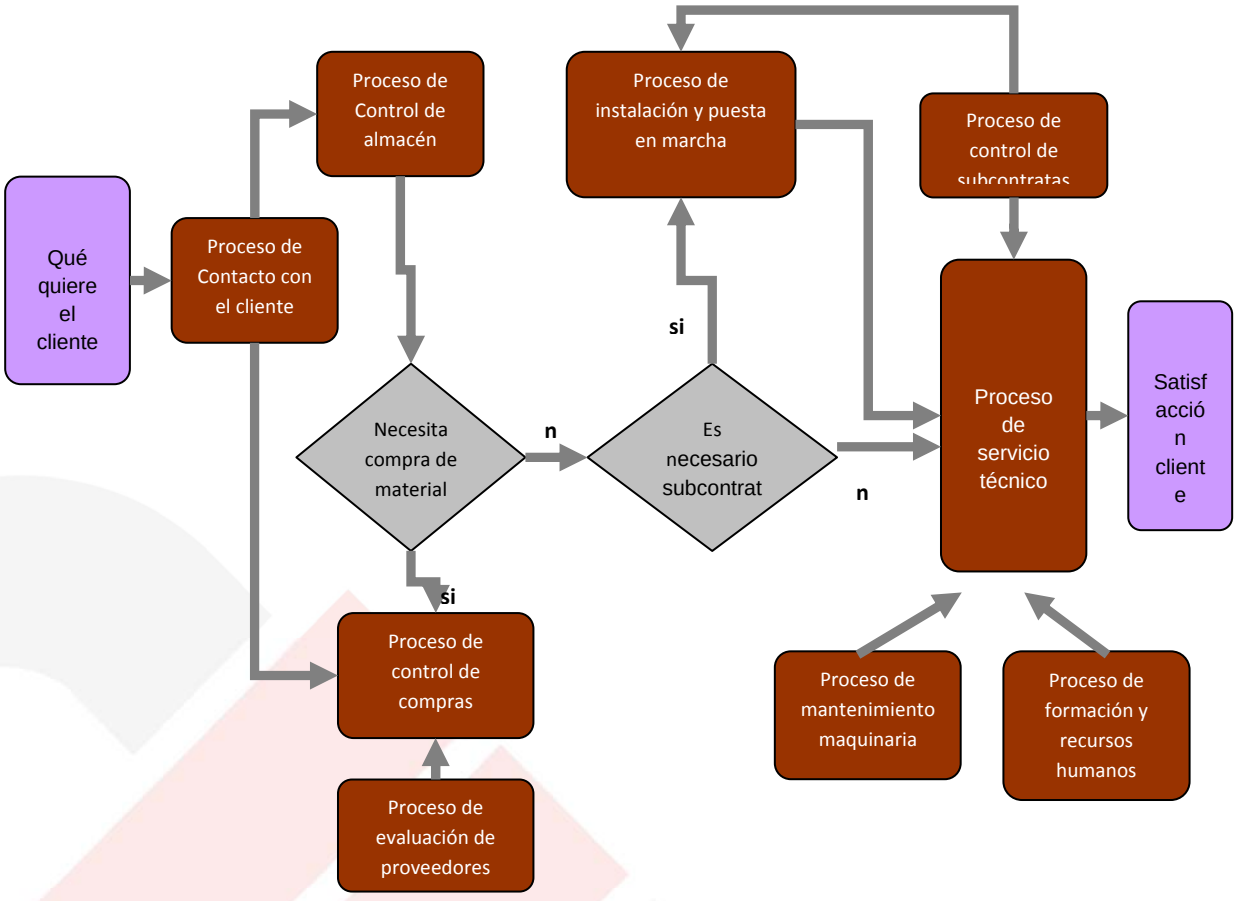

Figura 3: Diagrama de flujo empresa ejemplo

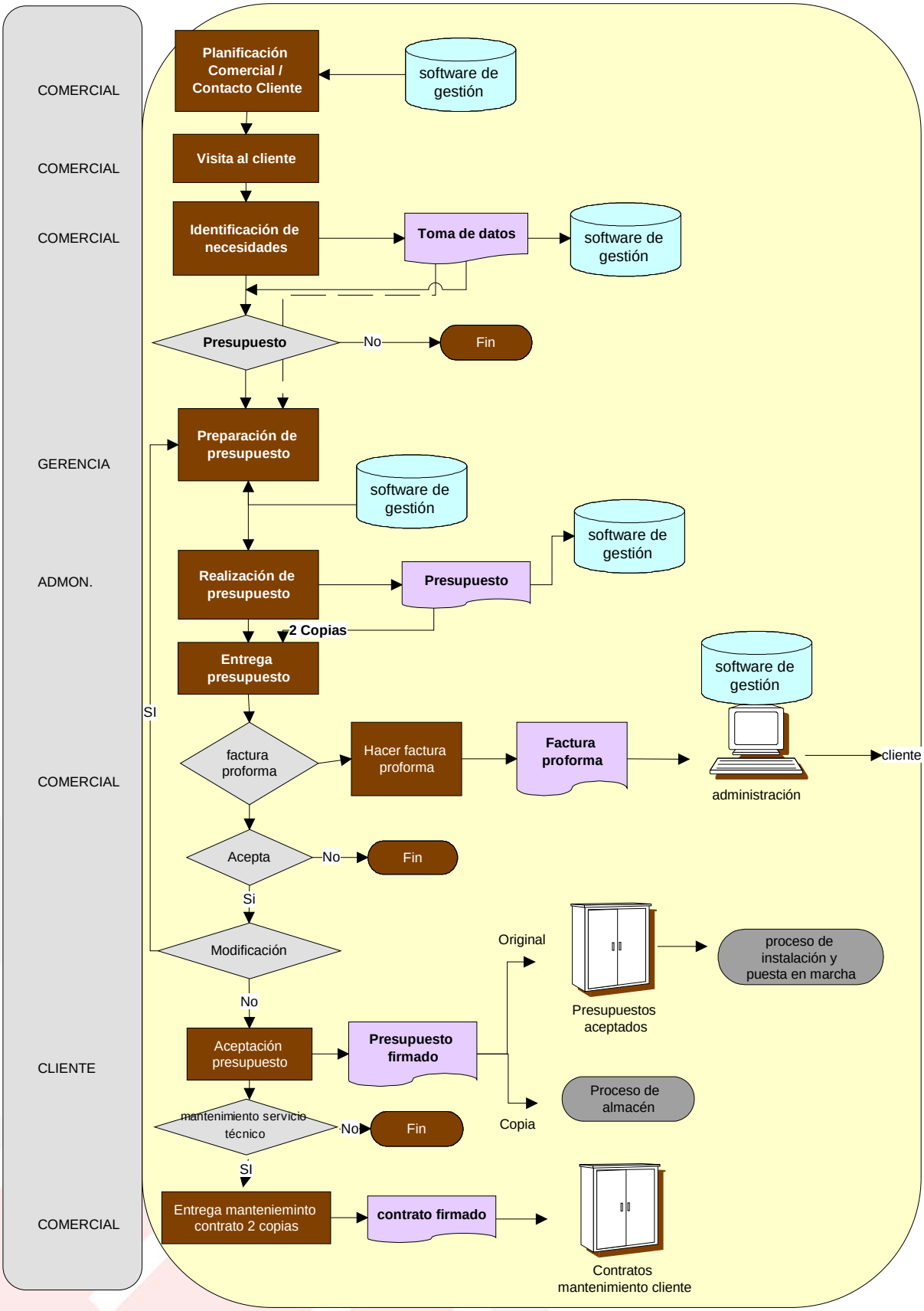

Figura 4: Flujograma proceso contacto con el cliente empresa ejemplo

Se identifica cada uno de los procesos, es decir, los flujos de trabajo.

Así, para el proceso de contacto con el cliente quedan representados en el flujograma que se representa anteriormente (figura 4).

3.3.1.2. Etapa II: Identificación de activos.

La organización deberá hacer una identificación de sus activos. Dicha identificación se hará en base a los diferentes tipos de activos que podrán utilizar las diferentes líneas de actividad de la organización.

Para cada línea de actividad se realizará una identificación de activos.

> *Ejemplo: Así una empresa dedicada a la venta de software específico para el sector sanitario, que dispone de aulas formativas para impartir formación tutorial subvencionada o particular, diferenciará tres tipos de clientes, y tres líneas de negocio diferenciadas:*
>
> *Cliente 1: organizaciones que compran software como son clínicas privadas, hospitales públicos o privados.*
>
> *Cliente 2: organizaciones públicas que subvencionan la actividad formativa.*
>
> *Cliente 3: alumnos particulares que reciben la formación.*
>
> *Para cada tipo de clientes la actividad desarrollada es diferente y los activos críticos que se deben identificar difieren.*

3.3.1.3. Etapa III: Clasificación de activos

Dado el enfoque integral comentado, habría que identificar tanto activos físicos como activos relacionados con el tratamiento de información.

Activos físicos serían, por ejemplo, los emplazamientos de la organización, los edificios, los locales, las equipos móviles o la canalización.

Activos de información son, por ejemplo, ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información.

Figura 5: Tipos de activos de información

Una forma sencilla de identificar activos es la que se realiza teniendo en cuenta la siguiente clasificación:

Datos: Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización.

Aplicaciones: El software que se utiliza para la gestión de la información.

Personal: En esta categoría se encuentra tanto la plantilla propia de la organización, como el personal subcontratado, los clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización.

Servicios: Aquí se consideran tanto los servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo la comercialización de productos).

Tecnología: Los equipos utilizados para gestionar la información y las comunicaciones (servidores, PCs, teléfonos, impresoras, routers, cableado, etc.)

Instalaciones: Lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.).

Equipamiento auxiliar: En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, etc.)

Se identifican los siguientes activos de acuerdo con el flujograma.

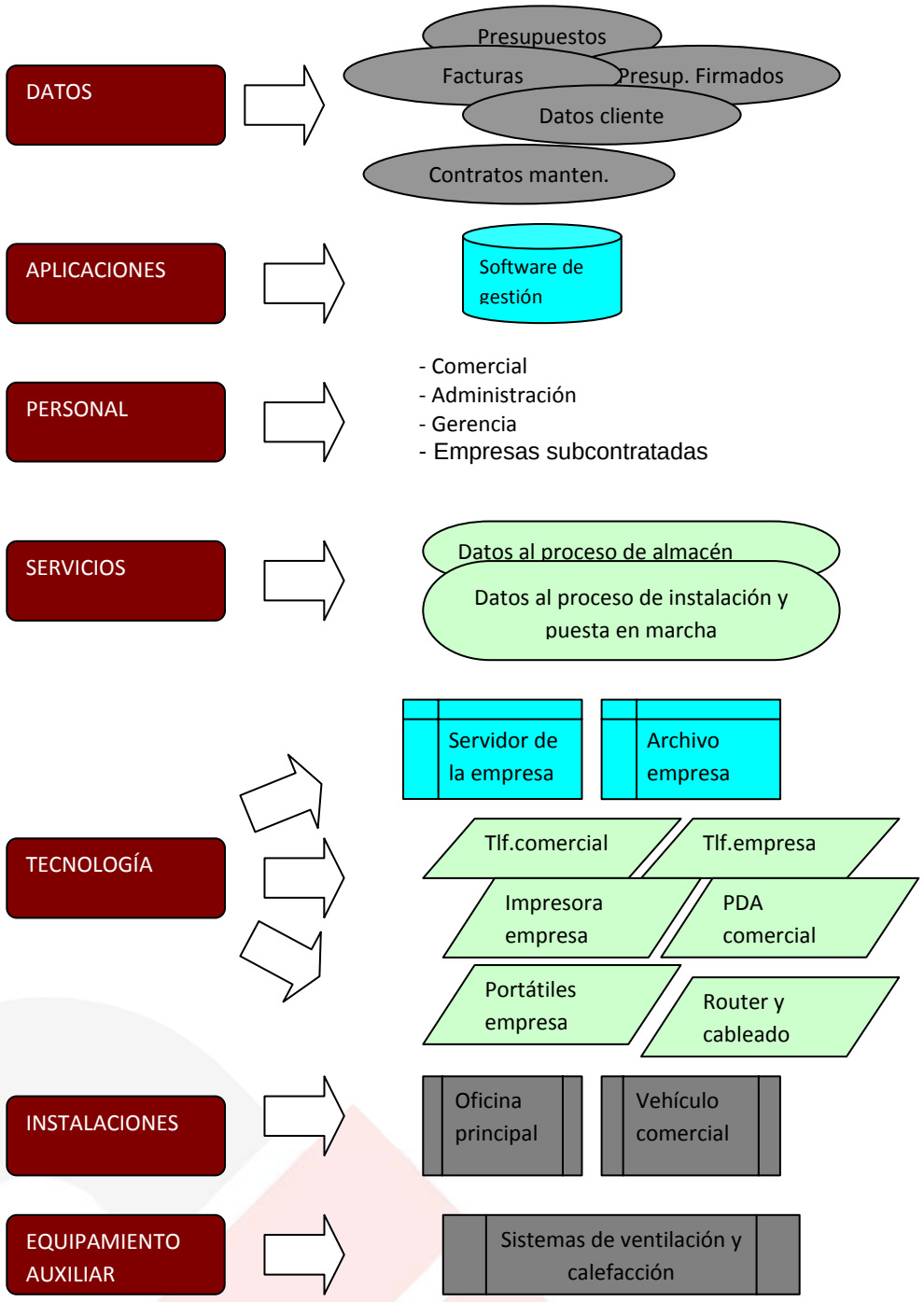

Figura 6: Flujograma de identificación de activos

3.3.2. Fase II: Asignar valor a los activos.

Una vez identificados los activos, el siguiente paso a realizar es valorarlos. Es decir, hay que estimar qué valor tienen para la organización, cual es su importancia para la misma.

Para calcular este valor, se considera cual puede ser el daño que puede suponer para la organización que un activo resulte dañado. Para los activos de infromación, está valoración

suele realizarse en cuanto a sus dimensiones, por ejemplo, su disponibilidad, integridad y confidencialidad. En el caso de los activos físicos se pueden utilizar esquemas de valoración que tomen en consideración factores como su valor material, el efecto sobre los beneficios, pero también el daño en vidas humanas, en daños ambientales o sobre la reputación que podría causar su destrucción, o también las consecuencias legales o sobre la sociedad.

Esta valoración se hará de acuerdo con una escala que puede ser cuantitativa o cualitativa.

Si es posible valorar económicamente los activos, se utiliza una escala cuantitativa. Este seria el caso de activos como el software o el hardware. Se trata de los activos tangibles.

En la mayoría de los casos, no es posible cuantificar un activo con valores monetarios o va a suponer un esfuerzo excesivo, por lo que se utilizan escalas cualitativas como por ejemplo: bajo, medio, alto o bien un rango numérico, por ejemplo, de 0 a 10. Este seria el caso de activos como el prestigio o la confianza de los clientes. Se trata de los activos intangibles.

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto a los demás. La limitación de este tipo de escalas es que no permiten comparar valores más allá de su orden relativo, es decir, no es posible sumar valores.

Las valoraciones numéricas absolutas (escalas cuantitativas) son costosas de elaborar, sin embargo no presentan los problemas existentes en las valoraciones cualitativas ya que sumar valores numéricos es algo normal.

Con independencia de la escala utilizada, para valorar un activo hay que tener en cuenta múltiples factores, entre los que se encuentran:

- Reducción del rendimiento de la actividad.
- Efecto negativo en la reputación.
- Pérdidas económicas.
- Trastornos en el negocio.
- Coste de reposición del activo.
- Coste de mano de obra invertida en recuperar el valor del activo.
- Sanciones por incumplimiento de la ley (violación de la legislación aplicable).
- Sanciones por incumplimiento de obligaciones contractuales.
- Daños a otros activos, propios o ajenos.
- Daños a personas.
- Daños medioambientales.

La valoración debe ser lo más objetiva posible, por lo que en el proceso deben estar involucradas todas las áreas de la organización, aunque no participen en otras partes del proyecto y de esta manera obtener una imagen realista de los activos de la organización.

Es útil definir con anterioridad unos parámetros para que todos los participantes valoren de acuerdo a unos criterios comunes, y se obtengan valores coherentes. Un ejemplo de la definición de estos parámetros podría ser la siguiente:

Disponibilidad:

Para valorar este parámetro debe responderse a la pregunta de cuál sería la importancia o el trastorno que tendría el que el activo no estuviera disponible. Si consideramos como ejemplo una escala de 0 a 3 se podría valorar de la siguiente manera:

Tabla 1: Ejemplos de criterios de disponibilidad

VALOR	CRITERIO
0	No aplica / No es relevante
1	Debe estar disponible, al menos, el 10% del tiempo
2	Debe estar disponible, al menos, el 50% del tiempo
3	Debe estar disponible, al menos, el 99% del tiempo

Por ejemplo, la disponibilidad de un servidor central, sería de 3 con estos criterios.

Integridad:

Para valorar este parámetro la pregunta a responder será qué importancia tendría que el activo fuera alterado sin autorización ni control. Una posible escala sería la siguiente:

Tabla 2: Ejemplos de criterios de integridad

VALOR	CRITERIO
0	No aplica / No es relevante
1	No es relevante los errores que tenga o la información que falte
2	Tiene que estar correcto y completo, al menos, en un 50%
3	Tiene que estar correcto y completo, al menos, en un 95%

Por ejemplo, que en el servidor central fueran modificadas, por personal no autorizado, las cuentas de usuario de los demás departamentos. En este caso, el valor sería 3.

Confidencialidad:

En este caso la pregunta a responder para ponderar adecuadamente este parámetro será cual es la importancia que tendría que al activo se accediera de manera no autorizada. La escala en este caso podría ser la siguiente:

Tabla 3: Ejemplos de criterios de confidencialidad

VALOR	CRITERIO
0	No aplica / No es relevante
1	Daños muy bajos, el incidente no trascendería del área afectada
2	Serían relevantes, el incidente implicaría a otras áreas
3	Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas

Por ejemplo, dependiendo de la organización y su contexto, el valor del servidor podría ser incluso 3 si la dependencia de esa máquina es muy grande y el simple acceso físico al servidor sería un trastorno para la organización.

Escalas para activos físicos:

Tabla 4: Ejemplo de criterios de valoración físicos

VALOR	REDUCCIÓN BENEFICIO	SALUD Y SEGURIDAD	ENTORNO NATURAL	PATRIMONIO SOCIAL/CULTURAL	COMUNIDAD / GOBIERNO / REPUTACIÓN	LEGAL
5	10 MM – 100 MM EUR	Múltiples víctimas o efectos irreversibles >50 pers.	Efectos muy serios, a largo plazo que afectan al ecosistema			Persecución y sanciones significativas.
4	1 MM – 10 MM EUR	Solo una víctima mortal o discapacidad irreversible (>30%)		Daños significativos permanentes a estructuras, elementos de importancia cultural	Protestas serias (cobertura internacional)	Incumplimiento de legislación significativo
3	100.000 – 1MM EUR	Discapacidad irreversible moderada o discapacidad <30%	Efectos serios a medio plazo		Atención significativa a nivel nacional	Incumplimiento de legislación con investigación e informe a las autoridades

VALOR	REDUCCIÓN BENEFICIO	SALUD Y SEGURIDAD	ENTORNO NATURAL	PATRIMONIO SOCIAL/CULTURAL	COMUNIDAD / GOBIERNO / REPUTACIÓN	LEGAL
2	10.000 – 100.000 EUR	Requiere hospitalización pero es reversible	Efectos moderados a corto plazo que no afectan al ecosistema	Daños permanentes a elementos de importancia cultural	Atención de medios y/o comunidades locales y ONGs	Aspectos legales menores, incumplimientos de regulación
1	< 10.000 EUR	No implica tratamientos médicos	Efecto menor sobre el medio	Impactos menores sociales. Principlamente reparabe¡	Atención o quejas pequeñas de públicos o medios locales.	

La valoración de los activos deben realizarla un grupo de personas que sean lo suficientemente representativas como para aportar, entre todos, una visión razonablemente objetiva de la organización. Por supuesto, deben ser personas que conozcan bien la organización. Si se van a hacer las valoraciones mediante reuniones de trabajo, el grupo no debería ser excesivamente numeroso para que las reuniones no se alarguen demasiado. Si se van a utilizar cuestionarios o entrevistas, se puede involucrar a más personas, siempre teniendo en cuenta el coste asociado a ello.

También debe decidirse cómo se va a calcular el valor total de los activos, bien como una suma de los valores que se han asignado a cada uno de los parámetros valorados, bien el mayor de dichos valores, la media de los mismos, etc.

Los criterios para medir el valor del activo deben ser claros, fáciles de comprender por todos los participantes en la valoración y homogéneos, para que se puedan comparar los valores al final del proceso. De esta manera se sabrá cuales son los principales activos de la organización, y por lo tanto aquellos que necesitan de una particular atención.

A estos activos, a los que se debe prestar una especial atención, se les denomina activos críticos. Para identificar qué activos son críticos y cuáles no, es necesario realizar un sencillo cálculo con los parámetros que se han definido para valorarlos. Por cada activo identificado, se suman los valores obtenidos de los parámetros definidos. El resultado de dicha suma es el que va a determinar la criticidad del activo. La Dirección de la organización, junto con el grupo de personas que ha valorado los activos, marca el punto de inflexión a partir del cual el activo es considerado crítico. Se puede tomar como punto de inflexión, la mitad del resultado de la suma mas un punto, aunque la organización puede determinar cualquier otro.

Así, siguiendo con el ejemplo que nos ocupa, si se han tenido en cuenta 3 parámetros (disponibilidad, integridad y confidencialidad) para valorar los activos de la organización, se consideran activos críticos aquellos cuyo resultado de sumar los valores obtenidos de cada parámetro sea mayor o igual a 6.

En el caso del servidor,

Tabla 5: Ejemplo valoración servidor

	Disponibilidad	Integridad	Confidencialidad	Suma de parámetros
Servidor Central	3	3	3	9
Activo Crítico				**SI**

Una vez que se encuentran valorados todos los activos e identificados cuáles de ellos son activos críticos, es preciso, para los activos críticos, realizar el cálculo de dos criterios que serán necesarios para obtener el valor del riesgo. Estos criterios son:

- **Función**: Hace referencia a las consecuencias o daños que pueden alterar la actividad de la organización. Se representa con la letra "**F**". Para evaluar este criterio se responde a la pregunta, ¿las consecuencias pueden alterar la actividad?

Tabla 6: Valoración de la función

CRITERIO DE FUNCIÓN (ALTERACIÓN)	PUNTUACIÓN
Parada total de la actividad	5
Parada de un mes de la actividad	4
Retraso de una semana en la actividad	3
Retraso de un día en la actividad	2
Retraso de unas horas en la actividad	1

- **Sustitución**: Hace referencia a la posibilidad de sustituir los activos. Se representa con la letra "**S**". Para evaluar este criterio se responde a la pregunta, ¿se puede reemplazar el activo?

Tabla 7: Valoración de la Sustitución

CRITERIO DE SUSTITUCIÓN (REEMPLAZAR)	PUNTUACIÓN
Proveedor único en el extranjero	5
Proveedor único nacional	4

CRITERIO DE SUSTITUCIÓN (REEMPLAZAR)	PUNTUACIÓN
Varios proveedores nacionales	3
Varios proveedores en la región	2
Varios proveedores en la ciudad	1

Para cada uno de los activos críticos de la organización se calcula el valor de los dos criterios.

3.3.3. Fase III: Identificación de amenazas.

Una vez identificados y valorados los activos críticos, el siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo.

Una amenaza se define como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o inmateriales en sus servicios.

Es importante conocer las posibles amenazas que pueden afectar a los diferentes activos porque, de este modo, la organización es capaz de anticiparse a los efectos de las mismas.

Dado el objetivo marcado para la protección de las infraestructuras críticas respecto de las amenazas de origen terrorista, serán estas las que deberán ser reflejadas en los análisis que se aporten, considerando que pueden tener un origen, tanto logícas como físicas. Amenazas de este tipo podrían ser, por ejemplo, suplantaciones de la identidad de un usuario, abuso de privilegios de acceso, accesos no autorizados, difusión de malware, manipulación de las configuraciones, etc.

Una vez determinado que una amenaza puede afectar a un activo, es necesario estimar cuán vulnerable es el activo en dos sentidos:

- Degradación: Cuán perjudicado resultaría el activo.
- Frecuencia: Cada cuánto tiempo se materializa la amenaza.

La degradación mide el daño ocasionado por un incidente en el supuesto de que ocurriera.

La frecuencia pone en perspectiva dicha degradación, ya que una amenaza puede tener consecuencias muy graves en el activo pero ser de improbable materialización o, por el contrario, una amenaza puede tener escasas consecuencias y ser tan frecuente que ocasiona un daño considerable en el activo y por extensión en la organización.

A la frecuencia se le otorgan los valores que más se adapten a la organización, siendo un ejemplo típico el siguiente, si bien, como se indica, cada organización debe fijar los valores que considere más adecuados:

Tabla 8: Ejemplo de valoración de amenazas

1/10	Poco frecuente	Una vez al año
1	Normal	Mensualmente
10	Frecuente	Semanalmente
100	Muy frecuente	A diario

A la hora de analizar los riesgos hay que evaluar las distintas amenazas que pueden proceder de las más diversas fuentes. Entre estas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales.

La siguiente ilustración clasifica los diversos tipos de amenazas de los sistemas.

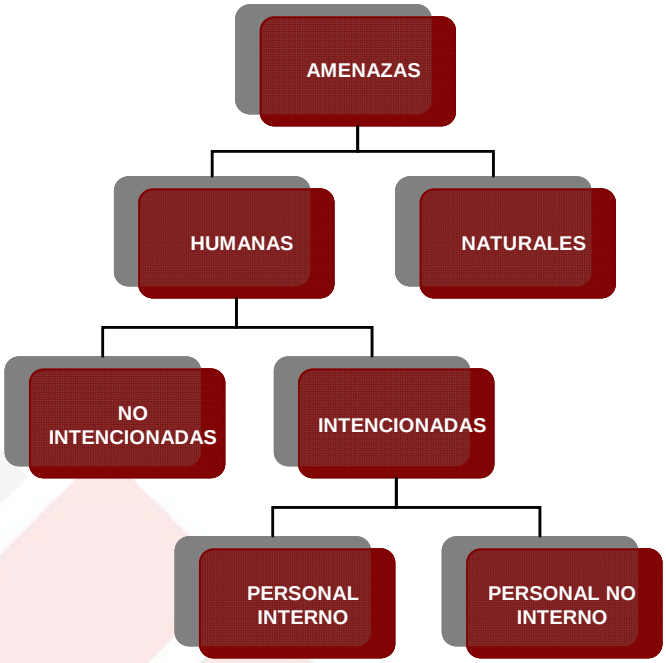

Figura 7: Clasificación general de amenazas

Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de las amenazas intencionadas.

No todas las amenazas afectan a todos los activos sino que, dependiendo de la organización, del proceso analizado y el tipo de activo, son aplicables distintos tipos de amenazas. Las

amenazas tendrán una probabilidad de ocurrencia que dependerá de la existencia de una vulnerabilidad que pueda ser explotada para materializarse en un incidente.

Las vulnerabilidades son debilidades que pueden ser explotadas para convertir una amenaza en un riesgo real que puede ocasionar daños en la organización.Las vulnerabilidades en si mismas no causan daño alguno sino que es una condición o un conjunto de condiciones que pueden permitir a una amenaza afectar a un activo.

Para identificar las vulnerabilidades que pueden afectar a una organización hay que responder a la pregunta, ¿cómo puede ocurrir una amenaza? Para responder a esta pregunta hay que poner como objetivo la amenaza y definir las distintas situaciones por las que puede llegar ocurrir la misma, evaluando si dentro de la organización puede darse esa circunstancia, es decir, si el nivel de protección es suficiente para evitar que se materialice la amenaza.

Así, por ejemplo, si una de las amenazas de la organización es que roben datos estratégicos de la compañía, se pueden establecer, entre otros, los siguientes escenarios:

Tabla 9: Ejemplos de escenarios

Escenarios	Niveles de protección
Entrada no autorizada a los datos a través del sistema informático	¿Existe un control de acceso de datos?
Robo de equipos / datos de dispositivos magnéticos	¿Están los dispositivos de almacenamiento protegidos y controlados de forma adecuada?
Robo de datos mediante accesos no autorizados	¿Existen perfiles adecuados de acceso a los datos?

En el caso de que no se responda afirmativamente a las preguntas de la columna de la derecha, es que existen vulnerabilidades que podrían utilizarse de forma que la amenaza se convierta en un incidente real y causar daños a la organización.

Al hablar de amenazas y vulnerabilidades es necesario definir los criterios de agresión y vulnerabilidad, imprescindibles para calcular el valor del riesgo. Así:

- **Agresión:** Hace referencia a la probabilidad de que el riesgo se manifieste. Se representa con la letra "**A**". Para evaluarlo se responde a la pregunta: ¿Qué probabilidad hay de que se manifieste el riesgo?

Tabla 10: Valoración de la agresión

CRITERIO DE AGRESIÓN (RIESGO)	PUNTUACIÓN
Muy alta	5
Alta	4
Normal	3
Baja	2
Muy Baja	1

- **Vulnerabilidad:** Hace referencia a la probabilidad de que se produzcan daños. Se representa con la letra "**V**". Para evaluar este criterio se responde a la pregunta, ¿qué probabilidad hay de que se produzcan daños?

Tabla 11: Valoración de la vulnerabilidad

CRITERIO DE VULNERABILIDAD (DAÑOS)	PUNTUACIÓN
Muy alta	5
Alta	4
Normal	3
Baja	2
Muy baja	1

Para cada uno de los activos críticos de la organización se calcula el valor de los dos criterios.

3.3.4. Fase IV: Identificación de impactos.

Los incidentes causan un impacto dentro de la organización, que es necesario tener en cuenta a la hora de calcular los riesgos.

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos y la degradación (cuán perjudicado resulta un activo) causada por las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

La valoración del impacto puede realizarse de una manera cuantitativa, estimando las pérdidas económicas, o de una manera cualitativa, asignando un valor dentro de una escala (por ejemplo, alto, medio, bajo).

Así, el robo de información confidencial de la organización puede causar un impacto alto si esta cae en malas manos.

En otro caso, se pueden estimar las pérdidas económicas de equipos tangibles valorando el coste de reposición o la puesta en marcha.

Así, al hablar de impacto o daños ocasionados, es necesario definir dos criterios que se han de tener en cuenta en el cálculo del riesgo. Estos criterios son:

- **Profundidad:** Hace referencia a la perturbación y a los efectos psicológicos que se producen en la imagen de la organización. Se representa con la letra "**P**". Para evaluarlo se responde a la pregunta, ¿cuáles son los efectos en la imagen?

Tabla 12: Valoración de la profundidad

CRITERIO DE PROFUNDIDAD (PERTURBACIÓN)	PUNTUACIÓN
Clientes Vips / Grandes cuentas	5
Clientes habituales	4
Clientes ocasionales	3
Proveedores	2
Personal interno	1

- **Extensión:** Hace referencia al alcance de los daños según su amplitud o extensión. Se representa con la letra "**E**". Para evaluar este criterio se responde a la pregunta, ¿cuál es el alcance del daño?

Tabla 13: Valoración de la Extensión

CRITERIO DE EXTENSIÓN (ALCANCE)	PUNTUACIÓN
Internacional	5
Nacional	4
Regional	3

CRITERIO DE EXTENSIÓN (ALCANCE)	PUNTUACIÓN
Local	2
Individual	1

Para cada uno de los activos críticos de la organización se calcula el valor de los dos criterios.

3.3.5. Fase V: Valoración del riesgo.

Se denomina riesgo a la medida del daño probable sobre un sistema. Al hablar de riesgo, hablamos de la probabilidad de que se produzca un determinado impacto que afecte a los activos y, por tanto, a la organización.

Teniendo en cuenta los distintos *criterios* definidos en los apartados anteriores, se puede calcular el riesgo asociado a los activos críticos de la organización y, por tanto, la actuación que deberá llevar a cabo la misma ante dichos riesgos.

Para ello se procede a realizar una serie de cálculos que podemos enumerar en cuatro etapas:

Figura 8: Fases para el cálculo del riesgo

3.3.5.1. Etapa 1 – Cálculo del carácter del riesgo

La fórmula para calcular el carácter del riesgo es la siguiente:

*CARÁCTER DEL RIESGO (**C**) = IMPORTANCIA DEL SUCESO (**I**) + DAÑOS OCASIONADOS (**D**)*

Para poder calcular tanto la importancia del suceso como el daño ocasionado es necesario conocer los criterios de función y sustitución (en el caso de la importancia del suceso) y de profundidad y extensión (en el caso del daño ocasionado) del activo seleccionado.

Los datos de estos criterios se habrán obtenido con anterioridad siguiendo las indicaciones de los apartados 3.3.2 Fase II: Valoración de activos y 3.3.4 Fase IV: Identificación de impactos.

*IMPORTANCIA DEL SUCESO (**I**) = FUNCIÓN (**F**) x SUSTITUCIÓN (**S**)*

*DAÑO OCASIONADO (**D**) = PROFUNDIDAD (**P**) x EXTENSIÓN (**E**)*

3.3.5.2. Etapa 2 – Cálculo de la probabilidad

Tomando los valores de los criterios de agresión y vulnerabilidad del activo sobre el que se quiera calcular el riesgo se obtiene la probabilidad.

Los datos de estos criterios se habrán obtenido con anterioridad siguiendo las indicaciones del apartado 3.3.3 Identificación de amenazas.

*PROBABILIDAD (**PB**) = AGRESIÓN (**A**) x VULNERABILIDAD (**V**)*

3.3.5.3. Etapa 3 – Cálculo del riesgo

Con los datos obtenidos en las etapas anteriores se calcula el riesgo del activo seleccionado.

*RIESGO (**R**) = CARÁCTER DEL RIESGO (**C**) x PROBABILIDAD (**PB**)*

Etapa 1 **Etapa 2**

3.3.5.4. Etapa 4 – Actuación de la organización

Una vez que se han realizado los cálculos anteriormente citados, se compara el dato obtenido del valor del riesgo (valor que estará entre 2 y 1250) con la siguiente tabla:

Tabla 14: Estrategias de gestión del riesgo

VALOR DEL RIESGO	CLASE DE RIESGO	ACTUACIÓN DE LA ORGANIZACIÓN
2 – 250	Insignificante	Riesgo despreciable, no requiere acción
251 – 500	Menor	Riesgo despreciable, no requiere acción
501 – 750	Normal	Riesgo aceptable, no requiere acción pero se recomienda tener en consideración la posibilidad de actuar a largo plazo
751 – 1000	Significativo	Riesgo inaceptable, requiere de una acción a corto plazo
1001 – 1250	Muy significativo	Riesgo inaceptable, requiere de una actuación inmediata

Al conocer en que intervalo se encuentra el valor del riesgo calculado, se obtiene que clase de riesgo deriva del activo crítico sometido a estudio.

Con todos los activos críticos de la organización, se repiten los cálculos citados con anterioridad (las 4 etapas) y se obtiene una relación de los riesgos de la organización asociados a cada activo crítico.

De este modo, la Dirección de la organización dispone de toda la información necesaria para decidir, teniendo en cuenta factores legislativos o compromisos contractuales con clientes y proveedores, las acciones a tomar.

Así, si el riesgo está por encima de lo aceptable se puede:

- Eliminar el activo, la Organización debe valorar si puede prescindir de ese activo porque no merece la pena mantenerlo.
- Introducir nuevas salvaguardas/contramedidas (mecanismos que reducen el riesgo, es decir, las medidas de seguridad) o mejorar la eficacia de las presentes.
- Transferir el riesgo a terceras partes.

3.4. HERRAMIENTAS

La realización de análisis de riesgos suele conllevar la valoración de múltiples variables y en diferentes dimensiones, por ello, es muy recomendable en apoyarse en algún tipo de herramienta que permita dar soporte al proceso de análisis y gestión de riesgos.

Existen múltiples herramientas de este tipo en el mercado, pero hemos de destacar que, normalmente, dichas herramientas van muy ligadas a una metodología de riesgos concreta por lo que se debe evaluar en detalle, antes de adquirir ninguna herramienta, qué metodología vamos a emplear, si la herramienta que queremos se adapta a nuestra metodología, o si, por el contrario, deberemos elaborar nuestra propia herramienta adaptada a nuestras necesidades.

Esta dependencia se produce, normalmente, porque además de actuar como repositorio de información, estas herramientas incluyen también soporte al proceso de realización de análisis y gestión de riesgos y mantienen su propio catálogo de amenzas, vulnerabilidades, etc. así como sus propios niveles de clasificación de riesgos.

Al valorar estas herramientas, también deberemos considerar si dan soporte a nuestros requisitos en cuanto a acceso a la información que alojaran, posibilidad de contar con distintos perfiles de usuarios, accesos remotos, realización de análisis de riesgos por varios usuarios con diferentes responsabilidades o posibilidad de visualizar los niveles de riesgos a distintos niveles (organización, servicio esencial, infraestructura crítica). Para finalizar, también hay que destacar que no es fácil encontrar herramientas que permitan realizar un análisis de riesgos integral considerando tanto las medidas de seguridad física, como las lógicas.

4. MEDIDAS DE SEGURIDAD

4.1. GESTIÓN DE LA SEGURIDAD

4.1.1. Objetivos

El objetivo de un Plan de Seguridad es identificar y evaluar los riesgos que afectan a una entidad, con el objetivo de implantar contramedidas, procesos y procedimientos para su apropiado control, tratamiento y mejora continua. Este Plan deberá ayudar a mantener un nivel de exposición siempre menor al nivel de riesgo que la propia entidad ha decidido asumir.

Un punto importante dentro de un Plan, es la Gestión de la Seguridad dentro de una entidad, entendiéndola como la preservación de los principios básicos de la **confidencialidad** (acceso a la información por parte únicamente de quienes estén autorizados), **integridad** (mantenimiento de la exactitud y completitud de la información y sus métodos de proceso) y **disponibilidad** (acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran) de la misma y de los sistemas implicados en su tratamiento. Estos tres principios son elementos esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen, necesarios para lograr los objetivos de cualquier entidad.

4.1.2. Descripción de la Gestión de la Seguridad en Operadores Críticos

La información, junto a los procesos, personas y sistemas que hacen uso de ella, son activos muy importantes dentro de una entidad u organización.

Las entidades y sus sistemas de información están expuestos a un número cada vez elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a los mismos a diversas formas de fraude, espionaje, sabotaje o vandalismo, entre otros.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de la entidad para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades, son algunos de los aspectos fundamentales en los que el Plan de Seguridad es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones y entidades.

Con un Plan de Seguridad, las entidades conocen los riesgos a los que está sometida su información y activos y los asume, minimiza, transfiere o controla mediante una metodología definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Además, será importante que en la entidad se establezca y facilite el acceso a una fuente especializada de consulta en seguridad de la información. Deberán desarrollarse contactos con especialistas externos en seguridad, que incluyan a las administraciones pertinentes, con objeto de mantenerse actualizado en las tendencias, la evolución de las normas y los métodos

de evaluación, así como proporcionar enlaces adecuados para el tratamiento de las incidencias de seguridad.

4.1.3. Mejores prácticas

4.1.3.1. Estructura y Compromiso de Dirección

Se deberá establecer una estructura de gestión con objeto de iniciar y controlar la implantación del Plan de Seguridad dentro de la entidad.

Es importante un enfoque multidisciplinario de la seguridad que implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en las diferentes áreas.

Estructura del Comité de Gestión

El Comité de Gestión se crea en la entidad, a propuesta de Dirección. Es un Órgano Auxiliar de Dirección, que durante la etapa de diseño e implantación del Plan de Seguridad, juega un papel fundamental en la elaboración y aprobación de la documentación soporte del Plan.

El Comité deberá tener autonomía para poder llevar a cabo todas las acciones necesarias para la implantación del Plan.

A las sesiones de trabajo del Comité, serán invitados los miembros de diferentes departamentos o áreas, cuando se considere necesario.

Asegurar el compromiso de Dirección y de los trabajadores

La Dirección debe proporcionar evidencias claras de su compromiso con el desarrollo e implementación del Plan de Seguridad, así como con la mejora continua de su eficacia. Es la Dirección, en primera instancia, quien debe tomar decisiones:

- Comunicando a la entidad la importancia de la implantación del Plan. Introduciendo cambios de mentalidad, de sensibilización, de procedimientos y tareas, etc.
- Asegurando que se establecen los objetivos.
- Llevando a cabo las revisiones.
- Asegurando la disponibilidad de recursos necesarios.

Sin el apoyo decidido de la Dirección no es posible la implantación del Plan en la entidad. Su éxito depende especialmente de su compromiso.

De igual forma, el resto de personal establece su compromiso de participar desde su inicio, en la identificación de los problemas, propuestas, soluciones y mejoras, y por el cumplimiento con las disposiciones que se establezcan una vez aprobado el Plan de Seguridad.

4.1.3.2. Coordinación de la Seguridad de la Información.

El **Comité de Gestión del Plan Seguridad** estará formado por:

- **Responsable del Comité**: Tiene funciones estratégicas, deberá formular la política del Plan de Seguridad, establecer los objetivos del mismo y velar por su cumplimiento, aprueba roles y responsabilidades en materia de seguridad, comunicará a la entidad la importancia de cumplir con los objetivos y la política de seguridad, sus responsabilidades legales y la necesidad de la mejora continua. Proporciona recursos suficientes para crear, implementar, operar, supervisar, mantener y mejorar el Plan de Seguridad. Vela por que se realicen las auditorías internas del Plan, dirigirá las revisiones del mismo, y deberá revisar los informes de auditoría, comprobar que se hacen controles periódicos, coordinar actividades, aprobar mejoras técnicas propuestas, etc.

- **Responsable del SGSI**: Es el encargado de llevar a cabo todas las directrices marcadas por la Dirección. Propondrá los roles de seguridad, recursos necesarios, estrategias, etc. encaminados a conseguir los objetivos de seguridad. Realizará las revisiones y mejoras del Plan de Seguridad, actualizará procedimientos, etc.

- **Responsable de Seguridad**: Sus funciones serán la realización del análisis de riesgos, proponer nivel de riesgo residual aceptable, evaluación de contramedidas, implantación de las contramedidas, proponer al responsable del Comité, mejoras prácticas...

- **Responsable de Departamento o Área**: Su función será principalmente la de comunicar las necesidades de seguridad. Deberá desplegar y mantener aquellas medidas que afecten a su área o departamento.

4.1.3.3. Asignación de Responsabilidades.

A continuación se muestra la asignación de responsabilidades por rol, alineadas con los objetivos de cualquier Entidad u Organismo considerado como Infraestructura crítica:

Tabla 15: Obligación /Rol asignado

Obligación / Rol asignado	Responsable Comité de Seguridad	Responsable SGSI	Responsable Seguridad	Responsables Departamentos/Áreas
Alineación Estratégica	Requerir un alineamiento demostrable.	Instituir procesos para integrar la seguridad con los objetivos de la entidad.	Desarrollar y revisar una estrategia de seguridad. Supervisar el Plan y las iniciativas, y vincularlo con las estrategias de cada área.	Aportar información sobre las estrategias del área. Validar estrategias de seguridad propuestas.

Obligación / Rol asignado	Responsable Comité de Seguridad	Responsable SGSI	Responsable Seguridad	Responsables Departamentos/Áreas
Administración del Riesgo	Crear una política de administración del riesgo en todas las actividades y asegurar su cumplimiento.	Proponer una política de administración del riesgo y las prácticas y actuaciones para desplegarla.	Identificar los riesgos y proponer evaluaciones de los mismos e impacto. Plantear estrategias de mitigación del riesgo.	Ejecutar la política y el cumplimiento regulatorio identificando los problemas de cumplimiento en el área.
Entrega del Valor	Requerir un informe de costes de actividad de seguridad.	Realizar estudios de iniciativas de seguridad.	Monitorear la utilización y la efectividad de los recursos de seguridad.	Revisar y asesorar las iniciativas respecto a seguridad y asegurar la satisfacción de los objetivos de la entidad.
Medición del Rendimiento	Requerir el informe de efectividad de la seguridad.	Desarrollar e implementar los métodos de monitorización y medición en las actividades de seguridad.	Monitorear y medir las actividades de seguridad.	Monitorear y medir las actividades de seguridad en el área.
Administración de Recursos	Instituir una política de administración de los conocimientos y utilización de los recursos.	Proponer y desarrollar métodos para la captación y divulgación de conocimientos. Desarrollar medidas de efectividad y eficiencia.	Desplegar los procesos para la captación y la divulgación de los conocimientos.	Desplegar los procesos para la captación y la divulgación de los conocimientos en el área.
Aseguramiento del Proceso	Aprobar una política de contratación de proveedores.	Proponer criterios de selección y contratación de proveedores.	Velar por el cumplimiento de los requisitos mínimos en la contratación de proveedores.	Comunicar necesidades.

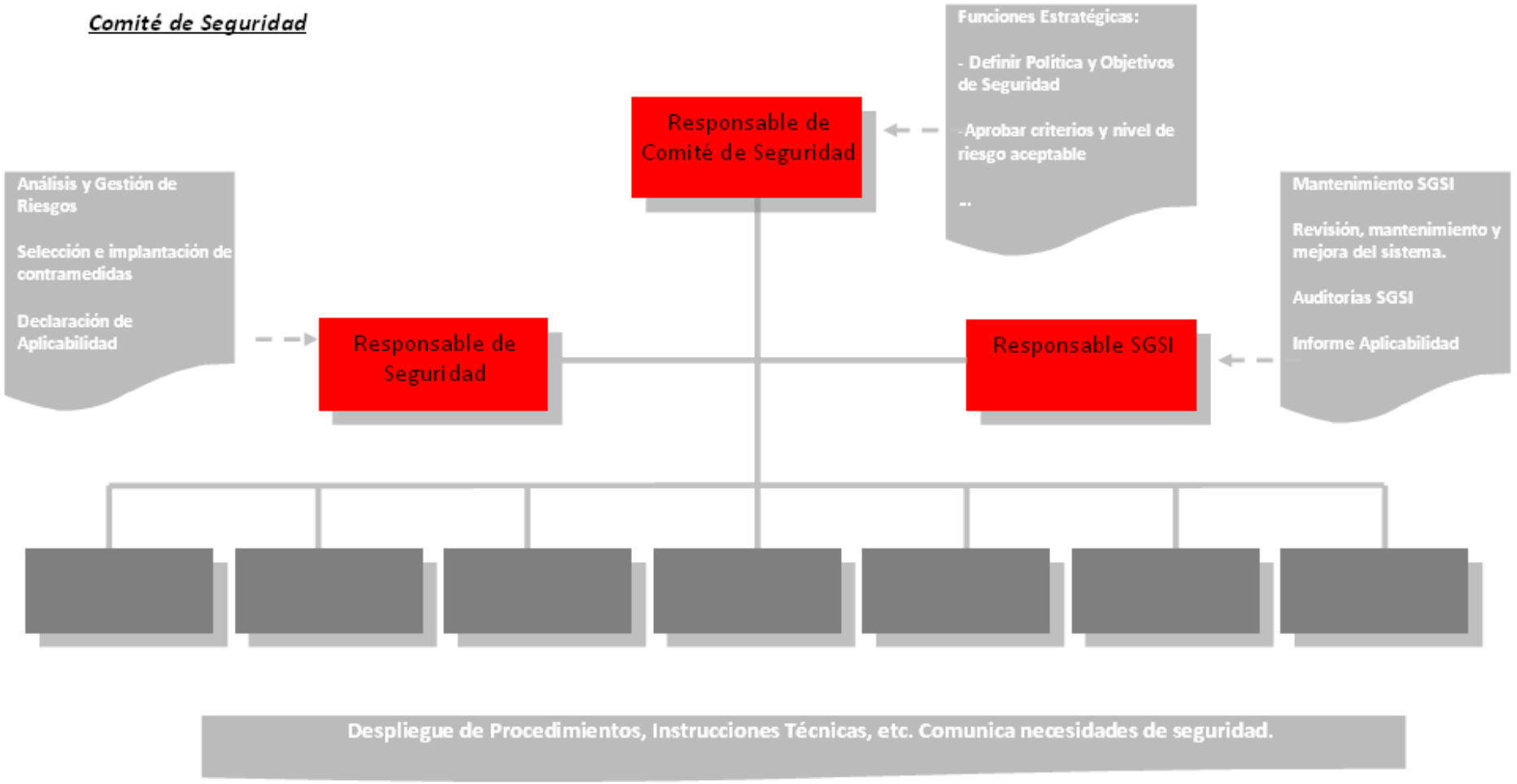

Figura 9 : Ejemplo de organigrama de seguridad

Organismos de Apoyo

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se recomienda mantener contactos con los siguientes Organismos especializados en temas relativos a la seguridad informática:

4.1.3.3.1. Contacto con las Autoridades

Se deberán mantener contactos con las autoridades pertinentes. Posibles entidades con las que mantener contacto serían las siguientes:

CNPIC

CNPIC, Centro Nacional para la Protección de las Infraestructuras Críticas, es el órgano director y coordinador de cuantas actividades relacionadas con la protección de las infraestructuras críticas tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior, a la que está adscrito.

Su principal objetivo es prestar una eficaz colaboración para **mantener seguras las infraestructuras críticas españolas que proporcionan los servicios esenciales a nuestra sociedad.**

ICS – CERT (Industrial Control Systems Cyber Emergency Response Team)

Ofrece un sistema de control de seguridad en colaboración con la US-CERT enfocado para:

- Responder y analizar sistemas de control relacionados con incidentes.
- Vulnerabilidad y análisis del malware.
- Proveer soporte in situ para respuesta a incidentes y análisis forense.
- Proporcionar conocimiento de la situación en forma de inteligencia procesable.
- Coordinar la divulgación responsable de vulnerabilidades / mitigaciones.
- Compartir y coordinar la información sobre la vulnerabilidad y el análisis de amenazas a través de productos de información y alertas.

El ICS-CERT es un componente clave de la Estrategia de Seguridad de los Sistemas de Control.

CCN-CERT, CNI (Centro Nacional de Inteligencia)

CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), dependiente del CNI (Centro Nacional de Inteligencia).

Su principal objetivo es contribuir a la mejora del nivel de seguridad de los sistemas de información de las tres administraciones públicas existentes en España (general, autonómica y local). Para lograr su objetivo, responden de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir y afrontan de forma activa las nuevas amenazas existentes.

Para contribuir a esta mejora del nivel de seguridad, el CCN-CERT ofrece sus servicios a todos los responsables de Tecnologías de la Información de las diferentes administraciones públicas.

Líneas de actuación:

- Soporte y coordinación para la resolución de incidentes que sufra la Administración General, Autonómica o Local. A través de su servicio de apoyo técnico y de coordinación, actúa rápidamente ante cualquier ataque recibido.
- Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las administraciones públicas. Las Series CCN-STIC elaboradas por el CCN ofrecen normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los Sistemas TIC en la Administración.
- Formación a través de los cursos STIC, destinados a formar al personal de la Administración especialista en el campo de la seguridad de las TIC e impartidos a lo largo de todo el año.
- Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas a partir de diversas fuentes de reconocido prestigio (incluidas las propias).

INTECO (Instituto Nacional de Tecnologías de la Comunicación) - INTECO (CERT) Centro de Respuesta a Incidentes de Seguridad

INTECO tiene encomendadas las misiones de sentar las bases de coordinación de distintas iniciativas públicas en torno a la seguridad informática, impulsar la investigación aplicada y la formación especializada en el ámbito de la seguridad en el uso de las TIC y convertirse en el Centro de Referencia en Seguridad Informática a nivel nacional.

Guardia Civil – GDT (Grupo de Delitos Telemáticos)

El GDT está creado para perseguir los delitos informáticos. Si se identifica en la entidad un problema de seguridad en la red, un contenido ilícito o detectamos u observamos una conducta que pudiera ser delictiva, se deberá comunicarlo al GDT. Todo lo que en ella se recibe es tratado con la máxima discreción.

Cuerpo Nacional de Policía

El desarrollo de la Sociedad de la Información y la difusión de los efectos positivos que de ella se derivan exigen la generalización de la confianza de los ciudadanos en las comunicaciones telemáticas.

Como respuesta a esta necesidad, y en el marco de las directivas de la Unión Europea, el Estado español ha aprobado un conjunto de medidas legislativas, como la Ley de Firma Electrónica y el RD sobre el Documento Nacional de Identidad electrónico, para la creación de instrumentos capaces de acreditar la identidad de los intervinientes en las comunicaciones electrónicas y asegurar la procedencia y la integridad de los mensajes intercambiados.

Además, el C.N.P. (Cuerpo Nacional de Policía) persigue actividades relacionadas con delitos tecnológicos tales como:

- Fraudes en Internet: Comunicación sobre uso fraudulento de tarjetas de crédito, fraudes en subastas, comercio electrónico, estafas en la red.
- Seguridad lógica: Seguridad lógica, virus, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidad o sustracción de cuentas de correo electrónico.
- Fraudes en las comunicaciones: Amenazas, injurias y calumnias cometidas con la utilización del correo electrónico, mensajes a través de teléfonos móviles (SMS y/o MMS), tablones de anuncios, foros de Internet, newsgroup, etc.… También sobre el uso indebido de señales de video y fraudes en las telecomunicaciones.

4.1.3.3.2. Contacto con Grupos de Especial Interés

AEI Seguridad

La Agrupación Empresarial Innovadora para la seguridad de las redes y los sistemas de información reúne a empresas, asociaciones, centros de I+D+i y entidades públicas o privadas interesadas en la promoción del sector de las Nuevas Tecnologías, sus industrias afines y auxiliares, así como otros sectores emparejados con el mismo, que deseen contribuir a los fines de la Asociación, en el ámbito nacional de las Tecnologías de Seguridad.

McAfee Alerts

Avisa a los usuarios de las nuevas y peligrosas amenazas que se pueden encontrar en la red. Se trata de evitar ser víctimas de los peligros online. Nos ofrecerá: actualizaciones de firmas malware, alertas de nuevas amenazas, notificaciones de .DAT, notificaciones de seguridad, etc.

Symantec

Symantec ayuda a los consumidores y a las organizaciones a proteger y administrar su información. Sus servicios y programas protegen contra una mayor cantidad de riesgos en más puntos y de una forma más completa y eficaz, lo que brinda tranquilidad sin importar dónde se utilice o almacene la información.

- Protección y administración de un mundo impulsado por la información. Su enfoque fundamental es eliminar los riesgos para la información, la tecnología y los procesos independientemente del dispositivo, la plataforma, la interacción o la ubicación.
- **Protección completa**. Por medio de Symantec, se puede proteger más información e infraestructura tecnológica, en un nivel más profundo, en cualquier ubicación donde se use o almacene la información. Desde la seguridad de las interacciones y de la identidad en línea de los usuarios hasta la protección de los datos de uso crítico de una organización, Symantec ofrece los mejores productos líderes en su clase orientados a la seguridad, las copias de seguridad y la recuperación, la disponibilidad de datos y la prevención contra la pérdida de datos.
- **Control automático**. Dado que cuenta con la cartera más completa de software de administración y seguridad, Symantec ayuda a controlar más procesos de manera automática, en el equipo particular o en el datacenter corporativo. Symantec ayuda a estandarizar y automatizar la manera en que las personas y las organizaciones implementan las políticas (desde la seguridad en línea hasta el cumplimiento de normas de TI en toda la empresa).

BSA (Business Software Alliance)

La BSA es una asociación comercial sin ánimo de lucro creada para defender los objetivos del sector de software y hardware. Fomenta un mundo digital seguro y legítimo.

Entre las prioridades de la BSA se incluyen:

- Proteger la propiedad intelectual (copyright, patentes, mandatos sobre tecnología).
- Abrir los mercados a un comercio sin barreras.
- La seguridad de los datos.
- La innovación y variedad del software.
- El gobierno electrónico.
- Mano de obra y educación

Alertas ESET

Consejos de seguridad para el uso seguro del ordenador y de la información sensible y personal.

OSI (Oficina de Seguridad del Internauta)

Es un servicio del Gobierno para proporcionar la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden afectar al navegar por Internet. Su objetivo es elevar la cultura de seguridad, prevenir, concienciar y formar proporcionando información clara y concisa acerca de la tecnología y el estado de la seguridad en Internet. Al mismo tiempo impulsa la detección y denuncia de nuevas amenazas en la red, de fraudes, estafas online o de cualquier otro tipo de ataque de Seguridad Informática.

CWE (Common Weakness Enumeration)

Se trata de una importante fuente de información de seguridad de aplicaciones en general, una comunidad perteneciente al MIT, que se dedica a enumerar y clasificar los tipos de debilidades y vulnerabilidades de las aplicaciones, incluyendo por supuesto a las aplicaciones web.

4.1.3.4. Terceros

4.1.3.4.1. Objetivo

La seguridad de la información de la entidad y las instalaciones de procesamiento de la información, no debería ser reducida por la introducción de un servicio o producto externo. Debería controlarse el acceso de terceros a los dispositivos de tratamiento de información.

Cuando la entidad requiera dicho acceso de terceros, se deberá realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que requieren. Estas medidas de control deberán definirse y aceptarse en un contrato con la tercera parte.

4.1.3.4.2. Identificación de los Riesgos del Acceso de Terceros

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la entidad, se llevará a cabo y documentará una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información de la entidad.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

Buenas prácticas

- Realizar inventario de conexiones de red y flujos de información significativos con terceras partes.
- Evaluar riesgos.
- Tras identificar los riesgos, se deberán implementar controles apropiados antes de conceder el acceso.
- Revisar los controles de seguridad de información existentes respecto a los requisitos.
- Considerar exigir certificados en ISO/IEC 27001 a los socios más críticos, tales como outsourcing de TI, proveedores de servicios de seguridad TI, etc.

4.1.3.4.3. Tratamiento de la Seguridad en los Contratos

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

- Cumplimiento del Plan de Seguridad de la entidad.
- Protección de los activos de la entidad, incluyendo:
    - Procedimientos para proteger los bienes, abarcando los activos físicos, la información y el software.
    - Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
    - Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
    - Restricciones a la copia y divulgación de información.
- Descripción de los servicios disponibles.
- Nivel de servicio esperado y niveles de servicio aceptables.
- Permiso para la transferencia de personal cuando sea necesario.
- Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
- Existencia de Derechos de Propiedad Intelectual.

- Definiciones relacionadas con la protección de datos.
- Acuerdos de control de accesos que contemplen:
    - Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas.
    - Proceso de autorización de accesos y privilegios de usuarios.
    - Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
- Definición de criterios de desempeño comprobables, de monitoreo y presentación de informes.
- Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
- Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia
- Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
- Proceso claro y detallado de administración de cambios.
- Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
- Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- Controles que garanticen la protección contra software malicioso.
- Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
- Relación entre proveedores y subcontratistas.

4.1.4. Herramientas

4.1.4.1. Gestión Documental

Servirá para evitar la pérdida de documentos, evitar la violación de la información o la destrucción no deseada de documentos, mantener información crítica oculta a quién no debiera tener acceso a ella, etc. Además, será importante tener un lugar donde almacenar las políticas de manera que puedan ser accedidas en cualquier momento por las personas responsables.

4.1.4.2. Gestión de flujos de trabajo

Será necesario controlar los documentos cuando se pasen de una persona a otra. Se establecerán unas reglas para el flujo de documentos.

4.1.4.3. Cuadro de mando

Herramienta útil para Dirección a la hora de evaluar su estado de seguridad. Se trata de una herramienta de gestión que facilita la toma de decisiones que recoge un conjunto coherente de indicadores que proporcionan a la Dirección y a los responsables, una visión comprensible del estado de seguridad de la entidad y de su área de responsabilidad, que indica si se han marcado los objetivos propuestos. Nos ayudará a contestar preguntas tales como: "¿cómo estamos afrontando los nuevos retos de seguridad?", "¿cómo gestionamos los controles de seguridad para lograr el máximo nivel de seguridad?", "¿cómo perciben la seguridad de la entidad los empleados?", "¿cómo contribuye la seguridad a cumplir los objetivos de la entidad?"

4.1.4.4. Cortafuegos

Herramienta para la prevención de ataques externos por parte de los intrusos de Internet (Hackers). Ofrece seguridad de protección contra intrusos determinando que servicios de la red pueden ser accesibles y quienes pueden utilizar estos recursos, manteniendo al margen a los usuarios no autorizados y generando, en caso de un ataque, alarmas de seguridad.

4.1.4.5. Access Control Lists (ACL)

Las Listas de Control de Accesos proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas Operativos. Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo pueden definirse sobre un Proxy una lista de todos los usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios.

4.1.4.6. Sistemas Anti-Sniffers

Esta técnica consiste en detectar Sniffers en el sistema. Generalmente estos programas se basan en verificar el estado de la placa de red, para detectar el modo en el cual está actuando, y el tráfico de datos en ella.

4.1.4.7. Gestión de Claves Seguras

La importancia de la utilización y robustez de las contraseñas y claves es muy elevada. Recomendaciones:

- Al menos 8 caracteres para crear la clave.
- Utilizar en una misma contraseña dígitos, letras y caracteres especiales.
- Alternar aleatoriamente en las letras mayúsculas y minúsculas.

- Contraseña que pueda recordarse fácilmente y escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.
- Cambio de contraseñas con una cierta regularidad.
- Utilizar signos de puntuación si el sistema lo permite.

Existe también la posibilidad de recurrir a herramientas y soluciones de software que creen las contraseñas seguras que vamos a utilizar.

- *ViPNet Password Roulette*: http://www.infotecs.biz
- *Cryptix*: http://www.rbcafe.com/
- *KeePassX:* gestor de contraseñas multiplataforma que permite guardar diversa información como nombre de usuario, contraseñas, direcciones web, archivos adjuntos, etc. en una base de datos. Además KeePassX ofrece una pequeña utilidad para la generación de contraseñas seguras de forma rápida y sencilla.

4.2. FORMACIÓN

4.2.1. Objetivos

La formación y concienciación en seguridad son elementos básicos para el éxito del Plan. Por ello, la Dirección deberá asegurar que el Plan sea comunicado y comprendido por todos los niveles de la entidad.

La concienciación en materia de seguridad dentro de la entidad es un factor de vital importancia para la seguridad efectiva de la misma. La primera barrera de protección son las propias personas.

Sólo podremos conseguir educar si somos capaces de que cada uno vea claras las ventajas de este Plan. Además, si el personal está debidamente formado y concienciado, lo más probable es que se puedan evitar imponer medidas disciplinarias.

4.2.2. Descripción

Para que el Plan de Seguridad llegue a todos y se llegue a entender y apoyar, será necesario crear un programa de concienciación enfocado a educar, habrá que mostrar casos prácticos para que se pueda apreciar clara la realidad.

	CONCIENCIAR	ENTRENAR	EDUCAR
Da respuesta a:	¿Qué?	¿Cómo?	¿Por qué?
Objetivo:	Ser capaces de identificar	Entrenar habilidades	Conocer los

	situaciones		motivos
¿Cómo hacerlo?	• Videos • Periódicos • Posters	• Practicar • Casos reales	• Debates • Charlas

Todos los empleados de la organización y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la organización, recibirán esta formación y una actualización periódica en materia de la política, normas y procedimientos de la organización. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general.

Además, el personal que ingrese a la organización recibirá una formación especial, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

4.2.3. Mejores prácticas

4.2.3.1. Estudiar las necesidades de la entidad

El paso previo a la preparación del programa de concienciación debe ser contar con un pequeño estudio previo que oriente a la hora de definir los objetivos a alcanzar. Será necesario saber lo que el personal realmente necesita. Para tener claro el alcance podemos:

- Preparar una encuesta para analizar los problemas que más nos preocupan.
- Mantener reuniones con algunos representantes (dirección, sistemas, operadores, etc.).
- Verificar la existencia de material utilizado previamente.
- Revisar la política de seguridad de la entidad: será la base de este programa.
- Recopilar información acerca de incidentes de seguridad previos (ataques sobre nuestra infraestructura, robo, virus, etc.).

Una vez conocido el nivel de concienciación de la entidad y, sobre la base de la realidad de la misma, se deberá proceder al diseño del plan de concienciación.

4.2.3.2. Desarrollar y definir el programa de concienciación

Este plan deberá contener estos elementos:

- ¿A quién va dirigido el plan? ¿Quién requiere mayor atención?
- ¿Obliga alguna ley o norma a realizar este programa? Concienciar a usuarios puede ser una exigencia legal (LOPD) o un requisito de alguna certificación voluntaria (ISO 27001).
- Objetivos para cada apartado del programa: Ayudará a saber si la formación y concienciación efectuada ha sido realmente efectiva.
- ¿Cómo se concienciará? Necesidad de un método para concienciar: charlas, envíos por correo de documentos, viñetas en tono de humor, etc.
- Frecuencia / repetición. Se planificará con qué frecuencia se volverá a realizar la concienciación. De poco o nada sirve hacer concienciaciones puntuales. Se debe conseguir incluir en la cultura de la entidad la concienciación en seguridad como un elemento más.
- Simulacros / ensayos. Se incluirán, dentro de las acciones formativas, simulacros o ensayos que ayuden a prevenir sucesos o accidentes de impacto negativo en la entidad.

4.2.4. Herramientas

4.2.4.1. Plataformas de formación online

Disponibilidad para utilizar herramientas Open Source. Ejemplos: Moodle, Atutor, Claroline, Dokeos, Chamilo, Ilias, .LRN, etc. Desde estas plataformas se podrán realizar cursos de formación on-line, así como poner a disposición de los empleados guías de buenas prácticas.

4.2.4.2. Encuestas

Será importante disponer de herramientas que nos permitan realizar encuestas, cuestionarios, entre los empleados, pudiendo conocer, de esta manera, su nivel de formación y concienciación en los temas de interés. Ejemplos:

Encuestas Moodle. Dentro de la plataforma Moodle, encontraremos este módulo que nos proporciona un conjunto de instrumentos que permiten recopilar datos: Questionnaire, Surveys, FeedBack, Quizes moodle desde Word (plantilla para generar encuestas desde Microsoft Word de una forma muy sencilla).

PHPESP. Aplicación eficaz, basada en la Web, que permite crear complejas y avanzadas encuestas, ver los resultados en tiempo real, y llevar a cabo análisis.

PHP Surveyor. Permite desarrollar, publicar y recoger respuestas de encuestas. Muestra las encuestas por respuestas únicas, grupo por grupo o todas en una página, o se puede usar un sistema de entrada de datos para administración de versiones en papel de las encuestas. Encuestas 'bifurcadas', plantillas para modificar el aspecto y análisis estadísticos.

phpFormGenerator. Aplicación que sirve para generar formularios dinámicos sin necesidad de tener conocimientos de programación. Los formularios generados con este sistema permiten enviar los datos ingresados por el visitante a una dirección de email, a una base de datos o ambos en forma simultánea

Survey monkey. Ofrece funciones para elaborar fácilmente un cuestionario con diversas modalidades de respuesta. Las herramientas de análisis le permiten organizar las respuestas a las preguntas y efectuar correlaciones múltiples.

4.2.5. Ejemplos

Ejemplo de aspectos a tratar en un programa de concienciación:

- Utilización de las contraseñas: ¿Cómo crearlas?, ¿con qué frecuencia cambiarla?, ¿cómo protegerla?
- Protección contra virus: importancia de tener el antivirus activado, escaneos periódicos, etc.
- Cumplir la política de seguridad: implicaciones de su incumplimiento (tanto para el usuario como para la entidad).
- Correo electrónico: buenas prácticas respecto al envío y recepción de adjuntos, cómo actuar cuando se recibe correo electrónico de direcciones no conocidas, etc.
- Utilización de Internet: Qué está permitido y qué prohibido.
- Backup de los datos: si la entidad no dispone de medios para hacer copias de seguridad, debería concienciarse a los usuarios de la importancia de hacer copia de los datos que utiliza en el día a día.
- Seguridad de los dispositivos USB.
- ¿Qué hacer en caso de incidente?, ¿con quién contactar?, ¿qué debo hacer?
- Ingeniería social: Mediante ejemplos de correos electrónicos solicitando claves, etc.
- Envío de información sensible/confidencial: medidas de seguridad que deben aplicarse.
- Seguridad en los viajes: prestar atención al equipo portátil, a las conversaciones, etc.
- Software permitido y no permitido: el software no permitido y no controlado puede poner en riesgo la seguridad de la entidad.
- Seguridad de los equipos: Protectores de pantalla, bloqueo de PC, etc.

4.3. MEDIDAS DE SEGURIDAD TÉCNICAS

4.3.1. Seguridad en la red

4.3.1.1. Objetivos

Fundamentalmente, en estos entornos de seguridad industrial, el objetivo la seguridad en la red es garantizar el correcto aislamiento de dichas redes que dan soporte a los sistemas de control del resto de la red corporativa.

Dado el estado de seguridad de dichos sistemas, su aislamiento es la principal medida para garantizar que dichos sistemas no se vean afectados por incidentes de seguridad.

4.3.1.2. Descripción

El uso de protocolos TCP/IP ha facilitado las conexiones entre los equipos, no obstante esto ha supuesto que haya menos seguridad en los sistemas de las organizaciones. Al mismo tiempo, el núcleo de la infraestructura de información - Internet - es objeto de múltiples ataques. Estos ataques en el futuro podrían tener graves consecuencias, tales como interrupción prolongada de los servicios esenciales. Existe gran variedad de caminos para tomar el control de las redes de las organizaciones:

- Conexiones a redes de empresa.
- Redes privadas virtuales comprometidas.
- Conexiones inalámbricas inseguras.
- Puertos abiertos y desprotegidos.
- Conexiones a Internet.
- Puestas traseras.

Un cortafuegos o firewall es un elemento esencial en la seguridad de cualquier red conectada a otra red no segura como Internet. El cortafuegos aporta protección contra virus, gusanos y otros tipos de código malicioso así como contra intrusiones.

4.3.1.3. Mejores prácticas

4.3.1.3.1. Crear una política de cortafuegos

La política de cortafuegos define cómo se debe manejar el tráfico de red entrante y saliente dependiendo de direcciones IP y rangos de direcciones, protocolos o aplicaciones basadas en tipos de contenido. Se debe realizar un análisis de riesgos para desarrollar una lista de los tipos de tráfico necesarios para la organización y cómo han de ser configurados, incluyendo qué tipo de tráfico puede atravesar un cortafuegos y en qué circunstancias. En general, todo el tráfico entrante y saliente que no esté expresamente permitido por la política de cortafuegos debe ser bloqueado porque no es necesario para la organización. Esta práctica reduce el riesgo de

ataque y también puede disminuir el volumen de tráfico sobre las redes de la organización. Existen varios tipos de configuraciones de cortafuegos:

- Cortafuegos de filtrado de paquetes. Operan a nivel de red (capa 3 del modelo OSI) y utiliza un criterio de filtrado para decidir si permite o deniega la entrada de paquetes a la red local. El filtrado puede hacerse según la IP de origen, IP de destino y los protocolos de Internet del paquete.

- Cortafuegos de inspección de estados. Estos cortafuegos almacenan y retienen la información de un paquete entrante en una tabla dinámica de estado de memoria. Estas tablas almacenan la información sobre el origen y el destino de la conexión asociada al paquete y determinan si la comunicación debe ser admitida según unas reglas.

- Cortafuegos Proxy. Este tipo de firewall opera a nivel de aplicación (capa 7 del modelo OSI). La definición general de la palabra proxy (en inglés) es la de representante, es decir, una persona autorizada a actuar por otra. El software proxy se puede situar entre un usuario y un servidor para ocultar la identidad del usuario, así el servidor ve el proxy y no puede identificar al usuario. También puede ser en el caso contrario, donde el usuario interactúe con el software proxy y no pueda identificar el servidor o su red asociada. Un firewall proxy es efectivo como escudo de otra red exterior no segura.

4.3.1.3.2. Identificar requisitos

Las organizaciones necesitan determinar qué áreas de la red deben ser protegidas y qué tipos de tecnologías de cortafuegos serán más eficaces para los tipos de tráfico que requieren protección. Existen consideraciones de rendimiento importantes así como los requisitos con respecto a la integración del cortafuegos en la red existente y en las infraestructuras de seguridad. Además es necesario dimensionar correctamente el cortafuegos que se va a implementar teniendo en consideración posibles necesidades futuras o posibles actualizaciones y nuevas tecnologías.

4.3.1.3.3. Gestionar la arquitectura

Hay muchos aspectos en la administración del cortafuegos, por ejemplo, elegir entre diferentes tipos de topologías pueden afectar significativamente a la de seguridad que el cortafuegos puede aplicar. Existen diferentes tipos de topologías y segmentaciones de red, y el motivo de segmentar una red es concretamente aislar el tráfico entre redes. Si la red no se segmenta, una vez que un atacante se encuentre dentro de la red, no tendrá muchas dificultades para acceder a los sistemas de control.

Los cortafuegos se pueden usar para crear arquitecturas de redes de seguridad efectivas. Estas arquitecturas se basan en el concepto de zona desmilitarizada o DMZ (Demilitarized zone). Una DMZ es una región que crea una separación entre una red externa o pública y otra interna o privada. Existen muchas arquitecturas que usan DMZs, pero existen dos en concreto que son especialmente efectivas:

- DMZ con un cortafuegos. En este caso se usa un cortafuegos para filtrar paquetes entre la red de empresa, por ejemplo, y la red local de control. La DMZ contiene los elementos a los que los ordenadores de empresa tienen que acceder, así como la

conexión hacia la red pública externa.
Como entre la DMZ y la red de control no existe ningún firewall, esta red puede ser vulnerable si la DMZ es penetrada con un ataque externo o de la propia red de empresa.

- DMZ de doble cortafuegos. La seguridad de la red se puede aumentar añadiendo un segundo firewall entre la red de control y la DMZ.

4.3.2. Auditoría

4.3.2.1. Objetivos

Una auditoría es el conjunto de actividades encaminadas a analizar una organización y realizar propuestas de mejora. El conjunto de actividades se denomina proceso de auditoría y el resultado, informe de auditoría o, simplemente, auditoría.

El objetivo puede ser descubrir las causas de las anomalías en el funcionamiento de la organización o la verificación de las presuntas causas, es decir, qué es lo que se está haciendo mal, o mejorar el funcionamiento para ser más eficaces y/o eficientes y a su vez más competitivos, es decir, cómo se puede mejorar.

4.3.2.2. Descripción

Existen múltiples tipos de auditorías en función de cuales sean sus objetivos y alcance, no obstante se pueden agrupar en dos grandes tipos. El primer tipo de auditorías son las llamadas **auditorías de conformidad** o auditorías de cumplimiento, que partiendo de un modelo o modelos acordados, evalúan si los procedimientos definidos en una empresa se adecuan a ella, y si los empleados siguen los procesos tal como están definidos. En el informe final de estas auditorías aparecen los llamados incumplimientos o disconformidades que, en caso de ser importantes, deberán ser solucionados antes de poder obtener la acreditación/certificación correspondiente, si éste es el objetivo de la auditoría.

El segundo tipo son las que se denominan **auditorías de mejora**, suele dividirse en dos etapas, una inicial donde se determina el estado actual de la organización y otra en la que habrá que definir el objetivo a conseguir. En estas auditorías puede ser de gran utilidad el disponer de empresas modelo. En el informe final se debe incluir los puntos fuertes y débiles detectados, las acciones que hay que emprender y, sobre todo, el sistema de seguimiento y evaluación de su rendimiento.

Por otro lado, se pueden clasificar las auditorías en base a otros múltiples criterios, como por ejemplo, según **su autoría**, obteniendo así la siguiente clasificación:

- Auditoría externa: llevada a cabo por auditores externos a la empresa auditada. La auditoría externa la puede realizar un cliente o elaborarse a petición suya (auditorías de segunda parte), o puede ser llevada a cabo por un organismo independiente homologado para obtener una certificación (este tipo de auditorías se conocen como auditorías de tercera parte).

- Auditoría interna: llevada a cabo por auditores de la empresa auditada, también se denominan de primera parte. Cuando las auditorías son ejecutadas por la propia empresa pero por un departamento diferente al auditado reciben el nombre de auditoría ajena al departamento, es común en empresas con numerosos departamentos donde existe uno de ellos dedicado exclusivamente a labores de auditoría, aunque no tiene por qué ser necesariamente así.

- Auditoría mixta. La llevan a cabo auditores externos que guían la auditoría y auditores internos que realizan funciones que no comprometan la calidad y que respetan el principio de independencia en relación con el área auditada

Podemos diferenciar los siguientes tipos en función de la parte de la empresa que es **objeto de la auditoría**:

- Totales: El alcance de la auditoría abarca toda la empresa

- Parciales: El alcance de la auditoría abarca uno o varios departamentos de la empresa pero no la totalidad de la misma.

En cuanto a la **temporalidad**, nos encontramos con los siguientes tipos:

- Periódica: dentro del plan de auditorías de la empresa, pueden estar contempladas como auditorías periódicas.

- Planificada: el plan de auditorías de la empresa puede prever la realización de auditorías para, por ejemplo, verificar que unas acciones de mejora se han cumplido.

- Puntual: este tipo de auditoría es llevada a cabo cuando se han detectado anomalías en la organización y no es posible determinar sus causas.

4.3.2.3. Mejores prácticas

Con el fin de obtener los mejores resultados en la realización de auditorías en base a los objetivos y alcance definidos, las mejores prácticas recomiendan que todo el proceso de auditoría se estructure como un proyecto en sentido amplio y, como tal, lo primero que necesita es una planificación adecuada y detallada. De forma general, se podría dividir la tarea de auditoría en las siguientes etapas:

- Inicio de la auditoría.

- Revisión de la documentación.

- Planificación.

- Desarrollo del plan de auditoría.

- Reunión de cierre de auditoría.

- Informe de auditoría.

- Seguimiento.

En los siguientes apartados se analizarán en más detalle los objetivos y finalidad de cada una de estas fases.

4.3.2.3.1. Inicio de la auditoría

Una vez se haya recibido el encargo de llevar a cabo una auditoría o simplemente se haya decidido internamente llevarla a cabo, se procederá a designar al líder del equipo de auditoría y definir el sujeto, los objetivos, el alcance y los criterios que aunque podría estar definido previamente, es conveniente detallarlo junto con el líder del equipo de auditoría.

En este punto, es necesario determinar la **viabilidad** de la auditoría, partiendo de criterios como la disponibilidad de información suficiente y apropiada para planificarla, la cooperación de los auditados, tiempo y recursos disponibles, etc.

Una vez solicitada la ejecución de una auditoría, y teniendo en cuenta el amplio abanico tipológico que incluye el concepto, es imprescindible la confección de un **contrato de auditoría** en el que se especificarán claramente al menos los siguientes elementos:

- El sujeto de la auditoría.
- Los objetivos o requisitos de la auditoría.
- El alcance.
- Los recursos destinados por equipo auditor y ente auditado, incluyendo recursos personales y materiales.
- Las responsabilidades de ambas partes.
- Los tiempos en la ejecución de la auditoría y los requisitos de tiempo que la empresa deberá tener en cuenta en cuanto a dedicación de los empleados para atender al equipo auditor, preparación de la documentación necesaria, etc.).

Uno de los aspectos más complejos en la planificación del sistema de auditorías es el de determinar su **alcance**.

La auditoría se debe plantear como un ejercicio de análisis del sistema para verificar su funcionamiento correcto y detectar sus puntos débiles con el fin de anularlos o encontrar sistemas alternativos que los mejoren.

Puede ocurrir que en el transcurso de una de auditoría se detecten puntos débiles del sistema que se encuentren fuera del alcance o de los objetivos de la misma. En dichos casos, las debilidades encontradas no formarán parte de la auditoría en cuestión, pero se informará de ello el auditado para que pueda tomar las medidas necesarias.

4.3.2.3.2. Revisión de la documentación

En esta etapa se debe analizar la documentación existente en la organización con el fin de orientar la auditoría y conseguir un conocimiento profundo de las prácticas existentes y los

objetivos de negocio. Este primer análisis, además, permitirá realizar una correcta planificación de la auditoría, y ayudará a identificar la normativa aplicable y si el cumplimiento de las políticas corporativas es adecuado. Así mismo, esta inspección inicial de la documentación, debe ayudar a determinar el tamaño y la composición del equipo auditor, así como las herramientas/técnicas que se podrán utilizar en caso de ser necesario.

Entre la documentación que debe incluirse en el análisis se pueden incluir los estándares que sigue la organización, políticas internas, planes estratégicos y de negocio, organigrama de la organización, etc.

Si alguna documentación necesaria no está disponible, se podría suspender la auditoría por falta de viabilidad.

4.3.2.3.3. Planificación

Como mínimo, antes de iniciar el proceso de realización de la auditoría es necesario preparar el plan de auditoría, asignar las tareas al equipo auditor y preparar los documentos de trabajo.

La planificación de la auditoria ha de hacerse **basada en el riesgo**. Mediante un análisis de los activos críticos de la organización es posible determinar cuáles son los riesgos potenciales lo que permitirá orientarla de una forma más efectiva focalizando los esfuerzos en los puntos más importantes. Este enfoque ayudará eficientemente al auditor a determinar la naturaleza y la extensión de las pruebas puesto que al entender la naturaleza del negocio se pueden identificar y clarificar los tipos de riesgo que determinarán mejor el enfoque de la auditoría.

Las pruebas que se deben realizar de los controles pueden ser de **cumplimiento** las cuales verifican la existencia y aplicación del control, o **sustantivas** que comprueban resultados de esta existencia y aplicación.

El **plan de auditoría** debe ser consensuado y aceptado por todas las partes antes de iniciar la realización de la auditoría, contendrá el detalle necesario para poder realizar la auditoría y tendrá en cuenta el alcance y la complejidad de ésta y ha de ser lo suficientemente flexible como para admitir cambios del planteamiento inicial surgidos durante su realización. El plan de auditoría debería contener, como mínimo, los siguientes puntos:

- Los objetivos de la auditoría.
- Los criterios de la auditoría y los documentos de referencia.
- El alcance, incluyendo la identificación de las unidades organizativas y funcionales, y los procesos que se auditarán.
- El calendario con las fechas y lugares previstos para la realización de cada una de las actividades de que se compone la auditoría.
- La hora en la que se realizará y la duración de cada una de las actividades de auditoría, incluyendo todo tipo de reuniones con la dirección y el equipo auditor.
- Las funciones y responsabilidades del equipo auditor y sus acompañantes, si son necesarias.

- La asignación de los recursos necesarios para realizar la auditoría, incluyendo la disponibilidad de los entrevistados, la disponibilidad de acceso a los sistemas, el permiso de acceso a los sistemas, los permisos de instalación de software y hardware de monitorización, etc.

Esto se puede completar con información sobre los temas que se deben tratar en el informe de auditoría, aspectos logísticos como viajes, salas de reuniones, equipamiento de trabajo, etc. Es importante también tratar en este punto todos los temas relacionados con la confidencialidad.

Organización de la inspección

Es responsabilidad del líder del equipo auditor asignar a cada miembro del equipo la responsabilidad de auditar procesos, funciones, lugares, áreas o actividades específicas, utilizando las técnicas y herramientas descritas en la planificación. La asignación se hará según la capacitación e independencia del auditor prestando especial atención al coste y el tiempo.

Los miembros del equipo se comunicarán entre sí de forma periódica, para evaluar el progreso de la auditoría y establecerá, además, un método fluido de trabajo con el ente auditado. Éste puede facilitar personas para asistir al equipo auditor en cuestiones como establecer contactos, el horario de las entrevistas, acordar las visitas a partes específicas de las instalaciones o de la organización, comprobar que la normativa en lo referente a la protección y seguridad de las instalaciones es conocida y respetada por el equipo auditor y también proporcionar las aclaraciones o ayudas necesarias en la recopilación de la información.

Debe existir un medio para **comunicar inmediatamente** al organismo auditado aquellas evidencias recopiladas que supongan un riesgo inmediato y significativo (temas de seguridad, medio ambiente o calidad), o en el caso de ser necesarios cambios (en el plan, el alcance u otros), para que haya evidencias registradas en el proceso de auditoría que indiquen que los objetivos de la auditoría no son asequibles.

Preparación de los documentos de trabajo

Una vez asignadas las actividades al equipo auditor, a partir de la revisión de la información disponible de las actividades asignadas, se procederá a preparar los documentos de trabajo necesarios, tanto los de referencia (por ejemplo, listas de verificación) como los de registro (por ejemplo, formularios).

Todos estos documentos se deberán guardar como mínimo hasta que finalice la auditoría. Su conservación, una vez que ha acabado la auditoría, se decidirá de mutuo acuerdo según su posible utilización posterior (estar dentro de un plan de auditorías), o por requisitos legales.

Los documentos que contengan información confidencial o de propiedad privada, deberán ser almacenados con la seguridad acordada.

4.3.2.3.4. Desarrollo del plan de auditoría

El desarrollo del plan de auditoría puede ser considerado el proceso de auditoría en sí mismo, ya que es donde se realiza la captura de la información para ser analizada posteriormente y ser presentada en el informe de auditoría.

Esta parte se inicia con una reunión de apertura o de inicio de la auditoría del equipo auditor con el ente auditado o los máximos responsables de éste.

Durante la auditoría se procede a la recopilación y verificación de la información.

Si el alcance y el ámbito de la auditoría son muy extensos, es posible que sea necesario utilizar técnicas estadísticas de muestreo para la recopilación de la información. Se debe verificar cualquier información obtenida para que pueda constituir evidencia de la auditoría. Si se utilizan técnicas estadísticas de muestreo, debe quedar constancia en las conclusiones de la auditoría del grado de incertidumbre que incorporan y, en consecuencia, de los riesgos asumidos por la auditoría.

Los hallazgos de auditoría pueden indicar tanto conformidad como no conformidad con los criterios de auditoría, o cuando éstas así lo especifiquen pueden identificar un proceso de mejora. Las no conformidades se pueden clasificar según su importancia. Es importante que las no conformidades estén lo suficientemente detalladas para que el ente auditado las comprenda perfectamente. Si no se consigue acuerdo en algún punto, debe constar como tal en el registro de la realización de la auditoría.

Antes de la reunión de cierre de la auditoría el equipo auditor deberá preparar las conclusiones conjuntamente. En esta reunión se revisarán los hallazgos y la información relacionada, se acordarán las conclusiones de auditoría y la incertidumbre asociada al proceso, se prepararán las recomendaciones y se comentarán las funciones de seguimiento de la auditoría, si las hay.

4.3.2.3.5. Reunión de cierre de auditoría

En la reunión de cierre de auditoría se presentarán los hallazgos y las conclusiones de la auditoría de manera que sean comprendidas y reconocidas por el auditado.

En el caso de no conformidad, en un período de tiempo acordado, el ente auditado presentará un plan de acciones correctivas y preventivas. En el caso de auditoría de mejora, se planificará la incorporación de las mejoras propuestas.

Esta reunión es previa a la elaboración definitiva y a la entrega del informe de auditoría con el fin de llegar a un acuerdo sobre su contenido. Se intentarán resolver las opiniones divergentes y en caso de no conseguirlo, deberá quedar constancia de esta situación.

4.3.2.3.6. Informe de auditoría

El resultado propio del proceso de auditoría es el informe de auditoría, que ha de ser un registro preciso, conciso, claro y completo de ésta. Debe hacer referencia a los siguientes puntos:

- Los objetivos.
- El alcance. En particular la identificación de las unidades de la organización y de las unidades funcionales o los procesos auditados y el intervalo de tiempo cubierto.
- La identificación del patrocinador de la auditoría.
- La identificación del equipo auditor y su líder.

- Calendario (fechas) y lugares donde se realizaron las actividades de la auditoría.
- Criterios de la auditoría.
- Hallazgos
- Conclusiones de la auditoría.
- Recomendaciones, si las hay, de la auditoría.

Según el ámbito y la complejidad de la auditoría, se puede hacer referencia también a:

- Plan de auditoría.
- Resumen del proceso/actividades de la auditoría, incluyendo la incertidumbre y/o cualquier obstáculo que pudiera disminuir la confianza en los resultados de la auditoría.
- La confirmación de que se han alcanzado o no, y en qué grado, sus objetivos.
- Áreas no cubiertas pro incluidas en el alcance de la auditoría.
- Plan de seguimiento, en el caso de existir.
- Una declaración sobre la naturaleza confidencial de los contenidos.
- La lista de distribución del informe de auditoría.

El informe de auditoría se deberá emitir en el período de tiempo acordado en la planificación. Por otra parte, estará fechado, revisado y se hará una presentación formal en la que se obtendrá la aprobación de acuerdo con los procedimientos preestablecidos. En esta presentación se ofrecerán las conclusiones y se recalcarán las propuestas/recomendaciones de mejora. Finalmente, se procederá a la distribución de los ejemplares del informe de auditoría según la lista de distribución acordada.

4.3.2.3.7. Seguimiento

Si la auditoría indica la necesidad de acciones correctivas, preventivas o de mejora que debe poner en marcha el ente auditado en un período de tiempo acordado, hay que a establecer un sistema de seguimiento de estas acciones, aunque conviene tener presente que estas acciones no se consideran parte de la auditoría.

El ente auditado deberá informar del progreso de estas acciones, se deberá verificar el inicio de cada acción y su eficacia que podrá hacerse mediante una auditoría posterior.

4.3.2.3.8. Perfil del auditor

Un auditor genera, ejecuta y controla todo el proceso de auditoría lo que requiere un conjunto de capacidades, habilidades, conocimientos, experiencia y rasgos personales para realizar su función.

La correcta formación académica de los auditores servirá para proporcionar una base de conocimientos técnicos que permitirá llevar a cabo los procesos de auditoría de mejor forma y

de un modo más amplio obteniendo unos mejores resultados. También es necesaria una formación específica en el proceso de auditoría, así como en las técnicas y herramientas utilizadas.

La experiencia profesional en auditoría favorece la interacción con el auditado y es una base para poder descubrir las deficiencias/incumplimientos y proponer acciones de mejora.

Teniendo en cuenta que las técnicas de auditoría a las cuales se recurre más, por ser más efectivas, son la entrevista y la encuesta, y que en ellas se interacciona con otros individuos, el auditor debe tener una serie de capacidades/habilidades personales entre las que destacan las siguientes:

- Ética. La actuación del auditor debe ser imparcial, sincera, honesta y discreta.
- Mentalidad abierta. La mejora procederá, en gran medida, de la creatividad, y eso obliga a estar dispuesto a considerar ideas o puntos de vista alternativos a los planteados hasta hoy.
- Diplomático. Es necesario saber interaccionar con cada uno de los interlocutores de la manera adecuada.
- Observador. Debe poder descubrir las actividades y su entorno, tanto si están planteadas de manera explícita como implícita.
- Perceptivo. No sólo debe detectar las actividades y su entorno, sino también la situación anímica y el carácter del auditado para poder entender las distintas situaciones.
- Versátil. Pese a la planificación, hay situaciones no previstas que requieren una gran adaptabilidad.
- Tenaz. La obtención de los objetivos de la auditoría puede ser una tarea ardua y, por lo tanto, la perseverancia será una virtud primordial.
- Analítico. La información obtenida por él mismo no es útil a menos que se extraigan las conclusiones oportunas basadas en análisis y razonamientos lógicos.
- Seguro de él mismo. Se debe actuar de manera independiente, ajena a las posibles presiones externas a los objetivos de la auditoría.

El auditor que dirige el equipo de auditoría, el líder del equipo auditor, debe adquirir experiencia adicional para desarrollar sus funciones. Naturalmente, esta experiencia como líder de un equipo auditor sólo la podrá adquirir bajo la tutela y orientación de un auditor calificado como líder.

4.3.2.4. Herramientas y ejemplos

4.3.2.4.1. Cuestionarios

Los cuestionarios deben descubrir aquellos aspectos que servirán de guía en las actuaciones posteriores de la auditoría. Se solicita que se rellenen unos cuestionarios a diferentes

personas, incluyendo todo el rango de categorías laborales. Los cuestionarios se deben generar con mucho cuidado en fondo y forma, y deben ser específicos para cada instalación.

4.3.2.4.2. Estándares

Para llevar a cabo una auditoría es imprescindible tener una buena base de estándares como marco de comparación y determinación de las buenas prácticas del auditado. Pudiendo éstos ser utilizados desde dos puntos de vista:

- Como base de referencia de las buenas prácticas o del cumplimiento normativo o legislativo.
- Como base de referencia para la obtención de una certificación, por ejemplo la basada en ISO 9000/2005.

4.3.2.4.3. Entrevistas

Es una de las actividades primordiales del auditor, permiten obtener mucha información que, adicionalmente, se deberá matizar mediante otras fuentes. Aunque en ocasiones a la entrevista se le pueda atribuir el concepto de interrogatorio, la relación se ha de planteas desde la buena fe de ambas partes.

La acción se desarrolla siguiendo un plan esmeradamente preconcebido para que, bajo la forma de una conversación correcta y con el mínimo posible de tensión, el entrevistado responda con sencillez y claridad a una serie de preguntas simples. Las entrevistas tendrán que ser elaborados para cada caso en particular. Pueden tener diferentes planteamientos:

- Solicitud de información concreta (documentación) responsabilidad del entrevistado.
- Batería de preguntas abiertas para obtener el máximo de información.
- Entrevista con un método preestablecido y unos objetivos claramente definidos.

4.3.2.4.4. Listas de comprobación o checklists

Las checklists, Son listas de preguntas sencillas que se utilizan sistemáticamente en las entrevistas para facilitar el análisis de las respuestas.

Es muy importante y recomendable que el entrevistador memorice las preguntas y no las recite para que la entrevista más coloquial, será más dinámica y evitará posibles reticencias del entrevistado.

Las respuestas de las listas de comprobación pueden ser binarias, únicas, excluyentes (de tipo sí/no) o de rango, con un conjunto de valores de 1 a n que matizan la respuesta

4.3.2.4.5. Matrices de riesgos

Las matrices de riesgos permiten representar de manera muy evidente la combinación de riesgos/amenazas con impactos/repercusiones de un sistema. No se deben omitir de las matrices de riesgos las medidas de cobertura que se pueden utilizar para paliar los riesgos.

En concreto, las matrices de riesgo pueden servir para analizar las amenazas al funcionamiento de los sistemas de información y comunicación, el impacto que pueden producir las amenazas si se materializan, los recursos afectados por el acontecimiento, el impacto de las medidas de cobertura utilizadas, etc.

4.3.2.4.6. Registros de auditoría

Los registros de auditoría se pueden utilizar, para constatar que se han llevado a cabo las validaciones de datos previstos o para verificar que los programas realizan las funciones encomendadas: una de las funciones de la gestión de la configuración es la trazabilidad de los cambios para su seguimiento posterior.

Últimamente han adquirido relevancia los registros de los servidores web, tanto por motivos legales como impone la LSSICE a los ISP o bien por su utilidad para perfilar el comportamiento de los usuarios. En cualquier caso, la obtención de estos registros se debe realizar de manera no intrusiva, es decir, sin modificar de ninguna manera el sistema.

4.3.2.4.7. Software estadístico

Cuando el volumen de datos que se debe analizar supera el tiempo que se puede dedicar a la auditoría, es necesario utilizar técnicas estadísticas que disminuyan este esfuerzo. Para ello hay aplicaciones que permiten el estudio estadístico de cualquier conjunto de muestras y que incorporan diferentes procedimientos y enfoques para el análisis. Estas herramientas permiten al auditor, además, controlar el grado de confianza del estudio.

4.3.2.4.8. Software de control de proyectos

El éxito de la auditoría reside en gran medida en su correcta planificación. Por ello es tan útil la ocupación de herramientas de control de proyectos que permiten la definición de las tareas, de su precedencia y de los tiempos asignados a cada una, así como la distribución de recursos, la asignación de responsabilidades e incluso la preparación de presupuestos.

En los sistemas de planificación modernos se aprovecha la capacidad de comunicación y de compartir información de las redes para la gestión del proyecto (mediante técnicas de software de grupo o groupware y de ciclo de trabajo o workflow), hecho que permite crear verdaderos sistemas de información de gestión de proyectos.

Estas herramientas no sólo se utilizan inicialmente para planificar y programar actividades, sino que se utilizan también durante y al final del proceso de auditoría, para el seguimiento del proyecto y la evaluación de las desviaciones entre lo que se ha planificado y la realidad.

4.3.2.4.9. Software de consulta

Estas aplicaciones permiten, mediante órdenes con una concepción mucho más sencilla que las de los lenguajes convencionales de programación, seleccionar y elaborar datos de los ficheros convencionales y/o bases de datos. Ejecutan verdaderas funciones de muestreo al azar, selección con criterios, inspección y captura desde fuentes externas. Permiten la realización de estudios estadísticos y la maquetación de informes.

La mayoría de los sistemas de gestión de bases de datos incluyen aplicaciones de este tipo.

4.3.2.4.10. Herramientas de monitorización de sistemas operativos, comunicaciones y bases de datos

Las aplicaciones de monitorización, que pueden ser sólo software, hardware o una combinación de los dos, tienen como objeto la medida real del comportamiento del sistema en la situación y el momento actual.

Este tipo de herramientas suelen estar íntimamente ligados a la instalación donde se ejecutan y al sistema operativo, sistema de comunicaciones y base de datos que miden, como es de esperar, estas herramientas no deben ser intrusivas o al menos serlo lo mínimo posible.

4.3.2.4.11. Técnicas de auditoría asistidas por ordenador

Podemos encontrar paquetes de software de auditoría especializados en auditoría en general o en aspectos concretos de la auditoría, y también en auditorías de sistemas de información. Algunas de estas aplicaciones nacieron en las auditorías financiero-contables.

Entre las técnicas de auditoría asistidas por ordenador, destaca la auditoría de sistemas expertos. Un sistema experto extrae el conocimiento o saber de unos especialistas en una determinada función, en nuestro caso auditoría, y lo conceptualiza y formaliza para poder utilizarlo como una ayuda en esta función, también podemos encontrar técnicas de minería de datos orientados a texto (datos no estructurados) para reconocer riesgos o situaciones similares.

4.3.3. Aseguramiento de equipos

4.3.3.1. Objetivos

En la actualidad es común encontrarse con situaciones en las que tanto servidores, sistemas operativos, aplicaciones o incluso elementos hardware cuentan con configuraciones de fábrica bastante inseguras o servicios que no son necesarios y que pueden, por ejemplo, permitir el acceso remoto a los sistemas. Mediante el bastionado conseguiremos un mejor nivel de seguridad configurando los sistemas/servicios con las opciones y parámetros adecuados.

Este capítulo da a conocer al lector, una serie de pautas y/o procedimientos a seguir en el bastionado de equipos con el fin de reducir la carga administrativa que puede llegar a suponer el proceso de aseguramiento de los mismos para el personal dedicado a su administración.

Los puntos que se mencionarán a continuación no están orientados a ningún sistema concreto por lo que el nivel técnico de las recomendaciones será bajo. Se pretende dar una visión general respecto a las mejores prácticas de bastionado en diferentes tipos de entornos.

4.3.3.2. Descripción

El bastionado de equipos consiste en elevar el nivel de seguridad mediante la implementación de ciertas políticas y controles. Este proceso implica la consideración de una serie de buenas prácticas relativa a diferentes aspectos de la seguridad como por ejemplo el parcheo y actualización de equipos, realización de copias de seguridad, correcta gestión de accesos, etc.

Para mantener dicho nivel, los equipos deberán ser monitorizados y actualizados de forma periódica para evitar que vuelvan a ser vulnerables. . De esta forma, reduciremos el grado de exposición a nuevas vulnerabilidades.

En el siguiente punto veremos un conjunto de buenas prácticas que servirán de ayuda a la hora de definir una política de seguridad completa.

4.3.3.3. Mejores prácticas

A continuación se detallan una serie de puntos que podrán seguirse para mejorar las características en cuanto a seguridad se refiere de los servidores de una organización.

4.3.3.3.1. Permisos

Es importante seguir el principio de privilegios mínimos o 'least privilege', también conocido como 'principle of least authority' o POLA por sus siglas en inglés. Este principio, en líneas generales nos indica que cada proceso, tarea y/o usuario debe disponer únicamente del menor número de privilegios para que pueda llevar a cabo su trabajo de forma correcta. Haciendo uso de este principio, si algún proceso o usuario es comprometido en algún equipo nos podemos asegurar que tendrá un impacto más limitado y sus efectos serán más contenidos que si por ejemplo se usara siempre una cuenta de administrador.

Las organizaciones son entornos cambiantes donde gran cantidad de personal entra y sale. Es común encontrar usuarios pertenecientes a antiguos empleados o listas de acceso desactualizadas. Por ello es importante realizar una revisión periódica de los permisos de los usuarios por parte de los propietarios de la información, así como integrar los procesos de alta y baja de usuarios con los procedimientos de Recursos Humanos para así evitar posibles accesos no deseados, como podría ser el un antiguo empelado descontento. La integración de la autenticación de sistemas y aplicaciones con los repositorios de usuarios centralizados de la organización facilita en gran medida el proceso de alta y baja de usuario, permitiendo la rápida eliminación de cuentas de acceso en todos los sistemas cuando se produce una baja.

4.3.3.3.2. Actualizaciones de software

Es importante contar siempre que sea posible con un entorno de pruebas en el que las nuevas actualizaciones se puedan probar antes de ser aplicadas en un entorno de producción. Así mismo, dichas actuaciones deben ser planificadas en lo que se denominan ventanas de mantenimiento para que cualquier problema que surja durante el proceso suponga un impacto mínimo en los servicios en producción de la organización. No disponer de un correcto procedimiento de actualización y parcheo de equipos podría llevar a que dichas actividades se descuiden por el miedo a posibles fallos en los procesos de actualización, dando lugar a sistemas vulnerables susceptibles de ser objeto de ataque.

No siempre es sencillo mantener un SO actualizado, aunque la mayoría de los sistemas operativos actuales cuentan con mecanismos de notificación de actualizaciones disponibles podemos encontrarnos en ocasiones con situaciones en las que este mecanismo ha sido desactivado. Mantener un entorno actualizado aplicando los diferentes parches o actualizaciones publicados es esencial para mantener los entornos asegurados. Tan importante como mantener el sistema operativo actualizado es mantener todas las aplicaciones y

paquetes software instalado. Dado que no todos los sistemas cuentan con procesos de notificación automática de actualizaciones, el responsable de los mismos deberá realizar las comprobaciones necesarias de forma periódica con el fin de garantizar que efectivamente las últimas versiones se encuentran instaladas. Para ello, el personal de sistemas tendrá que estar suscrito a las fuentes adecuadas y consultarlas con cierta periodicidad para verificar si hay nuevas actualizaciones disponibles.

Sólo se deberán instalar paquetes de fuentes confiables y verificar su integridad tras las descargas si se proporciona un método para ello como puede ser un hash que servirá para evitar problemas a la hora de actualizar debidos a ficheros corruptos

Como ya se ha mencionado anteriormente los procesos de actualización tendrán que hacerse en los momentos que supongan un menor impacto para la organización. Así mismo, las actualizaciones de software pueden llegar a tener tamaños de varios cientos de megas y habrá que considerar que el consumo de ancho de banda necesario en ocasiones será muy elevado por lo que no sólo la aplicación de dichas actualizaciones debe ser planificada sino también su descarga.

Es una buena práctica mantenerse informado de las vulnerabilidades que aparecen para nuestro software, ya que en ocasiones el impacto de muchas de ellas puede ser mitigado mediante la aplicación de unos sencillos pasos, lo que se denomina rodeo (*workaround)*, que proporcionará la seguridad necesaria hasta que la vulnerabilidad sea solucionada en un parche o actualización y probada para verificar su correcto funcionamiento en los entornos de la organización.

4.3.3.3.3. Contraseñas

De nada sirve asegurar un sistema si un usuario con permisos de administrador utiliza una contraseña débil ó fácil de adivinar, por ello hay determinados aspectos que habrá que tener en cuenta a la hora de definir una política adecuada en cuanto a las contraseñas se refiere.

Antigüedad máxima y mínima de contraseñas: es importante definir el tiempo máximo que se permitirá el uso de una contraseña para forzar su cambio cada cierto tiempo al igual que el tiempo mínimo para evitar que tras un cambio, un usuario vuelva a cambiarla por la contraseña que usaba anteriormente.

Longitud mínima y complejidad de la contraseña: para hacer menos probable el éxito de un ataque que intente adivinar una contraseña de un usuario conviene exigir una longitud mínima para la contraseña así como verificar que la complejidad de la misma es también suficiente. Es útil por ejemplo verificar que se están utilizando letras mayúsculas, minúsculas y números, así como que la contraseña no esté basada en una palabra que pueda aparecer en un diccionario.

Histórico de contraseñas: guarda un determinado número de contraseñas antiguas para que no se repitan y no puedan ser reutilizadas.

Algoritmo de cifrado: las contraseñas nunca deberán ser almacenadas en claro en los servidores, tendrán que ser cifradas previamente empleando un algoritmo de hash o cifrado fuerte que no permita la obtención de una manera sencilla o rápida de las contraseñas almacenadas en el caso de que alguien se hiciera con la información de los usuarios.

4.3.3.3.4. Cuentas de usuarios

Multitud de aplicaciones crean usuarios específicos para su correcto funcionamiento, estos usuarios suelen ser configurados con contraseñas por defecto que son ampliamente conocidas, por lo que hay que evitar siempre las configuraciones de fábrica, y eliminar o modificar las contraseñas por defecto con el fin de evitar accesos no autorizados a los sistemas, para evitar esto se debería definir un periodo de inactividad tras el cual las cuenta afectada quedaría deshabilitadas y sólo podrá ser desbloqueada por el responsable al cargo. En la misma línea, se deberían llevar un seguimiento de las cuentas inactivas para conocer el motivo de por qué se encuentran así y eliminándola si procede.

Es preferible asignar permisos a grupos de usuarios y posteriormente asignar los usuarios a los grupos que hayan sido definidos, esto facilitará la gestión y la trazabilidad de los permisos, una correcta configuración en ese aspecto mejorará la seguridad de los sistemas.

4.3.3.3.5. Permisos de archivos

Al igual que con las cuentas de usuarios debemos asegurarnos de que los permisos que tienen los archivos son gestionados de forma correcta, dando sólo acceso a los usuarios que realmente lo necesiten y siempre que sea posible en el intervalo de tiempo adecuado y de una forma lo más granular posible.

Es común asignar los permisos por directorios en lugar de por archivos concretos, esta es una práctica que puede simplificar el la gestión de los mismo, pero que puede acarrear problemas si la organización de los archivos dentro de los directorios no se lleva a cabo de una forma adecuada.

Si es necesario el uso de carpetas compartidas dentro de la organización su uso deberá estar permitido sólo de forma temporal y asignando permisos únicamente de lectura a usuarios concretos, nunca a grupos.

4.3.3.3.6. Servicios y aplicaciones del sistema

Idealmente un servidor debe tener habilitados sólo aquellos servicios que sean estrictamente necesarios para dar realizar la función para la que han sido concebidos. Durante el proceso de bastionado de un sistema operativo, todos los servicios, aplicaciones o protocolos que no sean necesarios, han de ser eliminados o deshabilitados en el caso de no ser esto posible. Idealmente el punto de partida para la configuración de un nuevo servidor ha de ser una instalación mínima del sistema operativo al que se irán añadiendo los diferentes componentes que sean necesarios, lo que ayudará a tener un control más estricto sobre qué se ejecuta en ese servidor.

Los servicios más habituales que debemos deshabilitar serán aquellos que permitan conexiones remotas contra nuestros servidores, servicios web o de correo electrónico, LDAP, etc. Del mismo modo, cualquier aplicación orientada a desarrolladores como pueden ser compiladores y/o librerías deberían ser eliminadas siempre que no sean necesarios.

Esta práctica mejorará la seguridad de los servidores reduciendo el número de vías por las que pueden ser comprometidos, aumentando su disponibilidad y facilitando su mantenimiento, al hacer un mejor uso de los recursos.

4.3.3.3.7. Registro de eventos del sistema

Los registros pueden ser utilizados no sólo para detectar comportamientos sospechosos y maliciosos e investigar los incidentes de seguridad, sino también para ayudar en la solución de problemas del sistema y problemas de aplicación.

Hay que buscar una configuración equilibrada entre en intervalo de tiempo del que queremos disponer de los registros, el nivel de información y el espacio en disco que queremos que ocupen, estos parámetros variarán según los requisitos de cada organización del mismo modo que las necesidades no serán las mismas para las diferentes aplicaciones. Es necesario tener en cuenta en este punto tanto los requisitos legales como los requisitos de la propia organización.

Centralizar los registros generados en un único servidor, ayudará a su análisis y correlación. De forma adicional en el caso de que algún servidor sea comprometido, los registros permanecerán a salvo. Los registros pueden contener información sensible y el envío ha de hacerse siempre que sea necesario usando un canal de comunicaciones cifrado.

Los registros de auditoría son de vital importancia en el caso de que se produzca un incidente de seguridad por este motivo habrá que protegerlos de forma adecuada, permitiendo su acceso sólo a superusuarios y registrando cualquier actividad que se lleva a cabo sobre ellos.

Análisis de registros

Es habitual que el volumen de registros generados por los servidores de una organización sea muy elevando llegando a hacer de su análisis algo inviable. Idealmente el análisis de los archivos de registros ha de hacerse de manera automatizada, avisando al responsable que proceda en el caso de detectar comportamientos anómalos o sospechosos.

Es este caso es especialmente útil contar con un sistema centralizado de correlación de eventos. Esto permite un análisis más detallado de las diferentes alertas y pudiendo contrastar la información en diferentes lugares permitiendo reducir de esta forma los falsos positivos y/o falsos negativos.

4.3.3.3.8. Copias de seguridad

Las copias de seguridad son un recurso esencial para garantizar la continuidad de las actividades críticas de la organización. Por lo tanto, la estrategia de realización de copias de seguridad deberá ser consistente con las necesidades de recuperación de cada servidor y/o aplicación y deberá ser analizada en detalle.

La periodicidad de las copias de seguridad ha de ser tal que garanticen una ventana de recuperación aceptable consiguiendo que el consumo de espacio de almacenamiento se mantenga en unos niveles aceptables, algo a tener muy en cuenta puesto que las copias de seguridad suponen un consumo de espacio considerable.

Cada cierto tiempo, debe verificarse que las copias de seguridad pueden ser restauradas sin problemas. Almacenar las copias de seguridad de un sistema y que estas estén corruptas o que se estén respaldando los ficheros incorrectos supondría un gran problema en el caso de que las copias de seguridad sean necesarias.

Es igual de importante contar con procedimientos que se ocupen de la copia de seguridad al igual que del proceso de recuperación y de la protección y el almacenamiento de los dispositivos de copia de seguridad y/o discos de recuperación. Es habitual que las copias de seguridad contengan datos confidenciales del usuario como por ejemplo contraseñas, por ello los dispositivos de copia de seguridad deben estar debidamente protegidos para evitar accesos no autorizados

4.3.3.3.9. Auditorías periódicas

El mundo de la seguridad informática es un entorno dinámico con una frecuencia de cambio muy elevada.

Cualquier sistema que haya sido asegurado ha de ser auditado con cierta periodicidad para verificar que los requisitos impuestos en el momento del aseguramiento se siguen cumpliendo.

Según el punto de vista que se adopte a la hora de llevar a cabo la auditoría, podremos distinguir las auditorías de caja blanca y las de caja negra.

En una auditoría de **caja blanca** el auditor tiene conocimientos detallados sobre el sistema que se está auditando. Gracias este enfoque es posible alcanzar un detalle y profundidad que no podría obtenerse mediante en enfoque de caja negra.

Las auditorías de **caja negra** tienen un punto de vista externo del sistema, sin conocimientos detallados de lo que se está auditando o lo que es lo mismo sin ningún conocimiento de la infraestructura que se está analizando, el auditor utilizará técnicas pasivas y activas para determinar el tipo de sistema que se audita y descubrir así posibles vulnerabilidades del sistema.

Estos enfoques a la hora de auditar son los más conocidos pero se pueden adoptar puntos de vista derivados de estos como el de la auditoría de **caja gris** donde la información de que dispondremos será estará en un punto medio entre el enfoque de caja negra y caja blanca y la de **doble caja negra** donde el objeto auditado desconoce las pruebas que se llevarán a cabo con el fin de probar su respuesta.

4.3.3.3.10. Cifrado de discos

Las soluciones de cifrado de discos, están principalmente orientadas para el uso en dispositivos portátiles, que son más susceptibles de ser extraviados y/o sustraídos. Es importante conocer que aplicar una solución de este tipo incondicionalmente tendrá un impacto en el desempeño de nuestros equipos puesto que las tareas de cifrado/descifrado son costosas computacionalmente hablando, pero es una práctica necesaria cuando la información que se quiera proteger en los dispositivos pueda contener datos sensibles.

4.3.3.3.11. Cifrado de las comunicaciones

De nada sirve cifrar la información almacenada si posteriormente la enviamos en claro. Hemos de ser consciente de que cualquier canal de comunicaciones es susceptible de ser intervenido por un atacante pudiendo llevar a cabo una escucha en el mismo interceptando la información que pasa por él.

Una comunicación cifrada reduce drásticamente la probabilidad de fuga de información sensible de la organización.

4.3.3.3.12. Servidores de prueba o preproducción

Los servidores de prueba han de replicar idealmente a su homólogo de forma idéntica en cuanto a hardware/software se refiere, este es el escenario ideal, aunque en la práctica no siempre es así.

Un servidor de prueba nos proporciona un entorno donde probar nuevas actualizaciones o parches para nuestras aplicaciones de una forma segura o probar nuevas configuraciones sin que pueda tener repercusiones graves en los procesos de la organización. Otro uso muy común para este tipo de servidores es como plataforma de desarrollo para el despliegue de nuevos contenidos y aplicaciones. Un nuevo desarrollo puede ser publicado inicialmente en un entorno de pruebas donde podrá verificarse su correcto funcionamiento y efectuar las pruebas que se crean necesarias sin que tenga repercusiones en los servicios que estén en producción.

4.3.3.3.13. Otras recomendaciones

Al igual que con los permisos, debemos tratar que los recursos de que dispone un servidor sean los mínimos, pero suficientes para su correcto funcionamiento.

Si hablamos de un servidor de correo por ejemplo, es interesante limitar el tamaño máximo de archivo que se permite como adjunto, al igual que el tamaño máximo de todos las adjuntos que se envíen, extensiones permitidas, destinatarios, etc. En la misma línea pero hablando de aplicaciones web, tendremos que controlar parámetros similares si mediante formularios se permite a los usuarios subir archivos a nuestro servidor.

4.3.3.4. Herramientas y ejemplos

En la mayoría de las situaciones las herramientas necesarias para asegurar los servidores estarán proporcionadas por el propio sistema operativo o los distintos servicios que se encuentren en nuestro servidor, solo será necesaria una correcta configuración de los mismos para que el nivel de seguridad obtenido sea el necesario. Así por ejemplo es habitual encontrarnos sistemas de notificación de actualizaciones que nos ayudarán a mantener los sistemas actualizados pero deberemos contar en la mayoría de las ocasiones con sistemas que nos permitan monitorizar a ser posible de una forma centralizada las aplicaciones instaladas y si éstas se encuentran o no actualizadas.

Los **permisos** de usuario, grupos y/o archivos podrán ser gestionados mediante cualquier sistema operativo actual, si bien es posible recurrir a herramientas que faciliten la aplicación de los mismos.

La mayoría de los paquetes de software que existen actualmente cuentan con un **sistema de actualizaciones automáticas** que periódicamente revisa si existe una nueva versión del software que tenemos instalado dando incluso la posibilidad de hacerlo todo el proceso de forma desatendida y sin intervención por parte del usuario. Si bien esta práctica no es aconsejada por los motivos que se han visto anteriormente (pruebas, consumo de ancho de

banda, etc.) lo que sí puede servir para estar informados son los sistemas de notificación por lo que no deberemos prescindir de ellos.

Uno de los aspectos más importante en cuanto a la seguridad de los servidores se refiere es el de las **copias de seguridad** ya que nos permitirán restaurar nuestros equipos a un estado previo en caso de accidente. Hay tres formas básicas de llevar a cabo una copia de seguridad: completa, incremental y diferencial. Las copias de seguridad completas se utilizan para hacer una copia de respaldo del contenido completo de una unidad de disco, directorios y/o archivos individuales, pueden contener una copia completa del sistema operativo y las aplicaciones que en él se ejecutan o simplemente de una serie de archivos o directorios que se especifiquen. La principal ventaja de este tipo de copias de seguridad es que son sencillas de restaurar pero la desventaja es que supone mucho tiempo el crearlos y el espacio que ocupan es considerable. Las copias de seguridad incrementales, sólo guardan los cambios que se han producido desde la copia de seguridad anterior, reduciendo de forma considerable el tamaño de los mismos, pero por el contrario, es necesario restaurar múltiples copias de seguridad en caso de que haya que recuperar información

Las copias de seguridad diferenciales, son similares a las incrementales, pero guardan las diferencias que se han producido con relación a la anterior copia de seguridad completa. Para conseguir una solución equilibrada es ente aspecto la copias incrementales o diferenciales se hacen usualmente de forma diaria mientras que las completas, siguen una frecuencia menor, por ejemplo cada mes o cada semana.

Algunas medidas de protección como el **cifrado de discos** suponen una fuerte penalización en el rendimiento de los sistemas ya que las operaciones de cifrado descifrado tienen un coste computacional elevado, como en la mayoría de las situaciones se debe buscar una solución equilibrada que satisfaga las necesidades de seguridad. No es una buena solución utilizar un sistema de cifrado de disco completo (*Full Disc Encryption* o FDE por sus siglas en inglés) si lo que se quiere es proteger sólo unos pocos archivos, en este caso sería mejor optar por otro tipo de soluciones como por ejemplo la creación de una partición de menor tamaño cifrada para guardar toda la información importante; del mismo modo no debería usarse esta solución si el servidor donde se aplica requiere que la partición cifrada se encuentre siempre montada. Como ya se mencionó anteriormente esta medida se seguridad es especialmente útil en equipo portátiles o móviles que puedan extraviarse con facilidad.

4.3.4. Control de accesos y autenticación fuerte

4.3.4.1. Objetivos

En general estos controles se refieren al acceso lógico de los usuarios a la información o de procesos de los sistemas de Información; los controles de acceso físico suelen tratarse en otros apartados.

El objetivo reside en prevenir accesos no autorizados. Por lo que no sólo se debe considerar el hecho de permitir o no el acceso a la información, servicios o recursos, sino también controlar a cuales y con qué nivel de privilegios. Lo más seguro es siempre posicionarse en un criterio de

mínimos, esto es, cuanto menor es el número de accesos, privilegios y activos de información, recursos o servicios a los que se permite acceder… mejor.

4.3.4.2. Descripción

Los controles de acceso lógicos ofrecen un medio técnico de controlar que información pueden utilizar los usuarios, los programas que puede ejecutar, y las modificaciones que pueden hacer.

Durante el proceso del acceso existe un orden implícito: autenticación, autorización y acceso.

El término "**acceso**" se confunde a menudo con **autorización** y **autenticación**.

El **acceso** es la capacidad de hacer algo con un de recursos del ordenador. Se refiere en general a una capacidad técnica (por ejemplo, leer, crear, modificar o eliminar un archivo, ejecutar un programa, o el uso externo de conexión).

La **autorización** es el permiso para usar una computadora de recursos. Se concede el permiso, directa o indirectamente, por el propietario de la aplicación o sistema. El proceso de autorización en el acceso lógico a la información, es la verificación de que una persona conocida (**autenticada**) tiene la autoridad para **acceder** al sistema y para realizar la acción solicitada (login, lectura de un fichero, acceso a un dispositivo o recurso…).

La **autenticación** (o **acreditación**) es demostrar (en un grado razonable) que la entidad que solicita la conexión es quien dice ser.

Así que uno de los puntos clave del control de acceso reside en la autenticación ya que una vez que se ha preconfigurado en el sistema una autorización con un cierto nivel de acceso para una identidad, resulta crucial poder garantizar que la “entidad” (usuario humano, aplicación o un equipo) es correctamente identificada.

Los medios por los que una persona se autentica pueden involucrar uno, dos o tres factores, así que los sistemas de autenticación se suelen categorizar por el número de factores que incorporan.

Los tipos de factores (en sentido creciente de nivel de confianza) son:

- Algo que sabes (un PIN, una contraseña, una frase…)
- Algo que tienes (una tarjeta de banda magnética, una SmartCard, un token…)
- Algo que eres; algún aspecto de tu persona (mediante la utilización de dispositivos biométricos: reconocimiento del Iris o huella dactilar…).

Y además las combinaciones de ellas; de modo que, a mayor combinación de factores mayor seguridad y complejidad.

Típicamente una autenticación de dos factores es la que involucra algo que se tiene y algo que se sabe.

La elección de las diferentes tecnologías del mecanismo de autenticación debe ser elegida en función de la criticidad del sistema o información y del riesgo que representaría para la organización la materialización de una amenaza. Por lo que para ello, es necesario tener una clasificación del sistema y de su información que refleje la sensibilidad, un análisis de riesgos y un mapeo que identifique dicho riesgo con nivel de seguridad requerido. De esta forma, se pueden determinar los requerimientos técnicos mínimos de seguridad para cada nivel y así se podrán elegir medidas de seguridad adecuadas según el principio de proporcionalidad.

A continuación se van a comentar los controles relativos a Control de Acceso para los estándares, guías o normativas más relevantes, así como las equivalencias entre ellos.

Finalmente se darán unas tablas de correspondencia de controles entre los distintos estándares y guías de seguridad aquí considerados.

4.3.4.3. Medidas de seguridad generales

4.3.4.3.1. Consideración de los requisitos de negocio

Es el negocio, en base a sus necesidades y criticidad de sus sistemas, el que debe marcar los requisitos de seguridad y de control para el acceso a su información, recursos y procesos.

Para ello se debe crear y difundir una **Política de control de acceso** documentada en la que se establezcan claramente los derechos y reglas a seguir en cuanto al control de acceso tanto físico como lógico.

En esta política es necesario que se consideren asuntos como: los criterios para la difusión y acceso a la información en base a su clasificación; la consistencia entre el control y el nivel de clasificación de la información; los requisitos para la autorización, revisión y retirada de los controles de acceso; la normalización de los perfiles de acceso; la segregación de funciones en la gestión del control de acceso; la legislación aplicable y obligaciones contractuales, …

4.3.4.3.2. Gestión de los accesos de los usuarios

Los accesos de los usuarios deben gestionarse correctamente controlando la localización de los derechos de acceso y cubriendo todas las fases del ciclo de vida del acceso de usuario (con especial cuidado de los privilegios que pudieran permitir invalidar los controles del sistema) para asegurar el acceso de un usuario autorizado y prevenir el acceso no autorizado.

Para ello se deben implementar controles que consideren:

- **La creación de un procedimiento formal del Registro de usuarios** para conceder y revocar el acceso a todos los sistemas y servicios de información. Dicho procedimiento debería contemplar: el uso de un único identificador de usuario; la comprobación de que el usuario tiene autorización del propietario del sistema y de que el nivel de acceso concedido es adecuado; la declaración y firma del usuario sobre la aceptación de sus derechos de acceso; el mantenimiento de un registro formal de todas las personas registradas para el uso del servicio; la retirada o bloqueo de los derechos de acceso de los usuarios que cambian de puesto o abandonan la organización; comprobaciones periódicas de los ID's en su ciclo de vida.

- **La Gestión de privilegios** de modo que la asignación y el uso de privilegios estén restringidos y controlados a través de un proceso formal de autorización. Contemplando en dicho proceso, por ejemplo: la identificación de privilegios de acceso asociados a cada producto del sistema; que los privilegios se asignen a los usuarios en base a la necesidad de uso; la creación de un registro de todos los privilegios asignados; la preferencia por el desarrollo y uso de programas que eviten la necesidad de ser ejecutados con privilegios, la asignación de los privilegios en un ID diferente al utilizado para el uso normal del sistema….

- **La Gestión de asignación y distribución de las contraseñas de usuario** controlada mediante un proceso formal en el que se incluyan requisitos como: requerir a los usuarios la firma de una declaración para mantener la confidencialidad de las contraseñas; la verificación de la identidad de un usuario previamente a proporcionarle una contraseña; la entrega inicial (con acuse de recibo y de forma segura) de una contraseña provisional fuerte (única, individual y no adivinable) la cual se vean obligados a cambiar inmediatamente; la necesidad de evitar el almacenamiento de las contraseñas en los ordenadores de una manera no protegida; la obligatoriedad de cambiar las contraseñas por defecto de un producto o sistema durante el proceso de su instalación …El servicio de recuperación de contraseñas debe ser especialmente cuidadoso ya que es un punto muy vulnerable a ataques del sistema de contraseñas.

- **La Revisión formalmente procedimentada de los derechos de acceso de usuario** a intervalos regulares. Considerando: la reasignación de los derechos de acceso y la revisión adicional después de cualquier cambio (como promoción, degradación o terminación del empleo); mayor frecuencia de revisión cuando haya privilegios especiales; la creación un registro de los cambios de privilegios en las cuentas…

- **La Identificación de los riesgos derivados del acceso de terceros** de modo que se pueda identificar cualquier requisito para la implantación de los controles específicos. Teniendo en cuenta aspectos como: a qué dispositivos y qué tipo de acceso será necesario; el valor, criticidad y sensibilidad de la información involucrada; los controles necesarios para proteger la información que se pretende que no sea accesible; identificación de la organización y personal al que se ha autorizado el acceso; los diferentes medios y controles que el tercero emplea cuando almacena, procesa, comunica, comparte e intercambia información; el impacto si el acceso no está disponible; las prácticas y procedimientos para tratar los incidentes de seguridad; los requisitos legales y reglamentarios y otras obligaciones contractuales aplicables al tercero; el aseguramiento de que el tercero conoce y es consciente de sus obligaciones y acepta las responsabilidades y limitaciones que lleva implícitas el acceso; uso de acuerdos de no divulgación …

- **La Retirada de los derechos de acceso** a la finalización del empleo (del contrato o del acuerdo) o bien la adaptación de dichos derechos, a los cambios producidos. Evaluando factores de riesgo tales como: si la finalización o cambio es a iniciativa del empleado, contratista o tercero, o por iniciativa de la Dirección, así como la razón de la finalización; las responsabilidades del empleado; el valor de los activos a los que tiene acceso.

4.3.4.3.3. Establecimiento de las responsabilidades de usuario

- Se debe concienciar a los usuarios de sus responsabilidades sobre el mantenimiento de los controles para prevenir el acceso de usuarios no autorizados y para evitar el que se comprometa o se produzca el robo de información o de recursos de tratamiento de la información. Conseguir la cooperación de los usuarios es crucial para una seguridad efectiva, en especial en cuanto a uso seguro de contraseñas y equipos.

- Para ello se deben implementar controles que consideren:

- **El Uso seguro de contraseñas**, requiriendo a los usuarios el cumplimiento de las buenas prácticas de seguridad en la selección y el uso de las contraseñas, como por ejemplo: mantener la confidencialidad de las contraseñas (y no compartirla); evitar el uso de registros o almacenamiento de claves no seguros (p.ej. un papel, un fichero en texto claro…); cambiar las contraseñas que pudieran estar comprometidas; la selección de contraseñas de calidad (fácil de recordar, sin información relativa a la persona para que sea difícil de adivinar, que no estén incluidas en diccionarios, con caracteres variados); evitar la reutilización cíclica así como su inclusión en procesos automáticos de registro (p.ej. una macro); no usar las mismas contraseñas para propósitos personales que para los profesionales ….

- **La protección adecuada del Equipo de usuario desatendido** mediante por ejemplo: bloqueo de salvapantallas con contraseña, bloqueo de sesión con apagado automático del terminal…Teniendo un especial cuidado con los ordenadores centrales o servidores.

- **La implantación de una Política de puesto de trabajo despejado y pantalla limpia** acorde con la clasificación de la información y requisitos legales y considerando directrices como: guardar bajo llave la información sensible; el bloqueo de terminales, protección de los puntos de entrada y salida del correo (físico) y las máquinas de fax así como el control del uso de dispositivos de reproducción.

4.3.4.3.4. Control de acceso a la red

Se debe prevenir el acceso no autorizado a los servicios mediante la colocación de interfaces y mecanismos de autenticación adecuados y respetando los controles de acceso.

Los controles a considerar para el control del acceso a la red son:

- **Creación de una Política de uso de los servicios en red** en la que se contemple el proporcionar a los usuarios únicamente el acceso a los servicios para que los que hayan sido específicamente autorizados. En la política se debe especificar: las redes y servicios de red a los que está permitido el acceso y a quien, los procedimientos de autorización y gestión así como los controles para proteger el acceso a las conexiones y servicios de red, los medios utilizados para acceder a las redes y a los servicios en red…

- C**ontrol de la Autenticación de usuarios para conexiones externas (remotas)** con métodos apropiados y proporcionados. Algunos de estos métodos pueden ser por ejemplo: uso de técnicas basadas en criptografía (autenticación fuerte), protocolos de

pregunta/respuesta, controles de rellamada (con vigilancia del sistema de desvío de llamadas), autenticación del nodo, controles adicionales en redes inalámbricas, VPN's, líneas dedicadas….
Métodos como la posibilidad de conexión a la red mediante el uso, como pasarela, de un ordenador remoto, pueden suponer brechas de seguridad. Sobre todo, si para la conexión se está usando una red fuera del control de la organización.
Para el acceso a redes inalámbricas se deberían implantar controles adicionales de autenticación ya en estas redes existe mayor oportunidad de interceptación inadvertida y de inserción en el tráfico de la red.
En un tal caso, unos métodos proporcionan un mayor nivel de protección que otros, pero también requieren un mayor nivel de recursos. Por lo que, para la selección adecuada del método de autenticación, se debe determinar el nivel de protección requerido a partir de una evaluación del riesgo.

- **La Identificación de los equipos en las redes** ya que supone un medio de autenticación de las conexiones provenientes de localizaciones y equipos específicos.
  Si existe más de una red (y si estas redes tienen distinto grado de sensibilidad), el identificador se puede usar para controlar a que red se permite la conexión del equipo.

- **Control del acceso al Diagnóstico remoto y protección de la configuración de los puertos** para evitar accesos no autorizados. Debido a que el control de acceso remoto se realiza a través de una correcta configuración de los puertos, se deberían deshabilitar todos aquellos que no sean imprescindibles para el funcionamiento de los servicios necesarios para el negocio.

- **Segregación de las redes** de usuarios, servicios y sistemas de información; dividiéndolas en dominios de red lógica protegidos por un perímetro de seguridad definido mediante por ejemplo: pasarelas seguras (cortafuegos), redes privadas virtuales para grupos, listas de control de acceso en función de la IP, segregación de las redes inalámbricas en redes internas y privadas…
  Los dominios deberían estar definidos en base a una evaluación del riesgo y así poder establecer los diferentes requisitos de seguridad dentro de cada dominio. De este modo la segregación de las redes estará basada en el valor y la clasificación de la información almacenada o procesada en la red, en los niveles de confianza, o en las líneas de negocio, para reducir el impacto global de una interrupción del servicio.
  Tras ello, se puede conseguir una segregación de entornos de seguridad de red (como: sistemas públicamente accesibles, redes internas, y activos críticos). Y aplicar un conjunto escalonado de controles en los diferentes dominios de la red lógica.

- **Control de la conexión a la red en redes compartidas**, sobre todo si éstas traspasan las fronteras de la organización. El control se puede realizar mediante por ejemplo la restricción de la capacidad de conexión de los usuarios a la propia red (o a determinadas horas y días) y a aplicaciones tales como: mensajería, correo electrónico, transferencia de ficheros…

- **Control de encaminamiento (routing) de red** de modo que se pueda garantizar que las conexiones de los ordenadores y los flujos de información se ajustan a la política de

control de acceso de las aplicaciones empresariales. Dichos controles de direccionamiento deberían estar basados en mecanismos de comprobación de direcciones de origen y destino verdaderas (proxies).

4.3.4.3.5. Control de acceso al sistema operativo

Con el objetivo de prevenir el acceso no autorizado a los sistemas operativos se deben usar recursos que sean capaces de: proporcionar los medios adecuados de autenticación y de acuerdo a una política de control de acceso definida, registrar los intentos exitosos y fallidos así como el uso de privilegios especiales, disparar alarmas cuando se infrinjan las políticas de seguridad, restringir el tiempo de conexión a los usuarios.

Para lo que se proponen los siguientes controles:

- **Implantar procedimientos seguros de inicio de sesión en los S.O.** de modo que se revelen el mínimo imprescindible de datos de entrada al sistema.
  Considerando por ejemplo: no mostrar los identificadores del sistema ni la contraseña que se está introduciendo y validar la información de entrada únicamente cuando se hayan completado todos los datos de entrada, sin indicar las partes incorrectas en los datos si se produce un error; no transmitir las contraseñas en texto limpio a través de la red; limitar el tiempo permitido para el procedimiento de entrada; mostrar un aviso general de que únicamente deberían acceder al ordenador los usuarios autorizados así como la fecha y la hora de la entrada satisfactoria anterior y detalles de cualquier intento no satisfactorio; limitar y registrar el número de intentos de entrada no satisfactorios considerando forzar un tiempo de retraso, desconectar las conexiones y enviar alarmas.

- **Una adecuada Identificación y autenticación de usuario con un identificador único** (ID de usuario) monitorizado, para su uso personal y exclusivo y distinto del usado para actividades que necesitan accesos privilegiados. Se debería elegir una técnica adecuada de autenticación para confirmar la identidad solicitada del usuario. Cuando se requiera una fuerte autenticación y verificación de la identidad, se deberían utilizar métodos alternativos de autenticación para las contraseñas, tales como medios criptográficos, tarjetas inteligentes, dispositivos o medios biométricos.

- **Uso de un Sistema de gestión de contraseñas** interactivo que fuerce el uso de ID's individuales y contraseñas de calidad; que permita a los usuarios seleccionar y cambiar sus propias contraseñas con mecanismos de confirmación de error, forzado de cambio de contraseñas, prevención de reutilización, ocultación de caracteres en la introducción de la contraseña y que cuente con sistema de registro, almacenamiento y transmisión protegido.

- **Restricción y control del Uso de los recursos del sistema** evitando el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación. Considerando, por ejemplo, para esos programas y utilidades: Procedimientos documentados para autorización de acceso a los mismos y registro de su uso; limitación y establecimiento de niveles de uso así como segregación de tareas relacionadas con el uso de estos recursos del sistema.

- **Desconexión automática de sesión inactiva** que debería cerrarse después de un periodo de inactividad definido en función del nivel de riesgo. Adicionalmente, la pantalla de sesión también debe limpiarse.

- **Limitación del tiempo de conexión** en las aplicaciones de alto riesgo, considerando: el uso de espacios de tiempo predeterminados; la restricción de las horas de conexión; la reautenticación a intervalos de tiempo.

4.3.4.3.6. Control de acceso a las aplicaciones y a la información

Con el objetivo de prevenir el acceso no autorizado a la información que contienen las aplicaciones, los sistemas de aplicación deberían: controlar el acceso del usuario a la información y a las funciones del sistema de aplicación, de acuerdo con una política de control de acceso definida; estar protegidos contra el acceso no autorizado al software del sistema operativo (y del software malicioso que es capaz de invalidar o evitar los controles del sistema o de la aplicación); no comprometer otros sistemas con los que se comparten recursos de información.

Para ello se proponen los siguientes controles:

- **Restricción del acceso a la información** y a las aplicaciones mediante por ejemplo: menús de control de acceso; control de derechos de acceso de los usuarios (y de otras aplicaciones) y aseguramiento de la cantidad de información de salida en los sistemas de aplicación con datos sensibles y de que ésta es sólo enviada a los terminales autorizados.

- **Aislamiento de sistemas sensibles** de modo que estos estén en entornos dedicados, siendo la sensibilidad explícitamente definida y documentada. Pudiendo usarse tanto métodos físicos como lógicos. Para aplicaciones que se ejecutan en entornos compartidos, deben ser considerados por el propietario de la aplicación los sistemas con los que se comparten los recursos y los riesgos asociados.

- **El Control de acceso restringido al código fuente de los programas**, para evitar cambios involuntarios o para evitar la introducción de funciones no autorizadas (ver este control con más detalle en el capítulo dedicado a SDLC (apartado 4.3.5).

4.3.4.3.7. Aseguramiento de los ordenadores portátiles y del teletrabajo

Los medios portátiles y el teletrabajo deben ser adecuadamente protegidos de forma proporcionada a los riesgos.

- **Los Ordenadores portátiles y comunicaciones móviles** deben estar sujetos a medidas de seguridad adecuadas y conforme a una política formal que incluya: los requisitos (legales y de los seguros, entre otros) para su protección física y ante la posibilidad de robos; los controles de acceso; las técnicas criptográficas; las copias de seguridad y la protección antivirus. Además de una formación específica para el uso de los dispositivos móviles, la política también debería incluir reglas y consejos para conectar los dispositivos móviles a las redes, así como una guía para el uso, especialmente cuidado, de estos dispositivos en lugares públicos y en redes

inalámbricas.
En el uso de ordenadores en zonas públicas debe evitar el riesgo que conllevan las miradas por parte de personas no autorizadas. La conexión por acceso remoto debe realizarse únicamente después de una identificación y autenticación satisfactorias, y a través de la implantación de los mecanismos de control bien configurados y actualizados.
Las copias de seguridad de estos dispositivos deben realizarse con frecuencia y estar debidamente protegidas.

- El **Teletrabajo** debe estar autorizado y controlado por la dirección. Sujeto a planes y procedimientos de operación, conforme a una política formal para esta actividad. De modo que se satisfaga su seguridad y los controles implantados contra por ejemplo: el robo del equipo y de la información; la revelación no autorizada de la información; el acceso remoto no autorizado a los sistemas internos de la organización o contra el mal uso de los recursos. Se deben considerar aspectos como: el acceso a la parte privada del propietario del equipo (para comprobar la seguridad de la máquina o durante una investigación); acuerdos de licencia de software; derechos de propiedad intelectual de lo desarrollado por el propietario del equipo de manera privada; la provisión del equipo adecuado y el mobiliario de almacenamiento para las actividades de teletrabajo; una definición del trabajo permitido; las horas de trabajo; la clasificación de la información que puede manejarse y los sistemas y servicios a los que el teletrabajador está autorizado a acceder; las reglas y directrices para el acceso de la familia y visitantes al equipo y a la información del teletrabajador; los procedimientos para las copias de seguridad y para los planes de continuidad; la provisión de seguro, soporte y mantenimiento de hardware y software; la auditoría y seguimiento de la seguridad; las condiciones de devolución del equipo así como la revocación de la autorización y los derechos de acceso una vez terminadas las actividades de teletrabajo…

4.3.4.4. Consideraciones específicas en la autenticación remota

La guía **NIST SP 800-63** sobre Autenticación Electrónica trata de los diferentes métodos técnicos de autenticación remota (de personas) basados en secretos (claves), definiendo los requerimientos mínimos de los mismos en función de 4 niveles crecientes de implantación de medidas de seguridad. Dichos niveles están definidos en base a las presumibles consecuencias derivadas de los errores de autenticación o del mal uso de las credenciales. De modo que cuanto más serias son las consecuencias de un error de autenticación, más se incrementa el nivel requerido de seguridad.

En particular, esta guía especifica los requerimientos técnicos para cada uno de los cuatro niveles de aseguramiento en las siguientes áreas:

- Tokens (típicamente una clave criptográfica o contraseña almacenada en un dispositivo electrónico) para probar la identidad.
- Comprobación de la identidad, registro y entrega de credenciales que ligan unívocamente una identidad a un token.

- Mecanismos de autenticación remota, que son la combinación de credenciales, tokens y protocolos de autenticación usados para establecer que un solicitante es en realidad el suscriptor que pretende ser.
- Mecanismos de certificación usados para comunicar los resultados de una autenticación remota a otras partes.

Para especificar los requerimientos técnicos se hace un estudio de cada una de estas áreas describiendo las amenazas y requerimientos necesarios según los niveles de seguridad.

Así, se desarrolla el modelo de la autenticación electrónica y se explica la serie de procesos que han de completarse: Registro (token y credencial), comprobación de la identidad en la RA (con los distintos requerimientos para cada nivel) y autenticación. También se dan recomendaciones para los procesos de registro y comprobación de la identidad (para más información ver los capítulos 5 y 7 de NIST 800-63)

Los tokens son algo que el solicitante de acceso posee y controla y que es usado para autenticar su identidad. Se trata de un "secreto" (clave) y debe ser protegido (por ejemplo puede ser una clave criptográfica protegida por encriptación con contraseña o contenida en un dispositivo hardware con un lector biométrico que activa la clave).

En cuanto a los "secretos", estas suelen estar basadas en claves de sistemas asimétricos (par público/privado; algo que se tiene) o secretos compartidos (contraseñas compartidas; algo que se sabe). En el caso del par de claves se ha de mantener a salvo la clave privada ya que de otra forma ambas serán puestas en compromiso. En el caso de las contraseñas los inconvenientes residen en el hecho de que (además de mantenerlas en secreto): generalmente no tienen tantos valores posibles como las claves criptográficas; en muchos protocolos son vulnerables a ataques a través de la red (que para las claves son impracticables) y que al ser introducidas habitualmente a través de teclados están más expuestas a ser descubiertas.

En cuanto a los mecanismos biométricos no se tratarán en la guía como tokens en sí, sino como apoyo para prevenir repudio o fraude del proceso de registro o como sistema de desbloqueo de tokens.

El concepto de "credencial electrónica de identidad" (certificado digital) es la correspondencia unívoca entre un nombre (y tal vez otros atributos) y un token (clave).

Por ser los más relevantes, sólo se tratarán 4 tipos de tokens: los de hardware, los de software, los de contraseñas y los dispositivos de contraseñas de un solo uso (OTP's).

4.3.5. Seguridad en el ciclo de vida del desarrollo de los sistemas

4.3.5.1. Objetivos

Las consideraciones de seguridad en el Ciclo de vida de desarrollo de los sistemas (SDLC) son esenciales para la implementación y la integración de una estrategia integral para la gestión de de riesgos para todos los activos de tecnología de información en una organización.

Las ventajas de integrar la seguridad en el SDLC son:

- Identificación temprana y mitigación de vulnerabilidades de seguridad y errores de configuración, lo que da como resultado en una disminución del costo de implementación del control de seguridad y reducción de la vulnerabilidad;
- Concienciación de los retos potenciales causados por los controles de seguridad obligatorios;
- Identificación de los servicios de seguridad compartida y reutilización de estrategias y herramientas de seguridad para reducir los costos de desarrollo y calendario;
- Facilitación de toma de decisiones ejecutivas bien informadas mediante la gestión integral de riesgo;
- La documentación de las decisiones importantes de seguridad hechas durante el desarrollo, garantiza que la seguridad es plenamente considerada durante todas las fases;
- Mejorar la confianza de los clientes y la organización para facilitar la adopción y uso, así como la confianza gubernamental, del fomento de la inversión continua;
- Mejora de la interoperabilidad e integración de los sistemas que de lo contrario podría verse obstaculizada por la securización en distintos niveles.

4.3.5.2. Descripción

El ciclo de vida de desarrollo de sistemas (SDLC) es el proceso, (que involucra varias etapas: desde establecer la factibilidad de llevarse a cabo hasta las revisiones posteriores a la implementación), utilizado para convertir una necesidad de la gerencia en una aplicación de sistema, que es desarrollada a medida o adquirida o es una combinación de ambas.

El SDLC de un sistema de aplicación dependerá del modo de desarrollo/adquisición elegido.

Cuando un sistema de aplicación se desarrolla en lugar de ser comprado como un paquete, el SDLC dependerá de la metodología de desarrollo utilizada, como el desarrollo de la cascada, prototipos, desarrollo rápido de aplicaciones, CASE y desarrollo orientado a objeto.

Durante el SDLC de un sistema de aplicación, los diversos riesgos que pueden ser encontradas incluyen:

- Aprobación del SDLC inadecuado para el sistema de aplicación
- Controles inadecuados en el proceso de SDLC
- Requisitos de usuario y objetivos no cubiertos por el sistema de aplicación
- Inadecuada participación de los interesados (incluida la auditoría interna)
- La falta de apoyo de la dirección

- Gestión de proyectos inadecuada
- Tecnología y la arquitectura inapropiada
- Variaciones del alcance
- Sobrecostes de tiempo
- Sobrecostes de costo
- Inadecuada calidad del sistema de aplicación
- Insuficiente atención a la seguridad y los controles (que incluirán validaciones y pistas de auditoría) en el sistema de aplicación
- Criterios de rendimiento no cubiertos
- Modelo de gestión de recursos/personal inapropiado
- Habilidades de personal inadecuadas
- Documentación insuficiente
- Protección contractual inadecuada
- Adhesión inadecuada al SDLC elegido y/o metodologías de desarrollo
- Insuficiente atención a las interdependencias con otras aplicaciones y procesos
- Inadecuada gestión de la configuración
- Insuficiente planificación para la migración conversión y transferencia de datos
- Interrupción de negocio tras la transferencia de datos

4.3.5.2.1. Buenas prácticas relativas a la seguridad en el SDLC

Tradicionalmente los estándares genéricos en seguridad no tienen capítulos dedicados, como tal, al ciclo de vida del desarrollo de los sistemas, sino que tienen determinadas medidas de seguridad que son aplicables al SDLC pero que no están agrupados con ese título. Este es el caso por ejemplo del NIST 800-53, que tiene una familia dedicada a la adquisición de sistemas y servicios, pero el resto de controles de seguridad que aplicarían a un SDLC, están diseminados en las distintas familias.

En el caso de la ISO 27002, el dominio 12 está dedicado por completo a Adquisición, desarrollo y mantenimiento de los sistemas de información (y a los Controles Criptográficos). Lo cual se ajusta al concepto de las medidas de seguridad que se implantan en un SDLC.

No obstante, ninguno de los dos estándares tratan el tema bajo el punto de vista de considerar todo el proceso de SDLC de forma pormenorizada y de incluir o incrustar la seguridad en este ciclo. Será la guía NIST 800-64 la que trate este tema en exclusiva.

En este capítulo se hablará de los controles de seguridad genéricos que son de aplicación en todo SDLC y en el siguiente capítulo, se hará un desarrollo de la metodología del SDLC en el que se va a incorporar la seguridad como una parte más.

4.3.5.2.2. Identificación de los requisitos de seguridad de los sistemas de información

Con el objetivo de garantizar que la seguridad está integrada en los sistemas de información (los sistemas operativos, la infraestructura, las aplicaciones empresariales, los productos disponibles en el mercado, los servicios y las aplicaciones desarrolladas por el usuario), se debe considerar que los requisitos de seguridad deberían ser identificados y acordados antes de desarrollar o implantar los sistemas de información.

Para lo cual se debe realizar un **análisis y especificación de los requisitos de seguridad** para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes (incluidos los paquetes de software desarrollados o adquiridos para las aplicaciones empresariales). Considerando la incorporación de controles automatizados y manuales, preferiblemente, en la fase de diseño.

En los productos adquiridos, debería seguirse un proceso formal de pruebas y compra. Debiendo abordar los requisitos de seguridad con el proveedor.

Cuando no se satisfacen los requisitos de seguridad de un producto propuesto, se debe reconsiderar el riesgo que supondrá y los controles asociados que serán necesarios, antes de adquirir el producto.

La incorporación de funciones adicionales pueden provocar un riesgo de seguridad, en este caso, ésta debería desactivarse o bien debería revisarse la estructura de control propuesta para determinar si dicha ampliación de funciones proporcionará un beneficio adicional considerable.

4.3.5.2.3. Tratamiento correcto de las aplicaciones

Con el objetivo de evitar errores, pérdidas, modificaciones no autorizadas o usos indebidos de la información en las aplicaciones, se deben diseñar controles adecuados y proporcionados al riesgo, que incluyan: la validación de los datos introducidos, el procesamiento interno y los datos resultantes.

Para lo cual se proponen los controles siguientes:

- **Validación de los datos de entrada** para garantizar que dichos datos son correctos y adecuados, considerando:
    - introducción dual u otras comprobaciones (como comprobación de la delimitación o limitación de los campos a un ámbito específico de datos), con el fin de detectar los siguientes errores: valores fuera del ámbito; caracteres inválidos en los campos de datos; falta de datos o datos incompletos; sobrepasar los límites superiores o inferiores de volumen de datos; control de datos no autorizado o incoherente.

- revisión periódica del contenido de los campos clave (para confirmar su validez e integridad) e inspecciones de las entradas de documentos impresos en papel (para buscar cambios no autorizados).

- procedimientos para reaccionar ante errores de validación así como para comprobar la verosimilitud de los datos introducidos.

- definición de las responsabilidades del personal que interviene en el proceso de introducción de datos así como la creación de un registro de las actividades relacionadas con dicho proceso.
  Si las comprobaciones están automatizadas se evitarán riesgos (errores y ataques)

- **Control del procesamiento interno** mediante comprobaciones de validación en las aplicaciones; de modo que se detecte cualquier corrupción de la información (pérdida de integridad) debida a errores de procesamiento o actos intencionados, considerando las siguientes áreas:

  - el uso de las funciones de añadir, modificar y borrar para implantar los cambios en los datos.

  - procedimientos para evitar que los programas funcionen en orden incorrecto o que funcionen después de un error del procesamiento anterior, así como el uso de programas adecuados de recuperación de fallos.

  - protección contra ataques de desbordamiento o de saturación de la memoria intermedia (búfer).

  Realizando las siguientes comprobaciones:

  - Tras actualizar las transacciones, uso de controles de sesión o de lote para cuadrar el saldo

  - controles del saldo para comparar los saldos iniciales con los anteriores saldos de cierre como por ejemplo: los controles entre ejecuciones (run to run), las actualizaciones totales de archivos y los controles entre programas.

  - validación de los datos de entrada generados por el sistema, así como la realización de comprobaciones de la integridad, la autenticidad o cualquier otra característica de seguridad de los datos o del software descargado o cargado entre el ordenador central y un ordenador remoto.

  - comprobaciones del grado de dispersión de los registros y archivos y de que los programas de la aplicación: se activan en el momento adecuado, se ejecutan en el orden correcto y finalizan en caso de error y que el procesamiento posterior se interrumpe hasta que se resuelve el problema;

  - creación y mantenimiento de un registro de las actividades relacionadas con el procesamiento.

- **Integridad de los mensajes** y autenticidad. Esta necesidad debe ser determinada mediante análisis de riesgos y, en caso positivo, garantizada mediante la implantación de controles adecuados (técnicas criptográficas).

- **Validación de los datos de salida** para garantizar que el tratamiento de la información almacenada es correcto y adecuado a las circunstancias, incluyendo en la validación:

    - comprobaciones de la verosimilitud para determinar si los datos resultantes son razonables.

    - cuentas de control de conciliación para garantizar el procesamiento de todos los datos;

    - presentación de la información suficiente para el lector o para el sistema de tratamiento posterior a fin de determinar la exactitud, la integridad, la precisión y la clasificación de la información.

    - procedimientos para reaccionar ante los errores de validación de salida de datos.

    - definición de las responsabilidades del personal que interviene en el proceso de introducción de datos así como la creación de un registro de las actividades relacionadas con dicho proceso.

4.3.5.2.4. Aseguramiento de los archivos del sistema

Mediante el control del acceso seguro a los archivos de sistema, los códigos fuente de los programas, los proyectos de TI y sus actividades de apoyo y cuidando la exposición de datos sensibles en entornos de prueba.

Para lo cual se proponen los siguientes controles:

- **Control del software en explotación y de sus cambios**, mediante procedimientos que regulen la instalación de software en los sistemas en producción o en explotación. Y así minimizar el riesgo de corromper los sistemas operativos, considerando que:

    - la actualización del software, aplicaciones y bibliotecas de programas sólo debe ser llevada a cabo por administradores formados y autorizados.

    - los sistemas operativos sólo deben manejar códigos ejecutables aprobados, y no códigos de desarrollo o compiladores;

    - el software de las aplicaciones y del sistema operativo sólo debe implantarse tras haber superado pruebas completas (de utilidad, seguridad, efectos en otros sistemas y facilidad de uso) que deben llevarse a cabo en sistemas independientes. Asegurándose de que todas las bibliotecas fuente del programa están actualizadas.

- debería emplearse un sistema de control de la configuración para supervisar todo el software implantado y la documentación del sistema.
- antes de implantar cambios, debería existir una estrategia de restauración.
- debería mantenerse un registro de auditoría de todas las actualizaciones de las bibliotecas de los programas operativos.
- las versiones anteriores del software de las aplicaciones deben conservarse como medida de contingencia; así como toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de apoyo durante todo el tiempo en que la información se conserve en el archivo.
- si un software adquirido no cuenta con asistencia técnica del proveedor, se deben considerar los riesgos de seguir utilizándolo.
- para pasar a una nueva versión se debe tener en cuenta la introducción de nuevas funciones de seguridad o el número y la gravedad de los problemas de seguridad que afecten a esta versión. Solo deben aplicarse parches cuando éstos puedan ayudar a eliminar o a reducir los puntos débiles de seguridad.
- si el software informático depende de software y de módulos adquiridos externamente, éstos deben ser supervisados y controlados para evitar cambios no autorizados, ya que podrían generar un punto débil de seguridad.
- sólo debería concederse acceso físico o lógico autorizado, a los proveedores para que presten servicios de asistencia técnica cuando sea necesario. Dichas actividades deberían supervisarse.

- **Protección de los datos de prueba del sistema**, los cuales, deben ser seleccionados cuidadosamente (evitando, omitiendo o modificando los sensibles). Las directrices para su control y protección deben ser las siguientes:
  - los procedimientos de control de acceso de los sistemas en pruebas deben ser los mismos que los de los sistemas en explotación;
  - cada vez que se copie información operativa a un sistema de prueba debería obtenerse una autorización independiente. Adicionalmente, se debe registrar la copia o el uso de información operativa para que pueda servir como pista de auditoría;
  - la información operativa debe borrarse del sistema de prueba inmediatamente después de finalizar la misma.

- **Control de acceso al código fuente de los programas** y a los elementos relacionados con él (diseños, especificaciones, planes de verificación y de validación) para evitar cambios involuntarios o para evitar la introducción de funciones no autorizadas.
  En el caso de estar almacenado en las bibliotecas fuente del programa, se debe tener en cuenta lo siguiente para protegerlas:

- las bibliotecas fuente de los programas no deben mantenerse en los sistemas en explotación;
- el código fuente y las bibliotecas fuente de los programas deben gestionarse conforme a procedimientos establecidos;
- el personal de asistencia técnica no debería tener acceso sin restricciones a las bibliotecas fuente de los programas;
- la emisión de fuentes de programa a los programadores y la actualización de las bibliotecas fuente de los programas y los elementos relacionados con ellas, sólo debería efectuarse tras haber recibido la autorización adecuada;
- los listados de programas deberían guardarse en un entorno seguro.

4.3.5.2.5. Seguridad en los procesos de desarrollo y soporte

Con el objetivo de mantener la seguridad del software y de la información de las aplicaciones, los entornos de proyecto y de asistencia técnica deberían estar estrictamente controlados por sus responsables en cuanto a su seguridad y a la revisión de todas las modificaciones del sistema propuestas.

Para lo cual se proponen los siguientes controles:

- **Existencia de Procedimientos de control de cambios formales** (observando su documentación, especificación, pruebas, control de calidad e implantación controlada) para minimizar la corrupción de los sistemas de información.
  El proceso de cambio debería incluir: una evaluación de riesgos, un análisis de los efectos de los cambios y una especificación de los controles de seguridad necesarios; garantizando que la seguridad y controles existentes no se ponen en peligro.
  En los procedimientos de cambio se debe:
  - mantener un registro de los niveles de autorización acordados;
  - garantizar que los cambios son propuestos por usuarios autorizados; que las propuestas están bien detalladas y son aprobadas antes de que se inicien los trabajos y que los usuarios autorizados aceptan los cambios previamente a su implantación; y todo ello, manteniendo pistas de auditoría de todas las solicitudes de cambio;
  - revisar los controles y los procedimientos de integridad para garantizar que no se verán vulnerados por los cambios;
  - tener identificado el software, el hardware, la información y las entidades de la base de datos que requieran modificaciones y que se mantiene un control de la versión de todas las actualizaciones del software;
  - garantizar que la documentación del sistema se actualiza al completar cada cambio, que la documentación antigua se archiva o se elimina y que la

documentación operativa y los procedimientos de usuario se modifican según sea necesario para que sigan siendo adecuados;

- garantizar que la implantación de los cambios se realiza en el momento adecuado y que no perturba los procesos de negocio implicados.

- **Revisión técnica de las aplicaciones** tras efectuar cambios en el sistema operativo (que debe recaer sobre un individuo o un grupo). Así se garantiza que no existen efectos adversos en las operaciones o en la seguridad de la organización. El proceso debe:

  - tener en cuenta que se deben notificar con tiempo suficiente los cambios en el sistema operativo, de modo que permita la realización de pruebas y revisiones adecuadas antes de su implantación;

  - considerar que tanto el plan como el presupuesto anuales de asistencia técnica deben cubrir las revisiones y las pruebas del sistema que conllevan los cambios del sistema operativo;

  - revisar los procedimientos de integridad y de control de la aplicación para garantizar que no se han visto comprometidos por los cambios del sistema operativo;

  - asegurar que se realizan los cambios oportunos en los planes de continuidad del negocio.

- **Aplicación de Restricciones a los cambios en los paquetes de software** limitándose a los cambios o modificaciones estrictamente necesarios, y siendo objeto de un control riguroso.
  En caso de ser modificado un software se debe tener en cuenta:

  - la posibilidad de que los controles integrados y los procesos de integridad se vean comprometidos;

  - si se debe solicitar el consentimiento del proveedor así como la posibilidad de obtener de éste los cambios requeridos, a modo de actualizaciones estándar del programa;

  - los efectos que ocasionarán los cambios, en caso de que la organización se responsabilice del mantenimiento futuro del software.

  - la instalación de los parches y las actualizaciones más recientes, de la aplicación aprobada, así como la conservación del software original claramente identificado;

  - que se deben probar y documentar todos los cambios de manera que puedan volver a aplicarse en caso necesario.

- **Evitar las Fugas de información** mediante: el escaneo de los medios y comunicaciones de salida en busca de información oculta; el sistema de enmascaramiento y modulación del sistema y el comportamiento de las comunicaciones para reducir la probabilidad de que un tercero pueda deducir información a partir de dicho comportamiento; la utilización de sistemas y software considerados de elevada integridad; la supervisión periódica del personal y de las actividades del sistema (legalmente permitidas); la supervisión del uso de recursos en los sistemas informáticos.

- **Supervisión y control del desarrollo de software externalizado**. Teniendo en cuenta: los contratos de licencia, propiedad del código y derechos de propiedad intelectual; la certificación de la calidad y la precisión del trabajo desempeñado; bloqueo de garantía (por contrato) en caso de error por parte de terceros; los derechos de acceso para auditar la calidad y la precisión del trabajo realizado; los requisitos contractuales para funcionalidades de calidad y seguridad del código; realización de pruebas antes de la instalación para detectar códigos maliciosos y troyanos.

4.3.5.2.6. Gestión de la vulnerabilidad técnica

Se deben gestionar las vulnerabilidades técnicas (incluidos los sistemas operativos) de forma, sistemática y adoptando medidas que confirmen su efectividad; con el objetivo de reducir el riesgo de que sean explotadas.

Para lo cual se propone el siguiente control:

- **Control de las vulnerabilidades técnicas** mediante la obtención de información sobre ellas, la evaluación de la exposición de la organización a dichas vulnerabilidades y la adopción de medidas adecuadas para afrontar el riesgo asociado.
  Para ello, se requiere tener un inventario actual y completo de los activos en el que se incluyan los siguientes datos: proveedor de software, números de versión, estado actual de implantación y la persona responsable.
  Considerando en la gestión de vulnerabilidades que:

  - se deben definir y establecer las funciones y responsabilidades asociadas con la gestión de las vulnerabilidades (incluyendo la supervisión de vulnerabilidades, la evaluación de riesgos de vulnerabilidad, el parcheo, el seguimiento de activos y cualquier responsabilidad de coordinación necesaria);

  - deben identificarse y actualizarse los recursos de información, utilizados para identificar las vulnerabilidades técnicas pertinentes y para mantener la alerta sobre ellas, según se modifique el inventario o cuando se encuentren otros recursos nuevos o que sean de utilidad;

  - se debe definir una escala temporal de reacción ante las notificaciones de vulnerabilidades técnicas;

  - se deben identificar los riesgos asociados y las medidas que deberían adoptarse ante la vulnerabilidad técnica (como el parcheo de sistemas vulnerables o la aplicación de otros controles);

- el tratamiento de la vulnerabilidad se llevará a cabo, dependiendo de la urgencia con que deba tratarse, mediante el procedimiento de gestión de cambios o bien siguiendo los procedimientos de respuesta a incidentes de seguridad de la información. Los sistemas con elevado riesgo deberían ser los primeros en tratarse;

- si existe un parche disponible, se deben evaluar los riesgos asociados con su instalación (comparando los riesgos planteados por la vulnerabilidad con los riesgos de instalar el parche). Adicionalmente, los parches deberían ser probados y evaluados antes de su instalación para garantizar que son efectivos y que no tienen efectos secundarios que no puedan ser aceptados.

- Si no hay ningún parche disponible, deberían considerarse otros controles, como: la desactivación de servicios o capacidades relacionadas con la vulnerabilidad; la adaptación o la inclusión de controles de acceso, como por ejemplo, cortafuegos, en los límites de la red; el aumento de la supervisión para detectar o evitar ataques reales; aumentar la concienciación de la vulnerabilidad;

- se debe mantener un registro de auditoría de todos los procedimientos adoptados;

- el proceso de gestión de las vulnerabilidades técnicas debería supervisarse y evaluarse periódicamente para garantizar su efectividad y su eficacia;

4.3.5.3. Consideraciones de seguridad en el proceso metodológico de SDLC

La guía NIST 800-64 sobre las consideraciones de seguridad en el Ciclo de vida de desarrollo de los sistemas (SDLC), describe las clave de los roles y responsabilidades de seguridad necesarias en el desarrollo de la mayoría de sistemas de información. En segundo lugar, se proporciona suficiente información sobre el SDLC para permitir a una persona que no está familiarizada con el proceso SDLC comprender la relación entre la seguridad de la información y el SDLC. Todo ello basándose en actividades de seguridad realizadas cuando se usa una metodología de SDLC en cascada, aunque puede ser trasladable, en sentido amplio, a cualquier otra.

Un típico **SDLC** incluye cinco **fases**: Inicio, desarrollo/adquisición, implementación/evaluación, operaciones/mantenimiento y eliminación. Cada fase incluye un conjunto mínimo de tareas de seguridad necesarias para incorporar eficazmente la seguridad en el proceso de desarrollo del sistema. Teniendo en cuenta que las fases podrán repetirse a lo largo de la vida de un sistema antes de la eliminación.

- **Iniciación**: Durante la fase de iniciación, se pone de manifiesto la necesidad de un sistema y se documenta el propósito del sistema.

- **Desarrollo/Adquisición**: Durante esta fase, el sistema es diseñado, comprado, programado, desarrollado o de algún otro modo, construido.

- **Implementación/Evaluación**: Después de la prueba de aceptación del sistema, el sistema es instalado o puesto en marcha.

- **Operación/Mantenimiento**: Durante esta fase, el sistema realiza su trabajo. El sistema casi siempre es modificado por la adición de hardware y software y por numerosos otros eventos.

- **Eliminación**: Las actividades llevadas a cabo durante esta fase garantizan el cese ordenado del sistema, salvaguardar la información vital del sistema y la migración de datos procesados por éste a un nuevo sistema o su conservación de conformidad con las políticas y normativas aplicables.

Los **fundamentos** de la seguridad de la información y el SLDC consisten en tener en cuenta: el poseer una política repetible y documentada de SDLC en la organización; ejecutar un enfoque sobre los sistemas y proyectos basados en la gestión del riesgo integrando la seguridad desde el comienzo; considerar el Proceso de Control de inversión y planificación de capital; poseer arquitecturas de seguridad alineadas con las buenas prácticas para la protección de la confidencialidad, integridad y disponibilidad así como para la integración de la seguridad en el SLDC; cumplir con los requerimientos legales de los sistemas; establecer claramente los roles y responsabilidades en el SLDC de forma que se sepa determinar quién debe ser consultado en cada fase.

A continuación se describirán una serie de consideraciones que ayudan a integrar la seguridad de la información en cada fase del SDLC. Para lo cual se hará una breve definición de la fase, se identificarán los puntos de control o hitos en los cuales se evaluará si el proyecto lleva la trayectoria adecuada y se describirán las actividades de seguridad a realizar en mediante su descripción, resultados esperados, sincronización entre las partes e interdependencias con otras tareas.

4.3.5.3.1. Incorporación de la seguridad en la fase de Iniciación

Durante esta primera las consideraciones de seguridad son clave para una integración diligente y temprana, asegurando que se consideran amenazas, requisitos y posibles limitaciones en la funcionalidad e integración. Lo que resultará en un ahorro de costos y tiempo.

En este punto, la seguridad es contemplada en términos de riesgos de negocio.

1. Las **actividades** clave de seguridad para esta fase incluyen:

   - Delimitación inicial de requerimientos del negocio en términos de confidencialidad, integridad y disponibilidad;

   - Determinación de categorización de la información y la identificación de requisitos conocidos de tratamiento especial para transmitir, almacenar, o crear información;

   - Determinación de los requisitos de privacidad.

2. Los **puntos a controlar** en esta fase incluyen:

   - Determinación de la estrategia de adquisición

- Verificación de que el proyecto es viable, completo, alcanzable y en consonancia con los objetivos de la organización y con el presupuesto.
- Revisión de que el diseño inicial del sistema ha abordado todos los requisitos de seguridad.
- Un alineamiento con la arquitectura empresarial que armonice la visión de IT, estándares, requerimientos de negocio y la alineación de la seguridad con los servicios actuales y próximos.
- Revisión financiera para comprobar que el costo está bien balanceado con el riesgo.
- Examen de la gestión del riesgo para comprobar que se ajusta a las buenas prácticas.

3. Desarrollo de **Actividades principales de Seguridad:**

- **Planificación inicial de seguridad**: Identificación de los roles claves de seguridad y de los requisitos de seguridad como leyes, reglamentos y normas; garantizar el mutuo entendimiento entre todas las partes implicadas en lo tocante a seguridad, requisitos y consideraciones; esbozar los hitos claves de seguridad incluyendo plazos o indicadores que señalen que se aproxima una etapa de seguridad.
  Para todo ello se generarán: documentos de soporte, reuniones y un calendario del proyecto.

- **Categorización del sistema de Información**: Mediante la identificación de la información que está manejada por la arquitectura empresarial para soportar las líneas de negocio; matriz de mapeo de tipos de información y de sistemas con las categorías se seguridad. Todo ello enfocado a la evaluación de la seguridad en términos del impacto en la pérdida de confidencialidad, integridad y disponibilidad.
  De aquí se deben obtener adicionalmente los requisitos de seguridad de alto nivel y la estimación del esfuerzo necesario para implementar los controles de seguridad mínimos conforme a la categoría.
  Estas tareas están directamente relacionadas con los Análisis de impactos del negocio (BIA), Planes de contingencia y de recuperación de desastres, Acuerdos de interconexión de sistemas y de información compartida… que deben ser tenidos en cuenta para la realización de estas tareas.

- **Evaluación de Impacto en el Negocio**: Con respecto a los servicios críticos para determinar, por niveles, las consecuencias de una interrupción en los componentes del sistema. De este modo se facilitan las decisiones a tomar en materia de seguridad.
  Se deberán obtener un mapa que relacione las líneas de negocio con los sistemas asociados, la identificación de los componentes clave del sistema que necesarios para mantener una funcionalidad mínima, el tiempo máximo que de interrupción del sistema sin impacto para el negocio y la tolerancia del negocio ante la pérdida de datos.
  Todas las tareas necesarias están íntimamente relacionadas con el BIA y la categorización de las actividades de seguridad.

- **Evaluación de Impacto en la privacidad**: Durante el proceso de identificación de los tipos de información para la categorización del sistema se detectará aquella relativa a la privacidad así que al desarrollar un nuevo sistema, es importante considerar si el sistema transmite, almacena o crea este tipo de información para que el propietario del sistema identifique y aplique las salvaguardias y controles de seguridad adecuados, además de procesos de tratamiento de incidentes y requisitos de estos informes.
  Todo ello generará documentos relacionados con el BIA, planes de continuidad y con el documento de Seguridad.

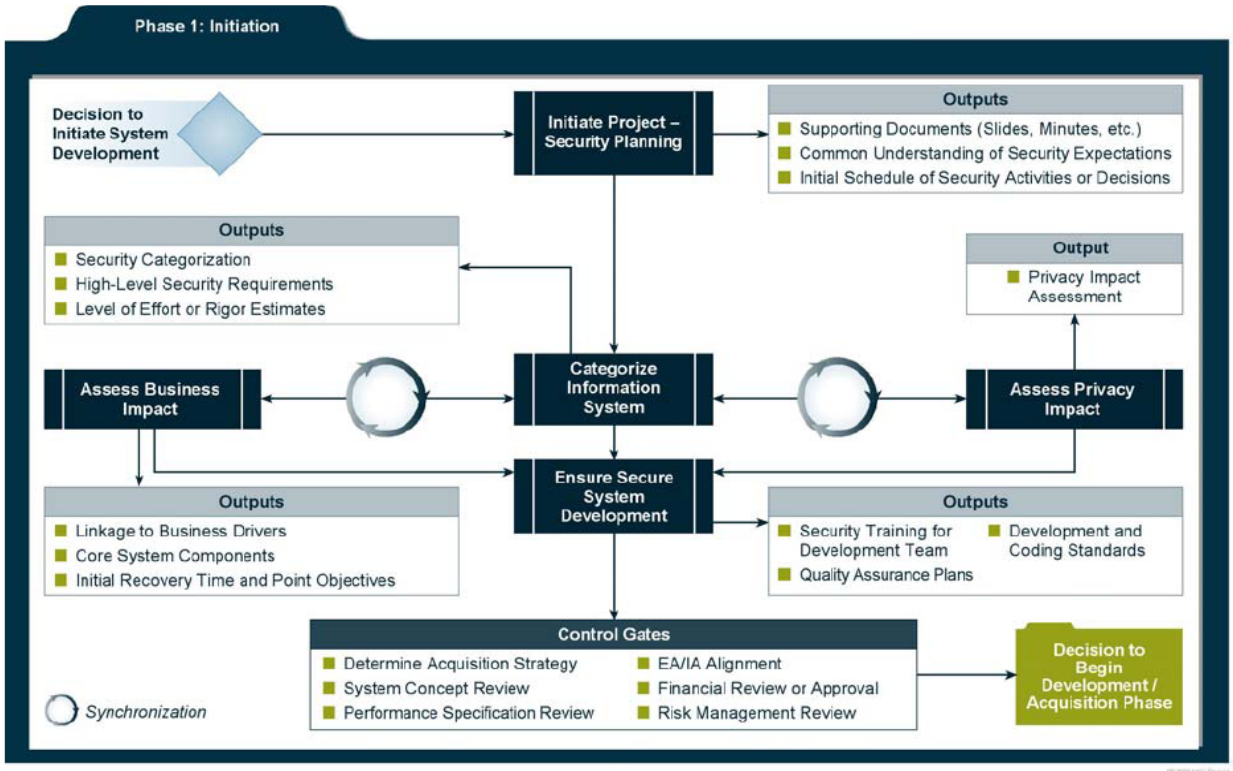

Ilustración 1: Consideraciones de Seguridad relativas a la fase de Iniciación (NIST 800-64)

- **Uso garantizado de procesos de desarrollo seguro de sistemas**: El equipo de desarrollo es clave para detectar defectos de seguridad y para implementar protección a las aplicaciones desde el propio código fuente, por lo que es imprescindible comunicarles nuestras expectativas en seguridad.
  Se deben incluir las siguientes consideraciones:

  a. Concepto de Operaciones para desarrollo seguro (CONOPS): Se debe establecer un documento de concepto de operaciones para el desarrollo seguro e incluir un plan de contingencias para el repositorio de código fuente del entorno de desarrollo.

  b. Procesos de desarrollo de sistemas estandarizados documentados y repetibles (considerando las prácticas de seguridad).

  c. Formación en seguridad para el equipo de desarrollo.

d. Gestión de la calidad. Para garantizar el mínimo de defectos, de vulnerabilidades y la correcta ejecución del sistema de información.

e. Protección del entorno de desarrollo: Incluyendo los servidores, dispositivos de red, estaciones de trabajo y repositorio de código fuente.

f. Repositorios y prácticas de código seguro: Con permisos de acceso basados en roles y revisión de registros. Uso de patrones estandarizados de código seguro y reutilización de componentes certificados como seguros en futuros desarrollos.

4.3.5.3.2. Incorporación de la seguridad en la fase de Desarrollo/Adquisición

1. Las **actividades** clave de seguridad para esta fase incluyen:

- Llevar a cabo la evaluación del riesgo y utilizar los resultados para complementar los controles de seguridad de línea base;
- Analizar los requerimientos de seguridad.
- Realizar pruebas funcionales y de seguridad.
- Preparar documentos iniciales para la certificación de sistema.
- Diseñar la arquitectura de seguridad.

2. Los **puntos a controlar** en esta fase incluyen:

- Revisión del Diseño/Arquitectura para evaluar el diseño del sistema planificado y su potencial integración con otros sistemas así como la incorporación de servicios compartidos y controles de seguridad comunes (autenticación, recuperación de desastres, detección de intrusiones o notificación de incidentes).
- Revisión del desempeño del sistema para ver si cumple con las expectativas, si se comporta de la forma prevista o si está sujeto a usos indebidos.
- Revisión funcional del sistema para asegurar que los requisitos identificados están suficientemente detallados y se puedan comprobar.
- Revisión financiera y del estado del proyecto en su fase media para detectar a tiempo desviaciones y asegurar que se vigilan las relaciones de coste-beneficio y se toman decisiones eficaces.
- Revisión complementaria de decisiones de gestión de riesgos de ser necesaria por haberse producido cambios a consecuencia de las revisiones anteriormente mencionadas o por un cambio en los controles o requisitos de seguridad.

3. Desarrollo de **Actividades principales** de Seguridad:

- **Evaluación del riesgo del sistema:** Para evaluar el conocimiento actual de diseño del sistema, requisitos establecidos y requisitos de seguridad mínimos derivados del

proceso de categorización de seguridad y así determinar su eficacia para mitigar los riesgos con anticipación y como dicho sistema puede afectar a otros con los que esté conectado. Los resultados deben mostrar que los controles de seguridad especificados proporcionan protecciones apropiadas, los controles comunes que hay que impulsar, los riesgos adicionales que mitigar o resaltar las áreas donde se necesita una planificación adicional.

Para la realización con éxito de una evaluación de riesgos debe realizarse antes de la aprobación de especificaciones de diseño y deben participar las personas que conocen las disciplinas dentro del dominio del sistema.

Tras la evaluación del riesgo es posible que haya que revisar algunos pasos previamente dados como el BIA o la categorización del sistema.

- **Selección y documentación de controles de seguridad**: Conforme a las regulaciones legales y rentabilidad. Debiendo ser plasmado en un plan de seguridad

- **Diseño de la arquitectura del sistema con la seguridad integrada.** Generando un esquema gráfico de la integración de la seguridad dando detalles de dónde, cómo y en qué sistemas está implementada y compartida la seguridad.

- **Diseñar seguridad y desarrollar controles:** Durante esta etapa, los controles de seguridad se implementan y forman parte del sistema en lugar de aplicarlos al finalizar. De este modo, los problemas de rendimiento del sistema son detectados desde el principio. Además, algunos controles de seguridad pueden limitar o entorpecer las actividades de desarrollo normal.

  Durante esta tarea, las decisiones se toman en función de las dificultades de integración y los pros y contras. Es importante documentar las principales decisiones e impulsores de negocio o tecnológicos. En casos donde la aplicación de un control previsto no es posible o conveniente, se debe considerar y documentar los controles compensatorios.

  Esta tarea está directamente relacionada con la revisión del análisis de los requisitos y con la estrategia de la arquitectura de seguridad. Las configuraciones específicas de deben documentar o referenciar en el plan de seguridad.

- **Desarrollo de documentación de seguridad:** El documento más importante es el Plan de Seguridad y los documentos auxiliares incluyen: El plan de gestión de la configuración; Plan de contingencia; Plan de monitorización continua; Concienciación, formación y educación de Seguridad; Plan de respuesta a incidentes y Evaluación del impacto en la Privacidad (PIA).

  El desarrollo de estos documentos debe considerar la documentación de la madurez de los servicios de seguridad. La confección de estos documentos debe comenzar lo antes posible durante el proyecto.

  En esta etapa, es importante consolidar el enfoque de la seguridad, el alcance y la comprensión de las responsabilidades. Documentar a medida que avanza el desarrollo de sistema puede proporcionar ahorros de costos y mejorar las capacidades de toma de decisiones a través de un enfoque integral que permite la detección temprana de las carencias.

  La documentación del sistema de seguridad debe estar alineada con el Análisis de requisitos de seguridad, la arquitectura de seguridad, BIA y la categoría del sistema.

- Pruebas de comportamiento (de desarrollo, funcionales y de seguridad): Los sistemas desarrollados o sometidos a modificaciones de software, hardware o comunicación deben probados y evaluados antes de ser implementados. El objetivo del proceso de prueba y evaluación es validar que el sistema cumple con los requisitos funcionales y de seguridad.

  El proceso se centra en la especificidad, la repetitividad y la iteración. En cuanto a la especificidad: las pruebas estarán destinadas a probar requisitos de seguridad relevantes hechos expresamente para su uso en el entorno. En cuanto a la repetitividad: el proceso de prueba debe ser capaz ejecutar una serie de pruebas contra un sistema de información más de una vez (o sistemas similares en paralelo) y obtener resultados similares cada vez. Para la iteración, será necesario ejecutar pruebas funcionales (para cada sistema), en su totalidad o en parte, un número de veces sucesivas a fin de alcanzar un nivel aceptable de cumplimiento de los requisitos del sistema. Para lograr esto, las pruebas funcionales serán automatizada en la medida de lo posible, y se publicarán los casos de prueba, en detalle, para garantizar que el proceso de prueba es repetible y repetitivo. Solo se deben utilizar datos de prueba o de "código auxiliar" durante el desarrollo del sistema. Absolutamente ninguna información operacional, relacionada con la seguridad o identificable (PII) debe residir en los sistemas o software durante el desarrollo.

  Tras las pruebas, es probable que haya que modificar el análisis de requisitos de seguridad, la arquitectura de seguridad o la evaluación de riesgo del sistema.

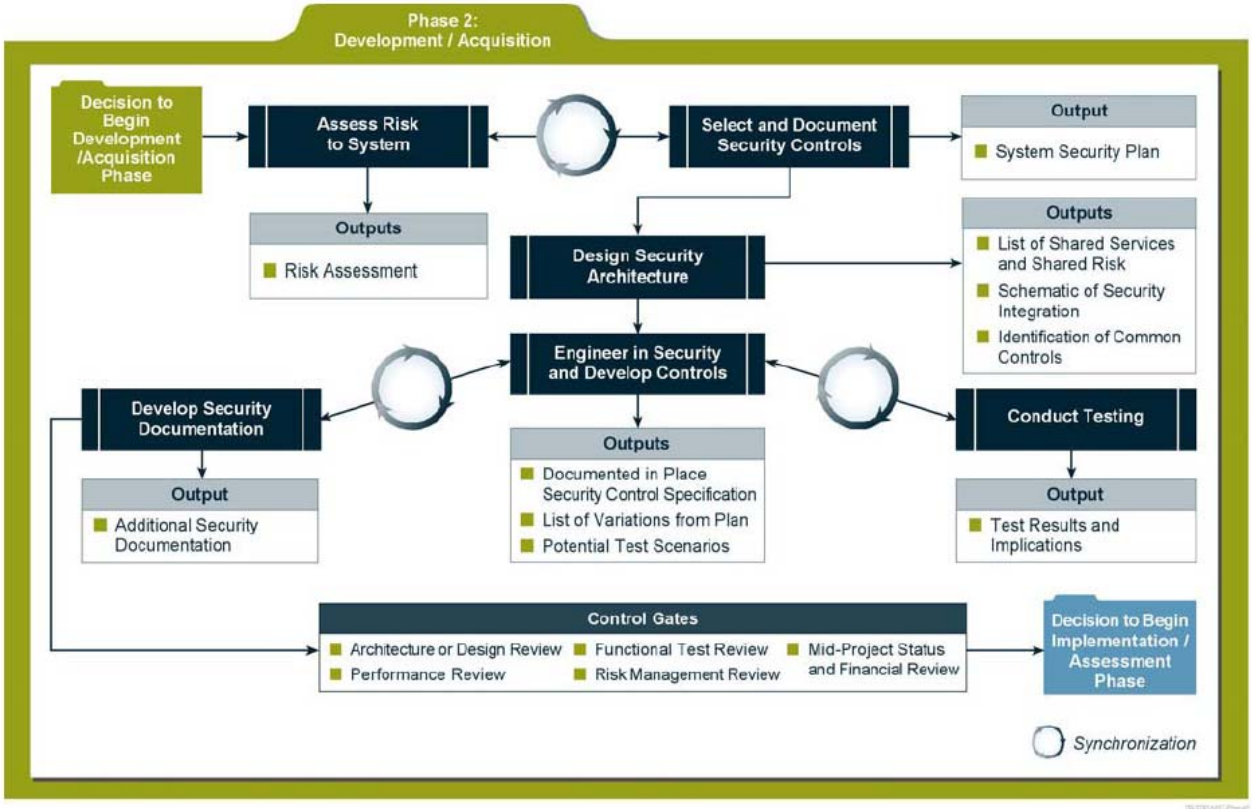

Ilustración 2: Consideraciones de seguridad relativas a la fase Desarrollo/Adquisición (NIST 800-64)

4.3.5.3.3. Incorporación de la seguridad en la fase de Implementación / Evaluación

Durante esta fase se instalará y evaluará el sistema en el entorno operacional de la organización.

1. Las **actividades** clave de seguridad para esta fase incluyen:
    - Integrar el sistema de información en su entorno
    - Planificar y llevar a cabo actividades de certificación del sistema sincronizándolas con las pruebas de los controles de seguridad.
    - Completar las actividades homologación del sistema.
2. Los **puntos a controlar** en esta fase incluyen:
    - Revisión de las pruebas de disponibilidad del sistema.
    - Revisión de la Certificación y homologación (C&A).
    - Revisión económica y del estado final del sistema.
    - Decisión del Responsable de la autorización.
    - Aprobación del despliegue o conexión de TI
3. Desarrollo de **Actividades principales** de Seguridad:
    - **Crear un plan detallado para la C&A**: El Responsable de la Autorización (AO) es el responsable de aceptar el riesgo del sistema, si éste le parece aceptable.
      Por lo que es fundamental que el equipo de desarrollo conozca con antelación el tipo y cantidad de evidencias (a obtener de las pruebas realizadas) que el AO requerirá para tomar la decisión. De este modo se podrá establecer un alcance y la adecuación de dichas pruebas para obtener los datos necesarios para determinar el riesgo residual.
      Esta actividad generará un Plan de trabajo inicial que identificará a los protagonistas principales, las limitaciones del proyecto, los componentes fundamentales, el alcance de las pruebas y el nivel de rigor esperado.
    - **Integrar la seguridad en los sistemas o entornos establecidos:** La integración y pruebas de aceptación se producen después de la instalación y ejecución del sistema de información. La configuración de los controles de seguridad se habilita de acuerdo con las instrucciones del fabricante, de las guías de implementación de seguridad disponibles y de los requisitos documentados de seguridad. De esta actividad se obtendrá un listado de controles operacionales de seguridad verificados y documentación completa del sistema.
    - **Evaluación del sistema de seguridad**: Los Sistemas desarrollados o sometidos a modificaciones de software, hardware o de comunicaciones deben evaluarse formalmente antes de homologarse oficialmente. El objetivo del proceso de evaluación de seguridad es confirmar que el sistema cumple con los requisitos funcionales y de

seguridad y operará dentro de un nivel aceptable de riesgo residual de seguridad. Además de comprobar la eficacia del control de seguridad, la certificación de seguridad puede descubrir y describir las vulnerabilidades reales en el sistema de información. La determinación de vulnerabilidades del sistema de información y la eficacia de control seguridad proporciona información esencial para facilitar a los responsables de autorización una toma de decisiones de homologación de seguridad creíble, basada en el riesgo.

Además, se realizarán pruebas periódicas y la evaluación de los controles de seguridad en un sistema de información para asegurar la eficacia continua.

De esta actividad se obtendrá el resultado escrito del paquete de homologación de la seguridad que se entregará al propietario del sistema, al administrador y al Responsable de Seguridad del sistema de información (ISSO).

- **Autorizar el sistema de Información:** Se requiere la autorización de seguridad de un sistema de información para procesar, almacenar o transmitir información. Esta autorización (también conocido como acreditación de seguridad), se basa en la eficacia comprobada de controles de seguridad con un nivel de garantía acordado y un riesgo residual identificado a los activos u operaciones (incluyendo la misión, función, imagen o reputación). Un autorización oficial se basa principalmente en: (i) el plan completo del sistema de seguridad; (ii) los resultados de pruebas y evaluación de seguridad; y (iii) el Plan de acción e Hitos (POA& M) para reducir o eliminar las vulnerabilidades del sistema de información, en la toma de decisión de autorización de seguridad para permitir la operación del sistema de información y en aceptar explícitamente el riesgo residual de activos u operaciones de la organización.

  De esta actividad se obtendrá el documento de la Decisión de Autorización de Seguridad que se entregará al propietario del sistema y al ISSO y el Paquete final de Autorización de Seguridad.

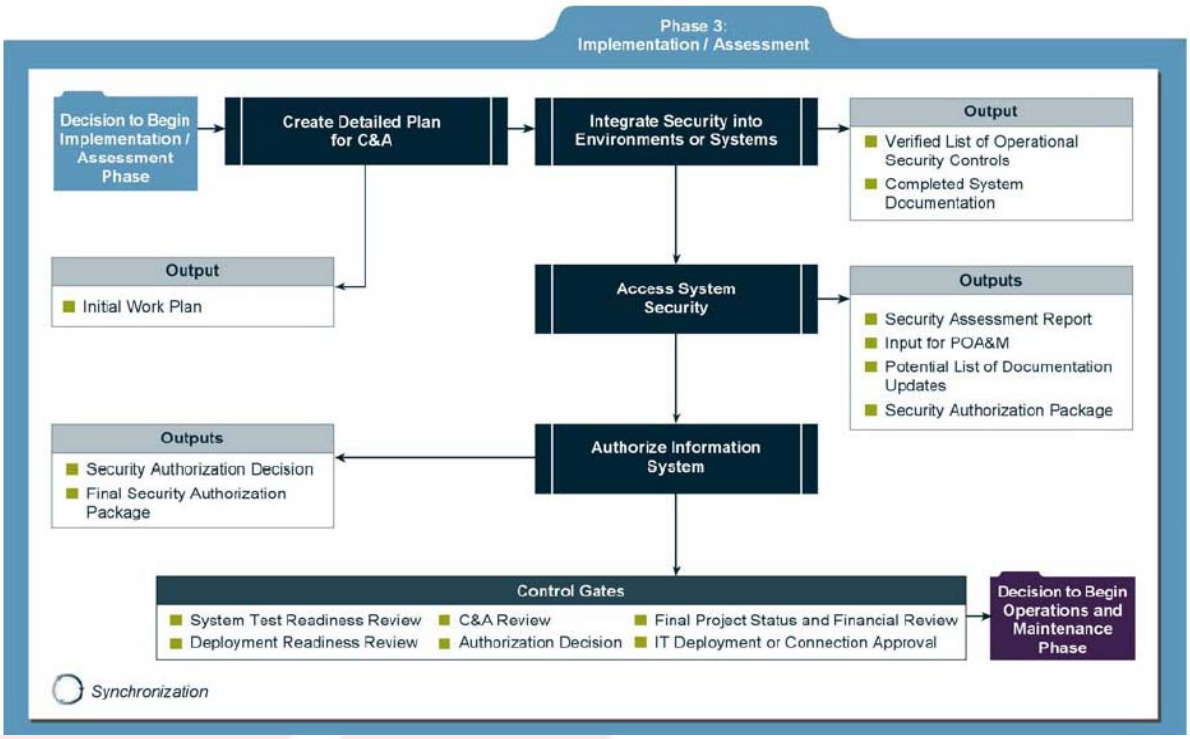

Ilustración 3: Consideraciones de Seguridad relativas a la fase de Implementación / Evaluación (NIST 800-64)

4.3.5.3.4. Incorporación de la seguridad en la fase de Operación / Mantenimiento

En esta fase, los sistemas están en funcionamiento. Se desarrollan y prueban mejoras o modificaciones en el sistema y se agrega o reemplaza hardware y/o software.

Se revisa continuamente el desempeño del sistema acorde con los requisitos de seguridad y se incorporan las modificaciones necesarias.

El sistema operativo se evalúa periódicamente para determinar cómo el sistema puede hacerse más eficaz, seguro y eficiente. Las operaciones continúan mientras el sistema se va adaptando para responder eficazmente a las necesidades de la organización manteniendo un nivel de riesgo acordado. Cuando se identifican modificaciones o cambios necesarios, el sistema puede volver a llevarse a una fase anterior de la SDLC.

1. Las **actividades clave** de seguridad para esta fase incluyen:
    - Llevar a cabo una revisión de disponibilidad operacional.
    - Administrar la configuración del sistema.
    - Crear procesos y procedimientos para las operaciones de seguridad y monitorización continua de los controles de seguridad del sistema de información.
    - Realizar la reautorización si fuera necesario.
2. Los **puntos a controlar** en esta fase incluyen:
    - Revisión de disponibilidad operacional.
    - Revisión de cambios propuestos al Comité de Control de Cambios
    - Revisión de POA&M's (Plan de acción e Hitos).
    - Decisiones de homologación (cada tres años o después de un gran cambio del sistema).
3. Desarrollo de **Actividades principales** de Seguridad:
    - **Revisión de disponibilidad operacional**: Muchas veces cuando un sistema se pasa a un entorno de producción, produce modificaciones imprevistas en el sistema. Si los cambios son significativos, puede necesitarse una prueba de controles de seguridad para garantizar la integridad de los mismos.
      Este paso no es siempre necesario; Sin embargo, se debe considerar para ayudar a mitigar el riesgo y abordar eficazmente sorpresas de última hora

- **Realizar Control y Gestión de la configuración**: Una política de gestión y control eficaz de la configuración y los procedimientos asociados son indispensables para asegurar la consideración adecuada de los impactos potenciales de seguridad debido a los cambios específicos en un sistema de información o su entorno.
  Los Procedimientos de gestión y control de configuración son fundamentales para establecer una línea de base inicial de componentes de hardware, software y firmware para el sistema de información y, posteriormente, para controlar y mantener un inventario preciso de los cambios en el sistema.
  La arquitectura de seguridad debería proporcionar detalles claves sobre el servicio de seguridad a nivel de componente, lo cual proporciona un punto de referencia para evaluar el impacto del cambio planificado.
  Esta actividad generará actualizaciones en los documentos de seguridad y documentos de evaluaciones de seguridad de los cambios del sistema.

- **Llevar a cabo monitorización continua**: El objetivo final del monitoreo continuo es determinar si los controles de seguridad en el sistema de información siguen siendo eficaces en el tiempo a la vista de los inevitables cambios que se producen en el sistema, así como el entorno en que opera el sistema.
  Un proceso de supervisión continuo bien diseñado y bien administrado puede transformar la evaluación de control de seguridad y proceso de determinación del riesgo estáticas en un proceso dinámico que proporciona información de estado de seguridad esencial casi en tiempo real. Esta información puede utilizarse para tomar acciones adecuadas de mitigación de riesgo y tomar decisiones de autorizaciones creíbles, basadas en el riesgo con respecto a la continuidad del funcionamiento del sistema de información y la aceptación explícita de riesgo resultante de esa decisión.
  Los resultados de la monitorización continua deben ser documentados y se deben documentar además las revisiones de seguridad, métricas, medidas y análisis de tendencias.

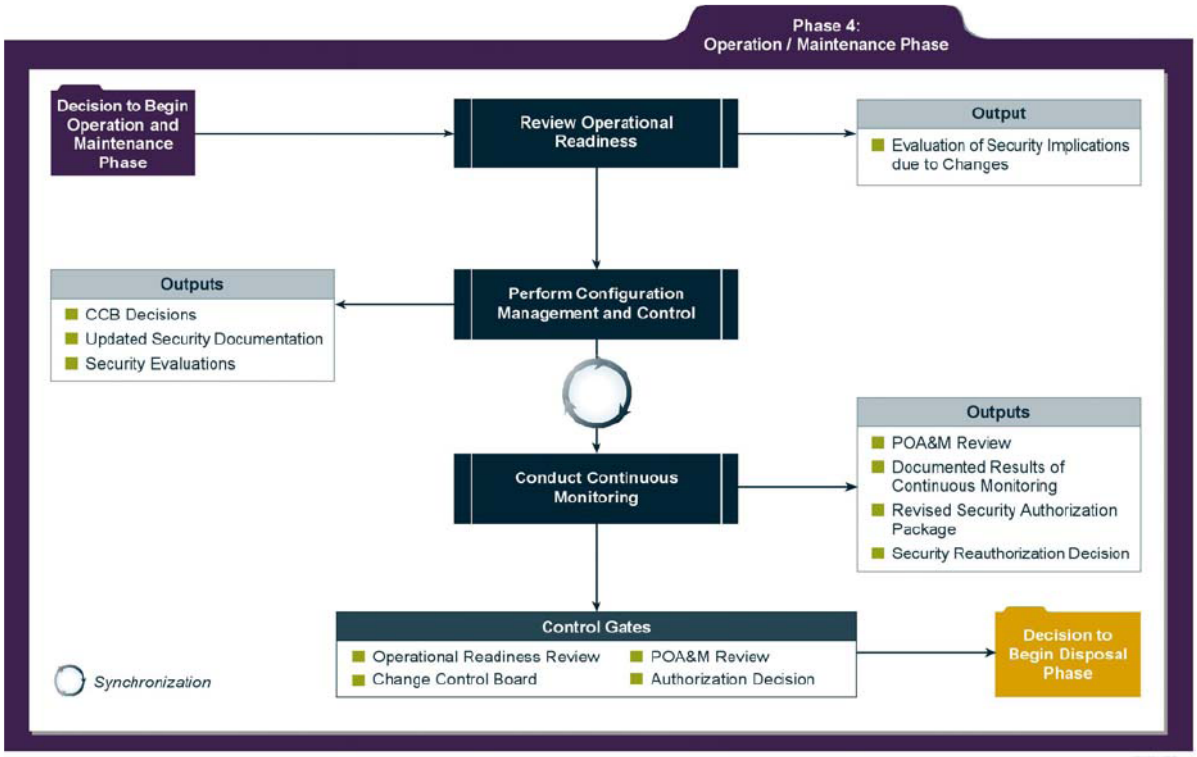

Ilustración 4: Consideraciones de seguridad relativas a la fase de Operación / Mantenimiento (NIST 800-64)

4.3.5.3.5. Incorporación de la seguridad en la fase de Eliminación

Las actividades llevadas a cabo durante esta fase garantizan el cese ordenado del sistema, salvaguardar la información vital del sistema para la migración de sus datos a un nuevo sistema o para su conservación de conformidad con las políticas y normativas aplicables.

1. Las **actividades clave** de seguridad para esta fase incluyen:
    - Crear y ejecutar un Plan de transición/eliminación.
    - Archivado de información crítica.
    - Limpieza de los soportes de almacenamiento.
    - Eliminación de hardware y software.
2. Los **puntos a controlar** en esta fase incluyen:
    - Revisión del cierre del sistema.
    - Comité del Control de Cambios.
    - Revisión de Seguridad del cierre.
3. Desarrollo de **Actividades principales** de Seguridad:
    - **Crear y ejecutar un Plan de transición/eliminación**: La creación de un plan de transición/eliminación documentado garantiza que todas las partes interesadas son conscientes del plan de futuro para el sistema y su información. Este plan debe dar cuenta del estado de la transición/eliminación para todos los componentes críticos, servicios e información. Como la mayoría de los planes de trabajo, este plan identifica los pasos, decisiones e hitos necesarios para el cierre correcto, transición o migración de un sistema o su información.
      En muchos casos, sistemas eliminados o los componentes del sistema han permanecido inactivos pero aún conectados a la infraestructura. Como resultado, a menudo se pasan por alto estos componentes, de modo que no mantienen una protección de seguridad óptima por lo que suponen un riesgo adicional e innecesario a la infraestructura y todos los sistemas conectados. Un plan de transición ayuda a mitigar estos posibles desenlaces. Como resultado de esta acción se deben actualizar los documentos y el plan de seguridad. Se debe elaborar un índice de la información preservada así como su localización y las características de retención.
    - **Garantizar la conservación de la información**: Cuando se preserva la información, las organizaciones deberían considerar los métodos que serán necesarios para recuperarla en el futuro, ya que la tecnología utilizada para recuperar los registros podría no estar

disponible (especialmente si está cifrada). Deben considerarse los requisitos legales para la retención de registros cuando se eliminan de los sistemas.

- **Limpieza de los soportes:** La organización limpia o destruye los soportes de información digitales del sistema antes de su eliminación o liberación para su reutilización fuera de la organización, para evitar que personas no autorizadas puedan acceder y usar la información contenida en los soportes.
  La limpieza de soportes se puede dividir en cuatro categorías: eliminación, borrado, depuración y destrucción. Además, sugiere que el propietario del sistema clasifique la información, evalúe la naturaleza del soporte en el que se registró así como el riesgo para la confidencialidad y determine los planes futuros para los soportes. Entonces, debe decidir sobre el proceso de limpieza adecuado, evaluando el costo, impacto ambiental, etc.
  Se deben generar registros de eliminación de los soportes.

- **Eliminación de hardware y software**: El hardware y software se pueden ser vendidos, regalados o descartados según lo dispuesto por la ley o reglamento aplicable. La eliminación del software debe cumplir con la licencia (u otros acuerdos con el desarrollador) y las reglamentaciones gubernamentales. Rara vez es necesario destruir hardware excepto para algunos medios de almacenamiento que contiene información confidencial y que no pueden ser limpiados sin ser destruidos. A veces es posible la eliminación y destrucción física de los soportes para que el hardware restante puede ser vendido o regalado. Pero algunos sistemas pueden contener información confidencial, después de quitar el soporte de almacenamiento.
  Se deben generar registros de eliminación de hardware y software y actualizar los inventarios.

- **Cierre del sistema**: El sistema de información es formalmente apagado y desmontado al llegar a este punto.
  Se debe generar la documentación de verificación del cierre del sistema incluyendo las notificaciones de las autorizaciones.
  Se debe archivar la documentación de seguridad de forma apropiada, actualizar los inventarios y notificar el cierre a los servicios de monitorización.

4.3.6. Protección frente al malware

4.3.6.1. Objetivos

Malware es la combinación de dos palabras inglesas, malicious software, también conocido como código malicioso o software malicioso en español. Se define como un programa que se instala en nuestro sistema operativo con la intención de comprometer la confidencialidad, la integridad y/o la disponibilidad de los datos del sistema infectado, las aplicaciones o el sistema operativo causando problemas o interrupciones en el sistema en el cual se ha instalado.

El malware se ha convertido en la amenaza externa más importante para la mayoría de los sistemas, causando daños generalizados, interrupciones y la necesidad de realizar, en la

mayoría de las organizaciones, inversiones de prevención para esta clase de ataques y de recuperación de sistemas en el caso de haber sido infectados.

Aunque la violación de la privacidad a través del malware se ha venido usando durante muchos años, se generalizado mucho más recientemente.

Esta guía contiene recomendaciones para que las empresas minimicen el impacto de un incidente producido por malware. También se incluyen nuestras recomendaciones para mejorar la capacidad de respuesta de una empresa ante un incidente de este tipo.

4.3.6.2. Descripción

Esta sección presenta las recomendaciones para prevenir incidentes de malware dentro de una organización. Los cuatro elementos principales de la prevención son la política, la concienciación, minimizar vulnerabilidades y minimizar amenazas.

El primer paso es asegurar que las políticas de prevención de malware proporcionan una base para la aplicación de controles preventivos. El establecimiento y mantenimiento general de programas de concienciación para todos los usuarios, así como la formación específica para el personal de sistemas que participan directamente en la prevención, son fundamentales para reducir el número de incidentes que ocurren por errores humanos.

Los esfuerzos empleados en la reducción de la vulnerabilidad pueden eliminar algunas posibles causas de ataque. La implementación de una combinación de técnicas de minimización de amenazas, tales como software antivirus y cortafuegos, pueden prevenir las amenazas de ataques con éxito en nuestros sistemas y redes.

Al planear un enfoque para la prevención de malware, las organizaciones deben ser conscientes de los puntos de ataque que son más susceptibles de ser utilizados en la actualidad y en el futuro próximo. Además, las organizaciones deben incorporar los medios existentes, tales como la implementación de software antivirus y programas de gestión de actualizaciones en sus esfuerzos de prevención de malware. Sin embargo, las organizaciones deben ser conscientes de que no importa cuánto esfuerzo se pone en la prevención de incidentes de software malicioso, los incidentes se seguirán produciendo. Por esta razón, las organizaciones deben tener una buena gestión de incidentes de malware para limitar el daño que el malware puede causar y tener un sistema eficiente para la restauración de datos y servicios.

4.3.6.3. Política

Las organizaciones deben redactar políticas de prevención de incidentes malware.

Si una organización no indica con claridad los términos de prevención de malware en sus políticas, es poco probable que se puedan llevar a cabo actividades de prevención de malware coherentes y eficaces en toda la organización.

Estas son algunas consideraciones comunes para la prevención de malware relacionadas con la política:

- Exigir el escaneo de cualquier dispositivo externo de la organización en busca de malware antes de utilizarlo.
- Exigir que los archivos adjuntos de correo electrónico, incluyendo archivos comprimidos (por ejemplo, archivos .zip), sean analizados antes de abrirlos.
- Prohibir el envío o la recepción de ciertos tipos de archivos (por ejemplo, archivos .exe) a través del correo electrónico.
- Restricción del uso de los privilegios de administrador a los usuarios, limitando los privilegios a disposición de los programas maliciosos introducidos en los sistemas por los usuarios.
- Configurar actualizaciones automáticas en el sistema operativo, las actualizaciones de aplicaciones y parches.
- Restricción del uso de medios extraíbles (por ejemplo, discos, discos compactos [CD], bus serie universal [USB] de unidades de memoria flash).
- Especificar qué tipos de programas de prevención (por ejemplo, el software antivirus, detección de spyware y utilidades de eliminación) son necesarios para cada tipo de sistema y una lista de los requisitos para la configuración y el mantenimiento del software (por ejemplo, la frecuencia de actualización de software, el sistema de cobertura de análisis y frecuencia).
- Permitir el acceso a otras redes (incluido Internet) sólo a través de los medios de la organización aprobados y garantizados.
- Segmentación de redes para reducir el impacto en caso de una infección por cualquier tipo de malware.
- Restricción del uso de dispositivos móviles en la red corporativa.

4.3.6.4. Concienciación

Un programa de concienciación eficaz explica las reglas de buen uso de los sistemas de información de una empresa. En consecuencia, el programa de sensibilización debe incluir orientación a los usuarios acerca de la prevención de incidentes de malware, que puede ayudar a reducir la frecuencia y gravedad de los incidentes malware. Todos los usuarios dentro de una organización deben ser conscientes de las formas en que el malware entra en los sistemas, las infecta y se propaga y los riesgos que el malware plantea. Además, el programa de concienciación debe abarcar las consideraciones de prevención de incidentes de malware en la organización políticas y procedimientos, así como las prácticas que se recomiendan para evitar incidentes de malware. Ejemplos de estas prácticas son los siguientes:

- No abrir correos electrónicos sospechosos o archivos adjuntos de correo electrónico de remitentes desconocidos o conocidos.
- No hacer clic en las ventanas emergentes del explorador web sospechosas.

- No abrir archivos con extensiones de archivo que pueden estar asociados con programas maliciosos (por ejemplo, .bat, .com, .exe, .pif, .vbs).
- No desactivar los mecanismos de seguridad adicionales de control (por ejemplo, el software antivirus, detección de spyware o el cortafuegos).
- No utilizar cuentas de administrador para el funcionamiento del sistema.
- No descargar o ejecutar aplicaciones de fuentes no confiables.

Las organizaciones deben tener a los usuarios al tanto de las políticas y procedimientos que se aplican a la manipulación de programas maliciosos y la forma de identificar si un sistema puede estar infectado, cómo reportar una sospecha de infección y lo que los usuarios pueden hacer para ayudar en el tratamiento de incidentes.

Como parte de las actividades de sensibilización, las organizaciones deben educar a sus usuarios sobre las técnicas que los delincuentes utilizan para engañar a los usuarios para que revelen información. Las organizaciones también deben proporcionar a los usuarios recomendaciones para evitar los ataques de *phishing*. Ejemplos de esas recomendaciones son las siguientes:

- Nunca responda a solicitudes por correo electrónico que solicitan información financiera o personal. Las organizaciones no deberían pedir información por correo electrónico, ya que es susceptible de control por terceros no autorizados.
- No proporcionar contraseñas, números PIN u otros códigos de acceso en respuesta a correos electrónicos o ventanas emergentes no solicitadas.
- No abra archivos adjuntos sospechosos de correo electrónico, incluso si provienen de remitentes conocidos.

Aunque los programas de sensibilización ayudan a reducir la frecuencia y gravedad de los incidentes de software malicioso, su impacto suele ser menor en comparación con las herramientas específicas como puede ser el software antivirus o un cortafuegos. Una organización no debe basarse en el conocimiento del usuario como su principal método de prevención de incidentes de malware, sino que deben complementar las herramientas implementadas para proporcionar protección adicional contra incidentes.

4.3.6.5. Minimizar vulnerabilidades

Los ataques de malware normalmente se producen a través de la explotación de vulnerabilidades en sistemas operativos, servicios y aplicaciones. Por consiguiente, minimizar las vulnerabilidades es muy importante para la prevención de incidentes de malware, sobre todo cuando el malware es liberado poco después del anuncio de una nueva vulnerabilidad, o incluso antes de que la vulnerabilidad sea reconocida públicamente. Una vulnerabilidad por lo general puede ser evitada por uno o más métodos, como la aplicación de parches o actualizaciones para actualizar el software o volver a configurar el software (por ejemplo, deshabilitar un servicio vulnerable).

Debido a los retos que representan la minimización de vulnerabilidades, incluyendo el manejo del continuo descubrimiento de nuevas vulnerabilidades, las organizaciones deben tener procesos y procedimientos documentados para reducir vulnerabilidades y también debe considerar la creación de un programa de gestión de vulnerabilidades.

También se deben evaluar vulnerabilidades constantemente para priorizar adecuadamente los esfuerzos de reducción de vulnerabilidades. Se debe buscar información sobre nuevas vulnerabilidades y las principales amenazas de nuevo malware a través de una combinación de fuentes, tales como los boletines de los CERTs (como, por ejemplo, el INTECO CERT - http://cert.inteco.es/cert) o los avisos de malware de los fabricantes de software antivirus. Las organizaciones también deben establecer un mecanismo de evaluación y seguimiento de vulnerabilidades y de notificación de amenazas.

Las técnicas que figuran en esta lista se podría aplicar a casi cualquier sistema, pero son particularmente útiles para la protección contra el malware:

- Herramientas de seguridad como el software antivirus pueden detectar y detener el malware antes de que alcance sus objetivos previstos.
- Gestión de parches y actualizaciones. La aplicación de parches y actualizaciones a los sistemas es la forma más común de reducir vulnerabilidades conocidas en sistemas operativos y aplicaciones. La gestión de parches implica varios pasos, incluyendo la evaluación de la criticidad de los parches y el impacto de que la aplicación pueda utilizarse o no.
- Antes de aplicar cualquier parche o actualización a nuestro sistema es necesario probarlos a fondo, la aplicación de los parches se debe hacer de una manera controlada y habrá que documentar la evaluación de parches y el proceso de decisión. Cada vez es más difícil de implementar los parches con la suficiente rapidez. El tiempo transcurrido desde el anuncio de una nueva vulnerabilidad hasta que aparece nuevo malware aprovechando esa vulnerabilidad se ha reducido de meses a semanas o días.
- A menudo no es posible o prudente implementar parches en toda la organización de inmediato, en algunos casos, es más seguro utilizar otras técnicas de reducción de vulnerabilidades y amenazas en lugar de parches porque incluso cuando un parche ha sido probado a fondo y se ha comprobado que es aceptable, a menudo es difícil asegurar que se aplicará a todas las máquinas vulnerables de la organización. Actualmente la aplicación de parches es una de las maneras más eficaces de reducir el riesgo de incidentes de malware, y muchos casos de malware han tenido éxito porque los sistemas no estaban parcheados de manera oportuna.
- Privilegio mínimo. El principio de mínimo privilegio se refiere a la configuración de los sistemas a prestar los servicios y privilegios mínimos necesarios. Esto puede ser útil en la prevención de incidentes de software malware ya que a menudo requiere se requieren privilegios de administrador para explotar las vulnerabilidades con éxito.

- Otras medidas. Las organizaciones también deben considerar la implementación de otras medidas de protección de los servidores que pueden reducir aún más la posibilidad de incidentes de malware. Ejemplos de tales medidas son las siguientes:
    - Deshabilitar o quitar servicios innecesarios (en particular los servicios de red) que podrían contener vulnerabilidades.
    - Eliminar archivos compartidos que no cumplen los requisitos de seguridad, estos son un mecanismo de infección común de los gusanos.
    - Quitar o cambiar nombres de usuario y contraseñas por defecto a los sistemas operativos y a las aplicaciones, lo que podría ser utilizado por el malware para obtener acceso no autorizado a los sistemas.
    - Requerir autenticación para permitir el acceso a un servicio de red.
    - Deshabilitar la ejecución automática de archivos binarios y secuencias de comandos.

4.3.6.6. Minimizar amenazas (herramientas)

Además de los esfuerzos para minimizar vulnerabilidades, las organizaciones deben minimizar las amenazas para detectar y detener el malware antes de que pueda afectar a sus objetivos.

En esta sección se describen varios tipos de herramientas de seguridad que pueden reducir las amenazas de malware: el software antivirus, servicios de detección y eliminación de *spyware*, sistemas de prevención de intrusiones (IPS – *Intrusion Prevention Systems*) y cortafuegos y routers.

4.3.6.6.1. Software antivirus

El software antivirus es el medio más utilizado en las técnicas para la reducción de amenazas malware. Para los sistemas operativos y las aplicaciones que son objetivo del malware, el software antivirus se ha convertido en una necesidad para la prevención de incidentes. Hay muchas compañías de software antivirus, y la mayoría proporcionan una protección similar a través de estas funcionalidades:

- Escaneado de componentes críticos del sistema tales como archivos de inicio y los registros de arranque.
- Actividades de monitorización en tiempo real para detectar actividades sospechosas, un ejemplo común es escanear todos los archivos adjuntos de correo electrónico. El software antivirus debe estar configurado para realizar análisis en tiempo real de cada archivo que se descarga, abre o ejecuta.
- Seguimiento del correcto funcionamiento de las aplicaciones, como clientes de correo electrónico, navegadores web, programas de transferencia de archivos y software de mensajería instantánea.

- Análisis de archivos de virus conocidos. El software antivirus en los sistemas debe ser configurado para analizar todos los discos duros con regularidad para identificar las infecciones del sistema de archivos y, opcionalmente, para explorar otros medios de almacenamiento. Los usuarios también deben ser capaces de iniciar un escaneo manualmente si es necesario, esto se conoce como análisis bajo demanda.

4.3.6.6.2. Herramientas de detección y eliminación Spyware

Las herramientas de detección y eliminación de spyware están diseñadas para identificar, poner en cuarentena y eliminar muchos tipos de spyware en los sistemas de archivos. La prevención de incidentes spyware es importante, no sólo porque violan la privacidad de los usuarios, sino también porque con frecuencia causan problemas funcionales en los sistemas. Este tipo de herramientas deben tener las siguientes funcionalidades:

- Realizar un seguimiento del comportamiento de las aplicaciones más susceptibles de ser infectadas, como son los navegadores web o los clientes de correo electrónico.
- Realizar exploraciones periódicas de los archivos, memoria y archivos de configuración.
- Identificación de varios tipos de spyware, incluyendo el código malicioso móvil, troyanos, cookies de seguimiento y poner en cuarentena o eliminar archivos de spyware.
- Monitorizar controladores de red.
- Monitorizar procesos y programas que se cargan automáticamente al arrancar el sistema operativo.
- Prevenir distintos métodos de infección spyware como las cookies de seguimiento o los complementos de los navegadores.

4.3.6.6.3. Sistema de Prevención de Intrusiones (IPS)

Las redes basadas en Sistemas de Prevención de Intrusiones (IPS) realizan la detección de paquetes y analizan el tráfico de red para identificar y detener actividades sospechosas. Las soluciones basadas en redes IPS se implementan normalmente en línea, lo que significa que el software actúa como un firewall de red que recibe los paquetes, los analiza y decide si se le debe permitir circular por la red. Este tipo de arquitecturas de redes basada en IPS permiten que se detecten muchos ataques antes de que alcancen sus objetivos. La mayoría de los productos basados en red IPS utilizan una combinación de firmas de ataques y el análisis de protocolos de red, lo que significa que comparan la actividad de la red con la actividad de las aplicaciones que son normalmente atacadas (por ejemplo, servidores de correo electrónico, servidores web) esperando identificar actividades potencialmente maliciosas.

Los IPS son altamente personalizables, permitiendo a los administradores crear e implementar firmas de ataques de muchas de las amenazas de malware en cuestión de minutos, aunque existen riesgos al hacer esto, por ejemplo una firma mal escrita puede provocar falsos positivos los cuales pueden bloquear la actividad benigna sin darse cuenta.

Para las amenazas de malware que generan un gran volumen de tráfico, como los gusanos, los IPS pueden reducir significativamente la sobrecarga de tráfico que el malware puede provocar en la red de la organización. Usando una combinación de software antivirus y software IPS no sólo se puede mejorar la tasa de incidencias malware, también puede ser útil a la hora de dividir la carga del manejo del malware. Durante un ataque, el software antivirus puede llegar a sobrecargarse debido a la cantidad de eventos que pueden suceder, dividir el trabajo entre varios tipos de controles pueden reducir la saturación de los sistemas causados por el procesamiento del malware.

4.3.6.7. Ejemplos de mejores prácticas

4.3.6.7.1. Minimizar los daños después de un incidente de tipo malware

Desarrollar e implementar un plan de prevención ante un incidente de tipo malware es esencial.

Las organizaciones deben planificar e implementar un plan de prevención ante incidentes malware basado en los puntos débiles que más se utilizan actualmente y las que se pueden llegar a utilizar en un futuro cercano adelantándose a un posible ataque y a sus consecuencias.

Hay que tener en cuenta que la efectividad de estas técnicas de prevención pueden variar dependiendo del entorno en que se establezcan por lo que cada empresa deberá seleccionar el método y las herramientas que más se adapten a sus necesidades.

Una empresa debe enfocar la prevención de incidentes de tipo malware implementando diferentes tipos de políticas de seguridad y de uso de los recursos de la empresa entendiendo por recurso, cada ordenador y la información que estos contienen, cada persona, cada papel o cada activo que se utiliza para el desarrollo de la actividad propias de la empresa.

Hay que concienciar y formar a los trabajadores de los riesgos que suponen estas amenazas ya que si estos están concienciados y formados podremos minimizar el número de amenazas y minimizar el impacto si sufrimos un ataque.

4.3.6.7.2. Garantizar políticas de apoyo a la prevención de incidentes de malware

Los puntos de la política de seguridad de cada organización se deben utilizar como base para la prevención de ataques malware. Estas políticas están dirigidas a los trabajadores y deben servir para sensibilizarles ante estas amenazas. Las políticas deben hacer referencia a minimizar vulnerabilidades y a implantar herramientas de seguridad y su configuración. Si una organización no indica con claridad los puntos de prevención de malware a la hora de redactar su política, es poco probable que se puedan llevar a cabo actividades de prevención de malware coherentes y eficaces.

Las políticas de prevención de malware deben ser tan genéricas como sea posible para permitir flexibilidad en la aplicación de las políticas y reducir la necesidad de actualizaciones frecuentes de las mismas, no obstante también deben ser lo suficientemente específicas para que el objetivo y el alcance de la política estén lo suficientemente claros.

La política debe incluir apartados relativos a los sistemas de trabajo remoto controlados por la organización y a los sistemas que están fuera del control de la organización (los ordenadores

de los proveedores y clientes, los ordenadores de los empleados que puedan realizar su trabajo desde su propia casa, dispositivos móviles, etc.…).

4.3.6.7.3. Incorporar la prevención de incidentes y procedimientos de utilización de software malicioso en las políticas

Se deben implementar políticas de sensibilización que incluyan la orientación a los usuarios sobre la prevención de incidentes de malware. Todos los usuarios deben ser conscientes de las formas en que se propaga el malware, los riesgos que representa, la incapacidad de los sistemas de prevención implementados en la empresa para evitar que suceda algún incidente y la importancia que tienen los usuarios en la prevención de los mismos.

Las políticas de sensibilización también deben hacer llegar a los usuarios cuales son los medios y los procedimientos que se aplican a la hora de manipular programas maliciosos, la forma de detectar malware en un ordenador, cómo reportar sospechas de infecciones y lo que los usuarios pueden hacer para ayudar a resolver incidentes. Además, se deben llevar a cabo actividades de sensibilización para el personal involucrado en la prevención de incidentes de malware y proporcionar formación en tareas específicas de prevención y resolución de incidentes de malware.

4.3.6.7.4. Capacidad de minimizar las vulnerabilidades para ayudar a prevenir incidentes de malware

Las organizaciones deben tener políticas documentadas de procesos y procedimientos de actuación detallados para minimizar las vulnerabilidades del sistema operativo y de las aplicaciones que el malware puede explotar. Una vulnerabilidad, por lo general, se puede solucionar a través de uno o más métodos, por lo que se debería utilizar una combinación adecuada de técnicas, incluyendo la gestión de actualizaciones, la aplicación de guías de configuración de seguridad, listas de control y medidas adicionales de protección de los servidores, esto nos aporta distintas técnicas eficaces para diferentes tipos de vulnerabilidades.

4.3.6.7.5. Capacidad de minimizar las amenazas para ayudar en la contención de los incidentes de malware

Se deben realizar esfuerzos de minimización de amenazas para detectar y detener el malware antes de que pueda afectar a sus objetivos.

La herramienta más utilizada para reducir amenazas es el software antivirus, se recomienda instalar software antivirus en todos los sistemas para los que existe este tipo de software.

Existen otras técnicas adicionales que son útiles para la reducción de amenazas de malware, son los sistemas de prevención de intrusos, firewalls y routers.

4.3.6.7.6. Rápida capacidad de respuesta ante incidentes de malware

El proceso de respuesta a incidentes tiene cuatro fases principales:

FASE 1. Preparación.

Se deben realizar medidas preparatorias para garantizar que puedan responder eficazmente a incidentes malware. Las acciones recomendadas incluyen:

- Desarrollo de políticas específicas de incidentes malware y procedimientos de actuación.
- Realización regular de formación orientada a la prevención y eliminación de malware, realización de simulacros y pruebas de contingencia.
- Designación de responsables de seguridad que se encargaran de coordinar las respuestas a los incidentes malware.
- Establecimiento de varios mecanismos de comunicación para que la coordinación entre los responsables de seguridad, personal técnico, de gestión y los usuarios no se interrumpa aunque ocurra un incidente malware.

FASE 2. Detección y Análisis.

Es necesario esforzarse por detectar y validar las incidencias malware rápidamente porque las infecciones pueden propagarse en cuestión de minutos. La detección temprana puede ayudar a reducir al mínimo el número de sistemas infectados, lo que disminuirá la magnitud de los esfuerzos de recuperación y la cantidad de daño ocasionado. Las acciones recomendadas incluyen:

- Monitorizar avisos, registros y alertas producidos por los diferentes sistemas y aplicaciones (por ejemplo, software antivirus, servicios de detección de spyware o sistemas de detección de intrusos) para identificar posibles incidentes inminentes de malware. Este seguimiento proporciona la oportunidad de evitar incidentes, modificando su respuesta de seguridad.
- Instalación de herramientas de seguridad en un medio extraíble que contenga aplicaciones actualizadas para la identificación de malware, que tengan la funcionalidad de administrar los procesos actualmente en ejecución y sean capaces de realizar otras acciones de análisis.
- Establecimiento de un conjunto de criterios de priorización que identifican el nivel adecuado de respuesta para diferentes tipos de incidentes relacionados con el malware.

FASE 3. Contención.

La contención de incidentes malware tiene dos componentes principales:

- Detener la propagación de malware
- Prevenir daños mayores a los sistemas.

Casi todos los incidentes malware requieren acciones de contención. Al abordar un incidente es importante decidir qué métodos de contención se van a emplear antes de comenzar a actuar. Se debe contar con estrategias y procedimientos para la toma de decisiones relacionadas con la contención que reflejen el nivel de riesgo aceptable para la organización.

Las estrategias de contención deben detallar una metodología a los responsables de la resolución del incidente a la hora de seleccionar la combinación adecuada de métodos de contención para una situación particular. Las políticas deben establecer claramente quién tiene la autoridad para tomar decisiones importantes de contención. Las recomendaciones específicas relacionadas con la contención, son las siguientes:

- Proporcionar a los usuarios instrucciones sobre cómo identificar las infecciones y las medidas a adoptar si un sistema está infectado, sin embargo, no se debe confiar principalmente en los usuarios como medio de contención de incidentes de malware.

- Si el malware no puede ser identificado y contenido por el software antivirus, es necesario estar preparados para utilizar otras herramientas de seguridad para contenerlo. Se debe estar preparado para presentar copias de malware desconocidos a los proveedores de software de seguridad para su posterior análisis, así como ponerse en contacto con organismos especializados en seguridad de la información y respuesta a incidentes como INTECO-CERT (http://cert.inteco.es), cuando se necesita orientación sobre el manejo de las nuevas amenazas.

- Las organizaciones deben estar preparadas para cerrar o bloquear servicios como el correo electrónico en el caso que esté siendo víctima de un ataque malware para contener un incidente y debe asumir las consecuencias de hacerlo. Es necesario estar preparado para responder a los problemas causados a otras organizaciones si están siendo víctimas de un ataque malware que está utilizando nuestros recursos desactivando nuestros propios servicios.

- Capacidad para efectuar restricciones temporales a la conectividad de la red para contener un incidente malware, como la suspensión de acceso a Internet o desconectar físicamente los sistemas de la red, asumiendo el impacto que las restricciones podrían tener sobre la actividad de la organización.

La identificación de los puestos infectados por el malware es otro paso fundamental en la contención de muchos incidentes de malware. Este proceso a menudo resulta complicado por la naturaleza dinámica de la informática (por ejemplo, acceso remoto, usuarios móviles). Se deben considerar cuidadosamente las cuestiones de identificación antes que un incidente de malware a gran escala se produzca de manera que los responsables de seguridad estén preparados para utilizar múltiples estrategias para la identificación de los puestos infectados como parte de sus métodos de contención.

Las organizaciones deberían poder seleccionar entre una gama suficientemente amplia de métodos de identificación, elaborar procedimientos y tener la capacidad técnica necesaria para realizar cada enfoque elegido eficazmente cuando un incidente de malware ocurre.

- Erradicación. El objetivo principal de la erradicación es eliminar el malware procedente de los sistemas infectados. Debido a la necesidad potencial de los esfuerzos de erradicación, se debe estar preparado para utilizar varias combinaciones de técnicas de erradicación al mismo tiempo para diferentes situaciones.

- Considerar la realización de actividades de concienciación que establezcan expectativas de los esfuerzos de erradicación y recuperación de los sistemas, estas actividades pueden ser útiles para reducir el impacto que los principales incidentes de software malicioso pueden causar.

- Recuperación. Los dos principales aspectos de la recuperación de los incidentes de malware son restaurar la funcionalidad de los sistemas infectados, recuperar el acceso a los datos y el levantamiento de medidas provisionales de contención.

Las organizaciones deben considerar cuidadosamente los posibles escenarios y determinar cómo se debe realizar la recuperación, incluyendo la reinstalación de los sistemas comprometidos desde cero o bien restaurar copias de seguridad que no hayan sido infectadas. La determinación de cuándo retirar las medidas temporales de contención, tales como la suspensión de los servicios o la conectividad, es a menudo una decisión difícil, durante los incidentes de malware los equipos de respuesta a incidentes debe esforzarse por mantener las medidas de contención en el lugar hasta que el número estimado de los sistemas infectados y los sistemas vulnerables a la infección sea lo suficientemente bajo para que los incidentes posteriores sean mínimos.

FASE 4. Actividad posterior a un incidente.

El manejo de incidentes de software malicioso puede ser muy costoso, es especialmente importante llevar a cabo una evaluación seria de las lecciones aprendidas después de los incidentes de malware para prevenir incidentes similares en el futuro. La documentación de las lecciones aprendidas en el manejo de incidentes de este tipo debe ayudar a una organización a mejorar su capacidad de gestión de incidentes, incluyendo la identificación de los cambios necesarios en la política de seguridad, cambios en las configuraciones de software y detección de malware y las implementaciones de software de prevención.

4.3.6.7.7. Establecer metodologías de prevención de incidentes y formación frente a las amenazas actuales y futuras a corto plazo

Debido a las nuevas amenazas malware que surgen constantemente, las organizaciones deben establecer metodologías de prevención de programas malware, debe tener capacidad de prevención de incidentes y que sean robustos y lo suficientemente flexibles para hacer frente a las amenazas actuales y futuras a corto plazo y que puedan ser modificados para hacer frente a futuras amenazas a largo plazo.

El malware y las defensas contra el malware siguen evolucionando, cada uno en respuesta a las mejoras en la otra. Por esta razón, las organizaciones deben mantenerse al día sobre los últimos tipos de amenazas y actualizar las medidas de seguridad disponibles para combatir cada tipo de amenaza. Cuando una nueva categoría de amenaza se torna más grave, se deben planificar e implementar las medidas adecuadas para minimizar el riesgo de ser vulnerable a esta nueva amenaza y reducir el impacto en caso de ser infectados. El conocimiento de nuevas soluciones de protección y de las amenazas emergentes deben ser considerados para prevenir incidentes de malware.

4.3.7. Gestión de registros

4.3.7.1. Objetivos

4.3.7.1.1. La necesidad de la gestión de registros

Los registros (*logs*, en inglés) pueden beneficiar a las organizaciones de muchas maneras, entre ellas y principalmente al control de la seguridad, registrando información muy valiosa frente a cualquier tipo de incidente, que además nos valdrá para prevenir y/o corregir nuestras políticas de seguridad.

Por otro lado, existen leyes y regulaciones que hacen énfasis en la gestión de los registros:

LOPD: La Ley de Protección de Datos en España pone especial atención en los registros (varios artículos 24, 103,…), especificando como deben ser los logs que reflejan accesos, control y almacenamiento de datos.

Ley de retención de datos de comunicaciones: tiene en cuenta los registros como una de las principales fuentes, especificando como debe ser su gestión.

SOX 2002: Aplicable primero a instituciones financieras y contables, después se extendió a organizaciones TIC. SOX se centra en la revisión periódica de los registros en busca de cualquier tipo de ataque o violación de seguridad. Además, pone especial énfasis en el almacenamiento para la auditoria posterior de los registros.

PCI DSS: Aplicable a organizaciones que tratan con datos de tarjetas, destaca por el registro de todos los accesos a este tipo de datos.

4.3.7.1.2. Desafíos en la gestión de registros

El desafío más común que se presenta a la hora de la gestión de registros es el encontrar el equilibrio que permite gestionar, con un número limitado de recursos, la cantidad de registros que se generan y que cada día aumenta más. Se podría generalizar el tipo de desafíos en tres tipos:

Generación de registros y su clasificación al comienzo

Los desafíos en este grupo vienen dados por la gran cantidad de fuentes que crean registros y la información que contienen, la cual debe ser gestionada para que los registros sean lo más eficientes posibles. Formatos inconsistentes y registro de momentos erróneos son otros de los problemas comunes a la hora de la generación.

Confidencialidad, integridad y disponibilidad de registros

Los desafíos en este grupo vienen dados por la gran cantidad de datos comprometidos que un registro puede incluir, como nombres de usuarios y contraseñas, etc. Los registros deben ser protegidos para evitar que sean accedidos por usuarios no autorizados. La integridad de los registros también debe ser observada, puesto que la configuración por defecto de algunos sistemas puede limitarlos en tamaño o en extensión, haciendo que se sobre-escriban y por tanto se produzca una pérdida de información.

Formación de administradores de registros

Actualmente, la falta de formación para los administradores de registros han hecho que la tarea de análisis de registros sea dura, aburrida y poco rentable en cuestión de tiempo-resultados. Sin procesos que nos permitan un análisis más rápido y eficiente, el valor de la información que nos proporcionan los registros se ve reducido.

4.3.7.2. Descripción

Un registro (o *log*) es la anotación de los eventos ocurridos dentro de los sistemas y redes de una empresa u organización. Originalmente, los registros fueron creados para poder analizar el origen de los problemas y solucionarlos, pero hoy en día tienen otros usos como la optimización de sistemas y redes, la identificación de las acciones realizadas por los usuarios y/o la provisión de información útil para la investigación de actividades maliciosas.

Debido al aumento de servidores, puestos de trabajo, redes y/o otros dispositivos que generan registros de seguridad, el volumen, la variedad y el número de los mismos se ha incrementado enormemente, creando la necesidad de una gestión eficiente. Esta gestión abarca los procesos de generación, transmisión, almacenaje, análisis y acceso a los registros.

Los registros de seguridad informática pueden contener una gran cantidad de información sobre lo ocurrido en los sistemas y redes de la organización. Dependiendo de la información que incorporen los registros, estos tendrán una mayor relevancia en la gestión de la seguridad.

Se puede diferenciar dos tipos principales de registros:

- Registros de software de seguridad
- Registros de sistemas operativos

4.3.7.2.1. Registros de software de seguridad

La mayoría de organizaciones usan varios tipos de software de seguridad (en red o en local) para detectar cualquier tipo de actividad maliciosa, por ello la mayor cantidad de registros son producidos por este tipo de programas:

Antimalware

El más común es el antivirus. Los registros procedentes de este tipo de software registran detecciones de malware, desinfección de archivos y sistemas, análisis del sistema, actualizaciones y todo tipo de evento relacionados. Los antispyware y similares son también una fuente común de este tipo de registros.

Prevención y detección de intrusiones

Producen registros de toda actividad sospechosa o ataque detectado, así como de las acciones llevadas a cabo por dichos softwares para la prevención. La mayoría hacen comprobaciones periódicas por lo que los registros contienen registros por lotes/periodos.

Acceso remoto

Los registros se centran en dejar constancia de los accesos correctos y fallidos a la red privada virtual (VPN), así como la cantidad de datos enviados y recibidos, tiempos de conexión… de cada usuario.

Web Proxies

Los registros se centran en las URLs accedidas a través de su sistema.

Gestión de vulnerabilidades

Estos sistemas suelen incluir software de parcheado y de valoración de vulnerabilidades, registrando los historiales de instalación, así como el estado de vulnerabilidad de cada sistema (junto con vulnerabilidades conocidas y actualizaciones no realizadas). Además registran la configuración del sistema y suelen generarse periódicamente.

Servidores de autenticación

Crean registros de cada intento de acceso así como el origen, nombre, éxito o fracaso y momento del acceso.

Routers

Normalmente solo generan registros con la configuración de bloqueo al tráfico que tengan.

Cortafuegos

Generan registros donde detallan la configuración según la política de permiso/bloqueo que tengan y como los usuarios interactúan con ella.

Servidores de cuarentena

Debido a su uso para análisis de equipos previo a su entrada en la red, registran los resultados de los tests e información detallada al respecto.

4.3.7.2.2. Registros de Sistemas Operativos

Los sistemas operativos de servidores, puestos de trabajo y dispositivos de la red incorporan en registros la información relacionada con la seguridad.

Actividad del sistema

El administrador puede especificar que incidentes registrar, normalmente se suele registrar aquella actividad que supone algún incidente. Al registro le acompaña tanta información como se configure, siendo lo más normal, el momento, situación del sistema, códigos de error, nombre de la actividad/servicio, usuario, cuenta asociada…

Control de registro

Este tipo de registros dejan constancia de aquellos incidentes de seguridad del sistema operativo como serían intentos de autenticación, acceso a archivos, cambios en la configuración de seguridad, cambios en las cuentas y uso de privilegios. Normalmente, el sistema operativo permite configurar la información que los registros deben registrar.

Los registros de los sistemas operativos tienen una importancia vital a la hora de identificar o investigar actividad sospechosa. Normalmente, después de que una aplicación detecte alguna incidencia, se consultan los registros del sistema operativo para obtener más información sobre la actividad.

4.3.7.2.3. Registros de aplicaciones

Las aplicaciones que las organizaciones usan para realizar sus funciones pueden generar sus propios registros o usan la capacidades de registro de los sistemas operativos o sistemas de gestión de bases de datos. La información que generan es muy variada, siendo los siguientes tipos de información los más registrados:

Peticiones de clientes y respuestas de servidor

El registro de estos eventos es importante para la reconstrucción de incidentes ocurridos y el análisis de los motivos. Los registros suelen contener la información desde que un usuario accede a la aplicación y deja constancia de todos las actividades, lo que facilita el rastreo y la comprobación en caso de necesidad.

Información de cuentas

Registro de toda actividad desde una cuenta, incluyendo intentos de accesos. Esto permite identificar intentos de acceso en caso de ataque, cambios en las cuentas, uso de privilegios…

Acciones operativas significativas

Registran las acciones mas críticas como los arranques y apagados del sistema, errores en las aplicaciones y los cambios de configuración más significativos. Estos registros son muy útiles a la hora de identificar los fallos de seguridad y operativos.

Mucha de la información generada suele ser dependiente de otras fuentes.

4.3.7.2.4. Utilidad de los registros

Los registros se generan con un objetivo, por ejemplo, los que hemos visto en relación a seguridad, buscan la detección de cualquier actividad sospechosa, así como información detallada en caso de incidente. Otros registros contienen información menos relevante pero que, contrastada con otros registros, puede ser de gran ayuda. Por ejemplo, si en el registro de incidentes, detectamos una IP con determinada actividad sospechosa y buscamos después en los registros de actividad del cortafuegos la misma IP, obteniendo así una información interesante sobre el suceso.

Por último, los administradores deben tener en cuenta la veracidad de los registros, ya que en un ataque, las fuentes de los registros o incluso los propios registros pueden ser alterados. Por lo que siempre es recomendable contrastar la información con otros con información común.

4.3.7.3. Mejores prácticas

Para afrontar la mayoría de los desafíos que hemos visto hay varios puntos clave:

Priorizar y configurar la gestión de registros

Establecer una estrategia de gestión de registros con objetivos para la generación y análisis de los mismos, así como el establecimiento de las políticas a seguir hará que se reduzcan notablemente los riesgos y empecemos a establecer una base correcta para la gestión de los registros.

Establer políticas y procedimientos

Establecer políticas basadas en la gestión de registros nos permitirá seguir unos pasos estudiados y estar acorde con la ley. La realización de auditorias regulares harán que nuestra organización se mantenga segura.

Crear y mantener una infraestructura de seguridad

Crear una infraestructura y determinar como interactúan sus componentes mantendrá la integridad de los registros frente a pérdidas de archivos y violaciones de confidencialidad. Un punto crítico dentro de la infraestructura es prepararla para que soporte el tráfico esperado y además los picos que pueden producirse en determinados momentos.

Soporte adecuado para responsables de la gestión de registros

Proveer de la formación, guías y software de gestión de registros a los responsables será necesario para que puedan desempeñar eficientemente sus funciones.

Como hemos comentado, dado el volumen de datos manejados es altamente recomendable contar con un sistema de información para la gestión de los registros. En los apartados siguientes se incluye información al respecto de este tipo de infraestructuras que incluye el hardware, el software, la red y los medios utilizados para la gestión de los registros. Las organizaciones suelen tener una o varias infraestructuras de gestión de registros, según el tamaño y necesidades.

4.3.7.3.1. Arquitectura

La arquitectura del sistema se define en tres líneas principales:

Generación de registros

Constituye la primera línea del sistema y consiste en la generación de registros desde los propios sistemas. Estos son accesibles desde una segunda línea mediante aplicaciones y/o accesos a los servidores.

Análisis de registros y almacenamiento

La segunda línea está compuesta por servidores de registros que reciben o copian los registros de la primera línea para su almacenamiento.

Monitorización

La tercera línea esta compuesta por una consola que puede monitorizar y revisar los datos de los registros y los resultados de los análisis automáticos. Estos suelen generar informes.

Normalmente se utiliza la propia red de la empresa como infraestructura. Si alguno de los elementos no estuviera conectado a la red, en la gestión de registros se deben preocupar por mantener actualizados los registros mediante el traspaso de la información.

4.3.7.3.2. Funciones

La infraestructura desempeña algunas funciones que no alteran los registros originales, pero facilita la gestión:

General

- Log Parsing: Análisis de valores de los campos de un registro para su uso en otro proceso.
- Filtrado de registros: Análisis y preparación del registro suprimiendo los que carecen de interés como los duplicados. Cabe destacar el especial cuidado que se debe tener a la hora de analizar y/o modificar registros, ya que su simple apertura para análisis (depende de la manera y software utilizado) puede cambiarlos casi imperceptiblemente. Esto afectaría a la naturaleza necesaria que deben tener todos los registros: exactitud y autenticidad. Cumpliendo estas premisas tendrían validez como pruebas. Una vez que un registro esta completo siempre debe ser auditado y protegido para conservarlo apropiadamente.
- Agregación de registros: Convirtiendo en un solo registro, los registros que se refieren al mismo evento contabilizando los diferentes momentos.

Almacenamiento

- Rotación de registros: Guardando archivos de registros completos por considerarlos finalizados y abriendo nuevos en su lugar. Periódicamente o debido al tamaño de archivo.
- Archivo de registros: Almacenaje de registros por un periodo concreto de tiempo según políticas o por interés concreto.
- Compresión de registros: Compresión de archivos para que ocupen menos espacio cuando estos son rotados o archivados.
- Conversión de registros: Conversión de tipo de registro para su análisis o almacenaje.

- Normalización de registros: Cada parte del registro se convierte a un formato común para un mejor manejo. Especial cuidado a la hora de convertir el registro, ya que la modificación supone normalmente su invalidez como prueba al no cumplir los principios de exactitud y autenticidad.
- Comprobación de integridad de archivos registro: Firma digital que acompaña al registro para asegurar su integridad y que no ha sido alterado. MD5 y SHA-1 son los más utilizados.

Análisis

- Correlación de eventos: Identificación de relaciones entre registros.
- Visión de registros: Posibilidad de visionado de registros en lenguaje comprensible para los usuarios. A través de las propias aplicaciones o de terceros.
- Informe de registros: Informes con información de los registros, determinada por el usuario.

Eliminación

Eliminación de datos dentro de un registro o de los propios registros debido a que la información ya no es necesaria o porque ya no tiene importancia.

4.3.7.3.3. Planificación de la gestión de registros

Para mantener una infraestructura en gestión de registros en perfectas condiciones debe haber una planificación determinada y unas actividades programadas que aseguren su correcto funcionamiento.

Definición de roles y responsabilidades

Para un correcto funcionamiento deben existir unos roles y responsabilidades bien definidos entre los usuarios y/o equipos que se ocupan de dicha gestión.

Administradores de sistemas y redes, administradores de seguridad, equipos de respuesta ante incidentes de seguridad informática, desarrolladores de aplicaciones, responsables de la seguridad de los datos, dirección de informática, auditores, usuarios responsables… son los diferentes puestos que deben estar definidos y sus responsabilidades y actuaciones programadas.

Dentro de los roles deben existir diferentes niveles de seguridad que permitan acciones y acceso a la información de manera responsable y confidencial. A la vez, debe existir una comunicación entre los diferentes participantes y roles que permita guiar, aprender y mejorar en la gestión.

Establecimiento de políticas

La organización debe tener claros sus objetivos, así como el equilibrio entre la gestión y los resultados. Para ello se gestionaran las capacidades y se priorizaran las tareas.

Al existir una política definida para la generación de registros, tendremos unos requerimientos mínimos y unas recomendaciones claras a la hora de que los usuarios actúen. Estos afectaran a la manera de gestionar la generación, transmisión, almacenamiento, acceso y análisis.

A la vez, se aplicarán las políticas y leyes nacionales e internacionales que correspondan como las anteriores vistas o la LOPD y/o Ley de retención de datos de comunicaciones. En ellas se define las pautas a seguir según la naturaleza de la organización.

Debido a la gran cantidad de datos comprometidos que los registros pueden contener, las organizaciones tendrán el deber de controlar periódicamente el cumplimiento de las políticas y actualizarlas en caso de necesidad.

Garantía de políticas viables

La auditoria sobre la gestión de registros que realizamos siempre es recomendable para la comprobación, no solo del cumplimiento de las políticas establecidas, sino de la eficiencia de los datos recogidos. Recoger una mayor cantidad de datos no es siempre la mejor opción, pues la importancia reside en el valor de los datos y la rapidez en el análisis. La flexibilidad y los resultados a la hora de gestionar serán los puntos clave para una buena gestión.

La política NIST SP 800-70 se centra en el análisis de los entornos informáticos comprobando como estos influyen en la actividad de gestión de registros. Se recomienda tener una política determinada según el tipo de entorno que tengamos. Los más comunes son:

SOHO: Política para pequeños sistemas que suelen usarse en casa o para negocios a pequeña escala. Normalmente con conexiones limitadas que hacen obligatorio que las transferencias de datos sean a pequeña escala, por tanto la política se caracteriza porque se debe intentar generar los mínimo e imprescindible.

Organización: La política más generalista y típica de grandes organizaciones donde es fácil la gestión debido a su propia naturaleza, es decir, los sistemas estan preparados para el uso necesario y la política a seguir es de fácil ejecución.

A medida: Política para sistemas especializados en seguridad o con cierta antigüedad lo que les hace difícil la integración dentro de la infraestructura. Los especializados en seguridad suelen trabajar con datos confidenciales y que necesitan un especial tratamiento por lo que suelen gestionarse de manera individualizada y local; mientras que los sistemas antiguos suelen tener incompatibilidades por naturaleza con una infraestructura demasiado moderna, siendo los datos transferidos manualmente en algún proceso especial

Diseño de las infraestructuras para la gestión de registros

La infraestructura siempre debe ajustarse a las necesidades de la organización. Si no tenemos infraestructura o esta no se ajusta a las necesidades, tenemos que tener en cuenta el cumplimiento de las políticas y otros puntos clave como:

- El volumen normal y los picos de transmisión de datos;
- El uso en momentos normales y picos del ancho de banda;

- El almacenamiento local y online de datos así como el análisis de todo el almacenamiento, incluído de los datos desechados;
- La seguridad necesaria para los registros;
- El tiempo y recursos necesarios para el análisis de los registros.

4.3.7.3.4. Procesos en la gestión de registros

Los administradores deben seguir procesos estandarizados para la gestión de los registros de los cuales son responsables. Se presupone que la organización tiene su infraestructura diseñada y acondicionada cuando realizan estos procesos:

Configuración de las fuentes de registros

La configuración de las fuentes de registros es la mayoría de las veces un proceso complejo, donde el administrador decide las fuentes y el modo en el que tienen que hacer los registros siempre teniendo en cuenta la política establecida.

Después, se configura la información que cada registro debe dejar dependiendo del evento, donde dependerá de las posibilidades que ofrezca la fuente. Tres secciones son las principales a configurar:

Generación del registro

Normalmente la fuente dejará elegir qué eventos registrar y de qué manera. El administrador debe sopesar la cuantía, puesto que en caso de que se generen muchos registros se puede saturar la red e incluso perder información. Para la configuración de fuentes que los administradores no conozcan totalmente, se recomiendan hacer pruebas en una infraestructura para tests y recurrir al fabricante para disipar cualquier duda.

Almacenamiento y acceso a registros

Los administradores decidirán dónde se deben guardar los registros que produzcan las fuentes. Hay varias maneras de hacerlo:

- No almacenamiento: Sería el caso de registros de depuración o con información no relevante para la organización.
- Almacenaje en el sistema: Los registros se guardan solo en los propios sistemas sin pasar de nivel. El acceso a ellos se realizar a través del sistema si fuera necesario.
- Almacenaje en sistema e infraestructura: Almacenaje en sistema con copia de ciertos registros en la infraestructura. Es la solución más segura frente a fallos o ataques, aunque puede entrañar ciertas dificultades por incompatibilidades de formatos.
- Almacenaje solo en infraestructura: Los registros se guardan solo en la infraestructura, pasando de los sistemas al nivel superior.

Otro punto a tener en cuenta es la rotación de los registros, donde pueden existir ciertos problemas como fuentes que no permitan la rotación o archivos que lleguen al límite de sus posibilidades. El administrador deberá llegar a soluciones que no impidan que los registros sigan generándose.

Seguridad de los registros

Es tarea del administrador proteger la integridad y acceso a los datos de los registros. Además de la propia seguridad implementada en la infraestructura, se deberá tener en cuenta:

- Limitar el acceso a los registros
- Evitar la grabación de datos confidenciales innecesariamente
- Proteger los archivos de registros
- Asegurar los procesos que generan los registros
- Configurar cada fuente para comportarse adecuadamente cuando ocurran errores
- Asegurar la transmisión de datos ya sean mediante la infraestructura o mediante soportes externos

Análisis de los datos generados por los registros

El análisis de los registros es, la mayoría de las veces, la actividad más difícil e importante de la gestión. Deberemos tener en cuenta:

Conocimiento sobre registros

La gran variedad de registros y de sus datos hace necesario un estudio de cada uno con el que se trabaje. Tener en cuenta el contexto del registro (fuente donde se genera) y llegar a entender los registros que resulten no entendibles (vía software o desarrollador) facilitarán esta tarea. Llegado el punto de no entender un registro y no tener a quien recurrir, la solución pasa por su estudio periódico para su comprensión.

Priorización de datos en registros

El administrador debe priorizar los datos de los registros para hacer más eficiente el trabajo, sobre la base de las políticas de la organización. Los datos más comunes a priorizar son: tipo de registro, novedad, fuente, fuente o destino (IP), momento y frecuencia.

El registro de la modificación de un fichero de registros podrá ser muy útil en la detección de ataques o errores en la infraestructura.

Comparación del análisis: sistemas (individuales) – infraestructura

Aunque los análisis que hacen los administradores son muy parecidos, la principal diferencia será que lo que es responsabilidad directa para los administradores de sistemas se convierte en responsabilidad secundaria para los administradores de infraestructuras. También se

diferenciarán en que la infraestructura es analizada constantemente mientras que los sistemas se harán de manera periódica.

Los administradores de sistemas deberán tener especial atención a:

- Registros referentes a los sistemas
- Registros referentes a la infraestructura y que no se trasmiten automáticamente
- Registros no entendibles sin el contexto que proporciona la infraestructura

Por otro lado los dos tipos de administradores tendrán que tener en cuenta:

- Políticas de las organizaciones y capacidad para reconocer una violación de las mismas
- Conocimiento del software de análisis y capacidad de detectar falsas alertas/positivos
- Sistema operativo y aplicaciones
- Características de ataques y técnicas comunes
- Software de gestión de registros para su análisis

Ambos deben crear informes que proporcionen información valiosa a la Dirección de la organización.

Respuesta a eventos identificados

Ante la detección de un evento o incidente recogido en las políticas o detectado por el administrador como importante, deben existir unos procedimientos (ver apartado **4.4 Gestión de Incidentes** más adelante) por los que se de solución siendo responsabilidad del administrador y de los equipos al cargo arreglar el incidente y reforzar la infraestructura o sistemas para evitar su repetición. Monitorización y análisis son las herramientas que ayudarán principalmente a realizar estas tareas.

Gestionando el almacenamiento de larga duración de los registros

Si los registros generados necesitan ser guardados durante periodos largos de tiempo (meses-años) los administradores deberán tener en cuenta:

Guardar también los registros en formatos especiales para almacenamiento

Esto hará que el registro, además de la información, contenga las pautas para ser leído y no exista problema si en el futuro no se encuentra un lector compatible al formato original.

Archivar los datos

La elección de soporte, así como la manera de archivarlos, serán factores importantes para encontrar rápidamente la información que necesitamos en el futuro. El administrador deberá revisar periódicamente los archivos para comprobar su correcto estado.

Verificar la integridad de los archivos transferidos

Una vez archivados los registros, se debe comprobar su estado una vez archivados para evitar que se encuentren modificados después del proceso. A través de la comparación de los "digest" calculados es la manera más rápida.

Guardar los datos de manera segura

El administrador será responsable de asegurar los datos guardados mediante:

- Protección física de los medios, situándolos en un lugar seguro y de acceso restringido.
- Entorno controlado para evitar que temperaturas extremas o humedades puedan afectar al medio donde estén guardados.

También será responsabilidad del administrador la destrucción apropiada de los archivos a la hora de eliminarlos (tanto digitalmente con re-escritura, como físicamente con los medios).

Proporcionando otro tipo de soporte operacional

Los administradores deberán proporcionar también soporte a la hora de trabajar con los registros en tareas como:

- Monitorizar el correcto funcionamiento de las fuentes
- Monitorizar las rotaciones y almacenamiento de registros
- Mantener la infraestructura actualizada
- Asegurar la sincronización de los relojes de toda la infraestructura para que sean correctos los registros de los tiempos
- Reconfigurar registros según los cambios en las políticas
- Detectar anomalías e incidentes. Los administradores de sistemas deberán notificar a los de infraestructura de cualquier incidente detectado.

Probando y validando

Las organizaciones deberán probar y validar periódicamente sus políticas, procesos y procedimientos para estar seguras del correcto funcionamiento de la gestión de registros. Esta revisión es útil para identificar prácticas efectivas, configuraciones eficientes y otro tipo de variables que irán haciendo mejor la gestión de registros.

Las técnicas más comunes para probar y validar son:

- Pasiva: Unos auditores comprueban y validan la infraestructura, viendo el funcionamiento que tiene dicha infraestructura.
- Activa: Los auditores crean pruebas, sobre todo de seguridad, para comprobar y validar el funcionamiento de la infraestructura.

El método activo es más efectivo y además se puede usar para probar nuevas funciones. También se deben hacer pruebas especificas de seguridad a la infraestructura periódicamente para comprobar lo siguiente:

- Saturación de la infraestructura mediante la comprobación de sucapacidad para gestionar registros.
- Comprobación de la seguridad en la generación de los registros.
- Comprobación del acceso limitado a sistemas e infraestructura, así como, la integridad de los registros y el software utilizado.
- Comprobación de seguridad de las comunicaciones.

Será recomendable comprobar nuevas versiones y actualizaciones de toda la infraestructura que permitan mejorar la gestión de registros y/o hacerla más segura.

4.3.7.4. Herramientas

4.3.7.4.1. Software de registros centralizado basado en syslog

Con el protocolo 'syslog', todos los registros utilizan el mismo formato y se gestionan de la misma manera, lo que permite un trabajo más rápido y eficiente.

Formato syslog

Syslog es simple y sus mensajes tienen tres partes. La primera, donde especifica numéricamente el tipo de mensaje y su prioridad, una segunda parte donde pone el origen vía IP y el momento (timestamp) y la tercera parte donde se describe el contenido.

Se asigna una prioridad a cada mensaje basándose en tipo de mensaje y prioridad (0 para emergencias hasta 7 para pequeñas depuraciones).

Seguridad syslog

Cuando los syslog fueron desarrollados no se tuvo en consideración la seguridad por lo que tienen ciertas carencias que se han intentado corregir vía estándares como RFC3195. Estos, aseguran la fiabilidad a la hora de la creación y envío de registros, la confidencialidad de la transmisión, la integridad y autenticación de los mismos.

Algunas características han sido implementadas posteriormente fuera de la RFC3195, como, por ejemplo: Filtrado mejorado, análisis mejorado, respuesta ante determinados eventos, formatos alternativos, encriptación, base de datos para registros, limites en la generación y transferencia según necesidades,… consiguiendo así suplir las carencias de los syslog.

4.3.7.4.2. Software SIEM (Security Information and Event Management)

La denominación SIEM se aplica al tipo de software utilizado para la gestión y la seguridad de los registros. Generalmente permiten dos maneras de recolectar registros:

- Sin agente: Los registros son recolectados de las fuentes sin tener ningún tipo de software instalado en los generadores de registros. Estos pueden ser enviados o recolectados según el tipo.

- Con agente: Un software instalado en los generadores de registros filtra, normaliza y transmite los registros.

Este tipo de software tiene la ventaja de tener interfaces gráficas, una base de seguridad, rastreo de incidentes e información adicional sobre el tratamiento de cada registro.

4.3.7.4.3. Otro tipo de software de gestión de registros

Otros tipos de software de gestión de registros pueden ser de ayuda a la hora de gestionar toda la información disponible:

- IDS – Sistema de detección de intrusiones. Software instalado en el propio host que monitoriza y avisa de actividades sospechosas.

- Herramientas de visualización: Software que muestra gráficamente todo tipo de actividades interesantes para la seguridad de la infraestructura (muchos SIEM las traen incorporadas).

- Utilidades de rotación de registros: Software para la rotación de registros con características de rastreo y seguridad.

- Utilidades de conversión de registros: Conversores de formatos de registros propios de los diferentes software a formatos estándar que permiten su uso por otras herramientas.

4.3.7.5. Ejemplo. Buena práctica sobre uso de SIM/SIEM

SIM/SIEM son el nombre que reciben aquellas herramientas que automatizan el proceso de la gestión y análisis de logs haciendo más fácil y eficiente el uso de los datos. En el mercado podemos encontrar varias destacadas de diversos desarrolladores como Cisco, Qlabs,…

Normalmente se componen de el servidor dedicado que almacena todos los logs que genera nuestra infraestructura, y el software SIM/SIEM que es el que lo gestiona, por lo que es independiente.

El sistema debe tener una serie de características para su buen funcionamiento:

- Debe estar configurada para la correcta recepción de todos los logs que se monitoricen

- El almacenamiento no debe incluir la manipulación de los logs, a fin de que sean originales y valgan por ejemplo como prueba judicial.

Con estas premisas las herramientas SIM/SIEM nos darán la capacidad de definir que tipo de datos queremos obtener, generándonos informes según nuestras necesidad. Por otro lado podremos definir alertas que nos informen cuando exista un tipo de incidente y/o reglas que entren en funcionamiento cuando ocurra un tipo de caso que programaremos previamente (por

ejemplo un número determinado de accesos fallidos desde una misma máquina en un corto periodo de tiempo).

La buena configuración de estas características nos darán una monitorización instantánea de nuestra infraestructura haciendo que la información generada en forma de logs nos resulte útil al momento.

Cabe destacar que dentro de estas herramientas encontraremos también otras características interesantes como creación de copias de seguridad, ayuda para cumplir normativas, etc.

4.4. GESTIÓN DE INCIDENTES

4.4.1. Objetivos

El objetivo de la gestión de incidentes es poder hacer frente a problemas que se producen en el día a día de una organización.

Para una gestión eficiente de los incidentes, debemos contar con un orden de preferencia para su tratamiento alineado con los resultados de un análisis de riesgos. De esta forma, cuanto mayor sea la recurrencia y gravedad de los incidentes, mayor será su nivel de riesgo y, por tanto, estarán primero en la escala. Este tipo de incidentes conllevarán un análisis de cada uno de ellos de manera exhaustiva. A continuación nos encontraremos con incidentes de tipo moderado y, finalmente, de riesgo bajo. Para estos tipos de incidentes, dado su nivel de relevancia, se realizará un análisis general de los mismos.

Un equipo de control de riesgos nos aporta una serie de beneficios:

- Respuesta a incidentes de forma sistemática para que se adopten las medidas apropiadas.
- Personal de ayuda para recuperarse de forma rápida y eficaz de los incidentes de seguridad, minimizando la pérdida o robo de la información y la interrupción de los servicios.
- Gestión de incidentes para preparar mejor para la gestión de incidentes en el futuro y proporcionar una mayor protección para los sistemas y datos.
- Tratar adecuadamente las cuestiones legales que puedan surgir durante los incidentes.

4.4.2. Descripción

Organizar un equipo de seguridad para la identificación y gestión de incidentes, implica varias decisiones importantes, así como una serie de pasos a seguir. Una de las primeras tareas a realizar es crear una definición específica del término “incidente” dentro de la organización para que el alcance de esta expresión quede clara en el ámbito organizativo. Hay que tener en cuenta las estructuras del equipo y los modelos que pueden proporcionar estos servicios y seleccionar y aplicar uno o más equipos de respuesta a incidentes. El plan de respuesta a

incidentes, la política, y la creación de un procedimiento son partes esenciales para que la respuesta a incidentes se lleve a cabo con eficacia, eficiencia y consistencia en toda la organización. El plan, las políticas y los procedimientos deben reflejar la interacción del equipo de respuesta a incidentes con otros equipos dentro de la organización, así como con terceros, tales como las fuerzas y cuerpos de seguridad del Estado, los medios de comunicación y otras organizaciones de respuesta a incidentes.

Eventos y sucesos de riesgo

Un evento es cualquier suceso observable en un sistema o red. Los eventos incluyen un usuario que se conecta a un recurso compartido de archivos, un servidor que recibe una petición de una página web, un usuario que envía un correo electrónico o un cortafuegos que bloquea un intento de conexión.

Los eventos adversos son aquellos que tienen una consecuencia negativa como, por ejemplo, caídas del sistema, inundaciones de paquetes de red, uso no autorizado de los privilegios del sistema, acceso no autorizado a datos sensibles o la ejecución de código malicioso que destruye los datos.

Un incidente de seguridad informática es una violación o la amenaza inminente sobre las políticas de seguridad informática, las políticas de uso aceptable o de las normas de seguridad.

Ejemplos de incidentes:

1. Denegación de Servicio
    - Enviar paquetes especialmente diseñados a un servidor web, provocando que se bloquee.
    - Redirigir paquetes a cientos de estaciones de trabajo.
2. Código malicioso
    - Un gusano.
    - Una organización que recibe un aviso de un proveedor de antivirus que un nuevo gusano se está extendiendo rápidamente por correo electrónico a través de Internet. El gusano se aprovecha de una vulnerabilidad.
3. Acceso no autorizado
    - Un atacante ejecuta una herramienta para tener acceso a archivo de contraseñas de un servidor.
    - Un usuario anónimo obtiene acceso no autorizado, con permisos de administrador y accede a los datos sensibles que contiene un fichero, luego amenaza a la víctima, normalmente exigiendo una remuneración económica para no desvelar esa información.

4. Uso inapropiado

- Un usuario proporciona copias ilegales de software a otros a través de servicios *peer-to-peer* para compartir archivos.
- Una persona que amenace a otra persona a través de correo electrónico.

4.4.3. Mejores prácticas

4.4.3.1. Política de gestión de incidentes

La política de gestión de respuesta a incidentes es muy subjetiva y depende de cada organización. Sin embargo, la mayoría de las políticas incluyen los mismos elementos clave, independientemente de si la capacidad de la organización de respuesta a incidentes es por parte de personal de la empresa o subcontratados:

1. Declaración de compromiso de gestión.
2. Fines y objetivos de la política.
3. Ámbito de aplicación de la política (a quién y para qué se aplica y en qué circunstancias).
4. Definición de los incidentes de seguridad informática y sus consecuencias en el contexto de la organización.
5. Estructura de organización y delimitación de funciones, responsabilidades y niveles de autoridad que debe incluir la autoridad del equipo de respuesta a incidentes de confiscar o desconectar el equipo y para monitorizar la actividad sospechosa, así como los requisitos para la presentación de informes de ciertos tipos de incidentes.
6. Priorización o gravedad de las calificaciones de los incidentes.
7. Medidas de la ejecución de informes y formularios de contacto.

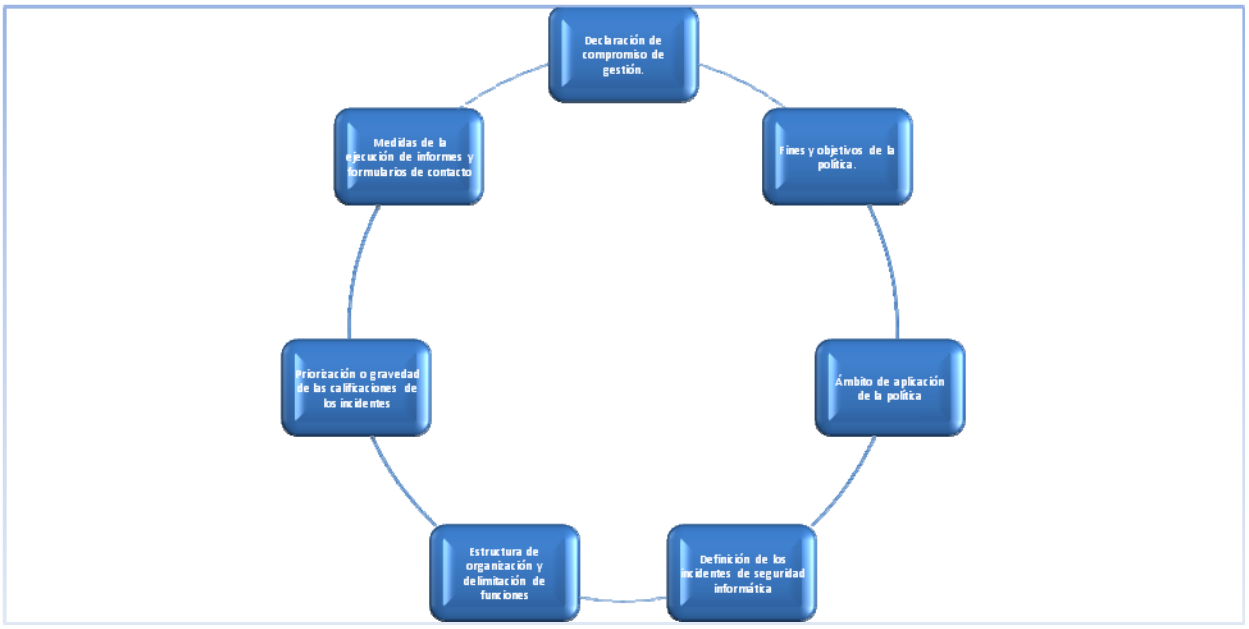

Ilustración 5: Etapas de la respuesta a incidentes

4.4.3.2. Plan de respuesta a incidentes

Es importante que las organizaciones tengan un enfoque formal y coordinado para responder a los incidentes. Para aplicar eficazmente dicha capacidad, una organización debe tener un plan de respuesta a incidentes. El plan dota a la organización con una hoja de ruta para la aplicación de su capacidad de respuesta a incidentes. Éste debería ofrecer una visión de alto nivel sobre cómo la capacidad de respuesta a incidentes encaja en la organización general. Cada organización necesita un plan que satisfaga sus necesidades dependiendo del sector de la organización, del tamaño, de la estructura y de las funciones. Debe determinar los recursos y apoyo a la gestión que se necesita para mantener con eficacia y madurez de una capacidad de respuesta a incidentes. El plan de respuesta a incidentes debe incluir los siguientes elementos:

1. Misión.
2. Estrategias y objetivos.
3. Aprobación de la Alta Dirección.
4. Enfoque de la organización de respuesta a incidentes.
5. Cómo el equipo de respuesta a incidentes se comunicará con el resto de la organización.
6. Métrica para medir la capacidad de respuesta a incidentes.
7. Hoja de ruta para la maduración de la capacidad de respuesta a incidentes.
8. Cómo el programa se adapta a la organización en general.

Ilustración 6: Etapas del Plan de Respuesta a Incidentes

La misión de la organización, las estrategias y las metas para la respuesta a incidentes deben ayudar a determinar la estructura de su capacidad de respuesta a incidentes y la estructura del equipo de respuesta a incidentes, así como los trabajos dentro del plan.

Una vez que una organización desarrolla un plan de gestión de incidentes y recibe la aprobación para ponerlo en práctica, el plan debe ser revisado, al menos, una vez al año y comprobar que la organización está siguiendo la hoja de ruta para la maduración de la capacidad y el cumplimiento de sus metas en respuesta a incidentes.

4.4.3.3. Los incidentes y el ciclo de vida de los sistemas

Muchos incidentes pueden ser manejados de manera más eficiente y eficaz si se han incorporado ciertas consideraciones en el ciclo de vida de la información del sistema. Ejemplos de tales consideraciones son las siguientes:

- Realizar copias de seguridad periódicas de los sistemas y mantener las copias de seguridad anteriores durante un período específico de tiempo.
- Habilitar la auditoría en estaciones de trabajo, servidores y dispositivos de red.
- Desvíar los registros de auditoría para asegurar servidores centralizados de registro.
- Configurar las aplicaciones críticas para activar sus funciones de auditoría, incluyendo la grabación de todos los intentos de autenticación.
- Usar un software de comprobación de integridad para los activos de especial importancia.
- Mantener los registros (por ejemplo, las líneas de base de datos) de configuraciones de red y el sistema.
- Establecer políticas de retención de datos que apoyan la realización de reseñas históricas del sistema y la actividad de la red, cumpliendo con las peticiones o exigencias para preservar los datos relativos a los litigios en curso e investigaciones y la destrucción de datos que ya no son necesarios.

La mayoría de estas consideraciones son extensiones de las disposiciones existentes en las políticas de la organización y sus procedimientos.

4.4.3.4. Recomendaciones en la gestión de incidentes

De manera ordenada podríamos decir que los pasos más destacables a seguir ante una situación de riesgo se resumen en cuatro:

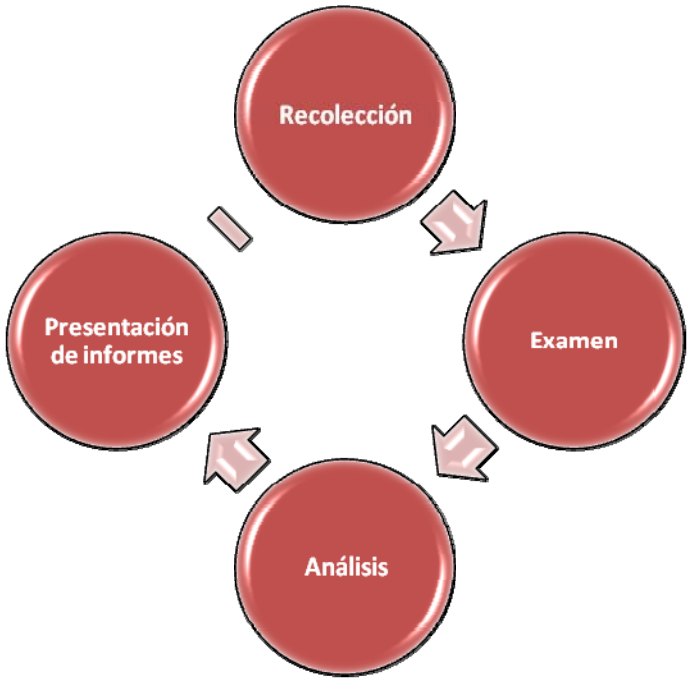

Ilustración 7: Pasos destacables para gestionar incidentes

- **Recolección**. La primera fase del proceso consiste en identificar, etiquetar, registrar y obtener datos de las posibles fuentes de datos pertinentes, siguiendo las directrices y procedimientos que permiten preservar la integridad de los datos. La recogida se realiza normalmente en el momento inicial debido a la probabilidad de pérdida de datos dinámicos, como las conexiones de red actuales, así como la pérdida de datos de los dispositivos alimentados por baterías (por ejemplo, teléfonos móviles, PDA's).

- **Examen**. Supone el procesamiento de grandes cantidades de datos recolectados a través de una combinación de métodos automatizados y manuales para evaluar y extraer datos de especial interés, mientras que se respeta la integridad de los datos.

- **Análisis**. La siguiente fase del proceso consiste en analizar los resultados del examen, utilizando el método legalmente justificable y técnicas, para obtener información útil que responda a las preguntas que fueron el origen para realizar la recogida y examen.

- **Presentación de informes**. La fase final es informar sobre los resultados del análisis, lo que puede incluir la descripción de las acciones realizadas, explicando cómo las herramientas y los procedimientos fueron seleccionados, para determinar qué otras acciones se deben realizar y proporcionar recomendaciones para la mejora de las

políticas, directrices, procedimientos, herramientas... La formalidad de la etapa de presentación de informes es muy variable dependiendo de la situación.

4.4.3.5. Condicionantes de la gestión de incidentes

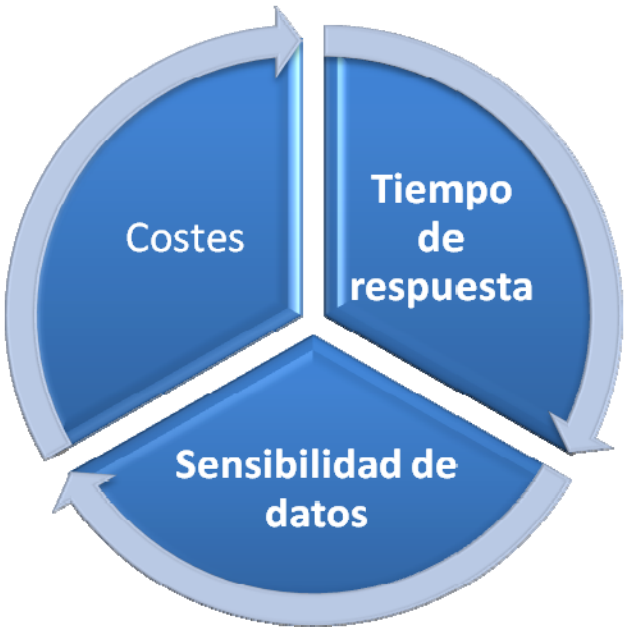

Ilustración 8: Condicionantes de la gestión de incidentes

Además de tener en cuenta los aspectos internos realizados con la gestión de riesgos y las políticas organizativas, para la gestión de incidentes hay que tener en cuenta también los siguientes factores:

- **Costes**. El software, el hardware y los equipos utilizados para recoger y examinar datos puede suponer a costes significativos (precio de compra, actualizaciones de software, mantenimiento…), y también puede requerir medidas adicionales de seguridad física para su protección frente a manipulaciones. Otros gastos significativos se refieren los costes de formación personal y laboral.

- **Tiempo de respuesta**. El personal interno de la empresa será capaz de iniciar una actividad de investigación intrusiva más rápidamente que personal externo contratado. En contraposición, empresas con ubicaciones geográficas dispersas deberán plantearse si ese personal interno le responderá de manera más rápida o bien una empresa de servicios que se lo pueda proporcionar.

- **Sensibilidad de datos**. Debido a la sensibilidad de los datos y la privacidad, algunas organizaciones podrían ser reacias a permitir que empresas externas puedan acceder a sus datos. Hay que tener en cuenta este aspecto a la hora de contratar empresas externas.

4.4.3.6. Equipos de respuesta a incidentes

Para conseguir los objetivos del plan de gestión de incidentes es necesario que la organización se dote de una serie de grupos especializados en ello. Las necesidades concretas siempre vienen determinadas por la empresa, aunque se suelen dividir en tres grandes grupos:

- Los **investigadores** son responsables de analizar las denuncias de mala conducta. Para algunas organizaciones, se hacen cargo de la investigación de cualquier caso en el que se sospecha una actividad delictiva. Suele utilizar muchas técnicas y herramientas. Estos investigadores pueden estar localizados en otros departamentos tales como recursos humanos y asesores legales.

- **Profesionales de TI**. Este grupo incluye a personal de apoyo técnico y el sistema, la red y los administradores de seguridad. Usan un pequeño número de técnicas y herramientas específicas para su área.

- **Operadores.** Este grupo responde ante una serie de incidentes de seguridad informática, tales como acceso a datos no autorizados, uso inapropiado del sistema, las infecciones de códigos maliciosos y ataques de denegación de servicio.

Ilustración 9: Roles para la gestión de incidentes

Es importante identificar a otros grupos dentro de la organización que pueden ser necesarios para participar en la gestión de incidentes a fin de que su colaboración pueda ser solicitada antes de que sea necesario. Todos los equipos de respuesta a incidentes se basan en la experiencia, juicio y habilidades de otros, incluyendo:

1. **Dirección**. Siempre juega un papel fundamental en la respuesta a incidentes. En el sentido más fundamental, establece la política de respuesta a incidentes, el presupuesto y la dotación de personal. En última instancia, la gestión es responsable de la coordinación de respuesta a incidentes entre las diversas partes interesadas, minimizando el daño y da cuenta al CNPIC (a través de la persona designada por la Organización), fuerzas y cuerpos de seguridad del Estado y otras posibles partes afectadas. Sin el apoyo de gestión, un equipo de respuesta a incidentes es poco probable que tenga éxito.

2. **Seguridad de la Información**. Los miembros del equipo de seguridad de la información a menudo son los primeros en reconocer que un incidente ha ocurrido o está ocurriendo y puede llevar a cabo el análisis inicial de los incidentes. Además, la información de los miembros del personal de seguridad puede ser necesaria durante otras etapas de la gestión de incidentes, por ejemplo, alterando los controles de seguridad de red (reglas de cortafuegos) para contener un incidente.

3. **Telecomunicaciones**. Algunos incidentes son relacionados con el acceso no autorizado a las líneas telefónicas.

4. **Soporte de TI**. No son expertos técnicos (en el sentido de los administradores de sistemas, administradores de red o desarrolladores de software) pero tienen la capacidad técnica necesaria para ayudar durante un incidente, además, de manera general, tienen una mejor comprensión de la tecnología con la que tratan a diario. Esta comprensión puede facilitar la toma de decisiones.

5. **Departamento Jurídico**. Los expertos legales deben revisar los planes de respuesta a incidentes, políticas y procedimientos para garantizar el cumplimiento de la ley, incluido el derecho a la intimidad. Además, la ayuda del departamento legal se debe buscar si existen razones para creer que un incidente puede tener consecuencias legales, incluyendo la recolección de pruebas, la persecución de un sospechoso o una demanda.

6. **Asuntos Públicos y Relaciones con los Medios**. Dependiendo de la naturaleza y el impacto de un incidente, puede existir la necesidad de informar a los medios de comunicación y, por extensión, al público (dentro de las limitaciones impuestas por la seguridad y los intereses del orden público).

7. **Recursos Humanos**. Cuando un empleado es el objetivo aparente de un incidente o se sospecha que es la causa de un incidente, el departamento de recursos humanos a menudo se ve involucrado, por ejemplo, en la asistencia de un procedimiento disciplinario o en el asesoramiento de los empleados.

8. **Plan de Continuidad de Negocio**. Los incidentes de seguridad informática pueden socavar la capacidad de recuperación de una organización y actúan como un barómetro de su nivel de vulnerabilidad y de los riesgos inherentes. Éstos deben estar al tanto de los sucesos y sus consecuencias para que puedan perfeccionar las evaluaciones de impacto sobre las empresas, las evaluaciones de riesgos,y la continuidad de los planes de operaciones.

4.4.3.7. La detección de incidentes

Para muchas organizaciones, la parte más difícil del proceso de respuesta a incidentes es precisamente la detección y evaluación de posibles incidentes, es decir, determinar si ha ocurrido un incidente y, en caso afirmativo, el tipo, extensión y magnitud del problema. Lo que hace esto tan difícil es una combinación de tres factores:

1. **Incidentes.** Se pueden detectar a través de muchos medios diferentes, con diferentes niveles de detalle y fidelidad. Las capacidades automatizadas de detección incluyen IPS

basados en red y en host (posteriormente haremos una breve mención), el software antivirus o los analizadores de registros. Los incidentes también se pueden detectar por medios manuales, tales como los problemas reportados por los usuarios. Algunos incidentes son signos evidentes que pueden ser fácilmente detectados, mientras que otros son casi imposibles de detectar sin la automatización.

2. El **volumen de los signos potenciales** de incidentes suele ser alta, por ejemplo, no es raro que una organización pueda recibir a miles o incluso millones de alertas de intrusión del sensor de detección de manera diaria.

3. Los **conocimientos técnicos especializados** y una amplia experiencia son necesarias para un análisis adecuado y eficiente de los datos relacionados con el incidente. En la mayoría de las organizaciones, las pocas personas con este nivel de conocimiento están probablemente asignadas a otras tareas.

Los signos de un incidente se dividen en dos categorías: *indicadores* y *precursores*. Un precursor es una señal que indica la posibilidad de que un incidente pueda ocurrir en el futuro. Un indicador es una señal que nos manifiesta que un incidente puede haber ocurrido o pueden estar ocurriendo ahora. Existen demasiados tipos de indicadores para enumerarlos en este documento, pero algunos ejemplos son los siguientes:

- La red de alertas sensor de detección de intrusos cuando un intento de desbordamiento de búfer se produce en un servidor FTP.
- El software antivirus avisa cuando detecta que un host está infectado con un gusano.
- Las caídas de los servidores web.
- El administrador del sistema ve un nombre de archivo con caracteres extraños.
- El usuario llama al help desk para informar de un mensaje de correo electrónico amenazante.
- El host registra un cambio en la configuración de auditoría en su registro.
- Los registros de aplicaciones muestran múltiples intentos fallidos de inicio de sesión desde un sistema remoto desconocido.
- El administrador de correo electrónico ve un gran número de mensajes devueltos, con contenido sospechoso.
- La notificación de una desviación típica inusual de los flujos de tráfico de la red.

4.4.3.8. Las revisiones periódicas y la gestión de incidentes

Mantener el número de incidentes razonablemente bajo es muy importante para proteger los procesos de la organización. Si los controles de seguridad son insuficientes, podemos encontrarnos con altos volúmenes de incidentes. Esto puede llevar a respuestas erróneas que se traducirán en un impacto negativo (por ejemplo, más daños, más tiempo de servicio y

disponibilidad de datos). Un buen planteamiento para mejorar la situación de la organización en seguridad y la prevención de incidentes es llevar a cabo evaluaciones periódicas de los riesgos de los sistemas y aplicaciones. Estas evaluaciones deben determinar cuáles son los riesgos planteados por los distintos tipos de amenazas y riesgos de vulnerabilidad. Cada una de estas evaluaciones debe tener prioridad y los riesgos encontrados pueden ser mitigados, transferidos o aceptados hasta un nivel razonable de riesgo general alcanzado. La incorporación o por lo menos el examen de las estrategias de control de las organizaciones responsables pueden proporcionar una garantía razonable de que los riesgos a los que se está expuesto.

Otro de los beneficios de llevar a cabo evaluaciones de riesgo con regularidad es que los recursos críticos están identificados, lo que permite al personal hacer hincapié en actividades de vigilancia y de respuesta. Tenga en cuenta que, independientemente de la eficacia de una evaluación de riesgos, solo muestra el riesgo actual. Las nuevas amenazas y las vulnerabilidades surgen constantemente y la seguridad informática es un proceso continuo que requiere diligencia para ser eficaz.

4.4.4. Herramientas

4.4.4.1. Utilización de Sistemas de Prevención de Intrusiones

Los Sistemas de Prevención de Intrusiones (IPS, por sus siglas en inglés, Intrusion Prevention Systems) se centran principalmente en la identificación de posibles incidentes. Por ejemplo, un IPS puede detectar cuando un atacante ha conseguido comprometer un sistema por la explotación de una vulnerabilidad del mismo. Los datos reportados por esta aplicación podrían iniciar acciones de respuesta a incidentes y de esa manera reducir al mínimo los daños causados por el incidente. Muchos sistemas además, pueden ser configurados para reconocer intrusiones de las políticas de seguridad. Por ejemplo, algunos IPS se pueden configurar con el cortafuegos, lo que les permite identificar el tráfico de red que viola la seguridad de la organización o las políticas de uso aceptables. Los IPS pueden controlar las transferencias de archivos e identificar los que podrían ser sospechosos.

Muchos IPS también pueden identificar actividades de reconocimiento, lo que puede indicar que un ataque es inminente. Por ejemplo, algunas herramientas de ataque examinan formas de malware, que después usan para realizar actividades de reconocimiento, tales como exploraciones de host y el puerto para identificar objetivos para ataques posteriores. El IPS puede ser capaz de bloquear el reconocimiento y notificar a los administradores de seguridad, que puede tomar medidas si es necesario modificar otros controles de seguridad para evitar incidentes similares.

Además de identificar los incidentes y apoyar los esfuerzos de respuesta a incidentes, las organizaciones han encontrado otros usos para los IPS, incluyendo las siguientes:

- Identificar los problemas de políticas de seguridad. El IPS puede proporcionar un cierto grado de control de calidad para la aplicación de políticas de seguridad, tales como la duplicación de reglas de cortafuegos y la generación de alertas cuando se comprueba que el tráfico de red que debería haber sido bloqueada por el cortafuegos no lo ha sido debido a un error de configuración.

- La documentación de la amenaza existente de una organización. El IPS facilita información de registro sobre las amenazas que detectan. Entender la frecuencia y características de los ataques contra los recursos informáticos de una organización es útil para identificar las medidas de seguridad adecuadas para proteger los recursos. La información también se puede utilizar para educar a la gestión de las amenazas que enfrenta la organización.

- Disuadir a las personas de que violen las políticas de seguridad. Si los individuos son conscientes de que sus acciones están siendo monitorizadas por las tecnologías ISD, el saber que se les monitoriza puede provocar que sean menos propensos a cometer tales violaciones a causa del riesgo de detección.

Debido a la creciente dependencia de los sistemas de información y la prevalencia e impacto potencial de las intrusiones en contra de los sistemas, los IPS se han convertido en un complemento necesario a la infraestructura de seguridad de casi todas las organizaciones.

4.4.5. Ejemplos

4.4.5.1. Recomendaciones ante una intrusión

Las principales recomendaciones ante una intrusión o violación de la seguridad informática que haya generado un incidente se resumen en los siguientes:

- Establecer una capacidad de respuesta a incidentes formales. Las organizaciones deben estar preparadas para responder con rapidez y eficacia cuando las defensas de seguridad informática no son suficientes.

- Crear una política de respuesta a incidentes. Se debe definir qué eventos se consideran incidentes, establecer la estructura dentro de la organización para dar respuesta a los incidentes, definir las funciones y responsabilidades, enumerar los requisitos para reportar incidentes, etc.

- Desarrollar un plan de respuesta a incidentes sobre la base de la política de respuesta a incidentes. El plan de respuesta a incidentes proporciona una hoja de ruta para la aplicación de un programa de respuesta a incidentes dependiendo de la política de la organización. El plan indica las metas a corto y largo plazo del programa, incluyendo indicadores para medir el programa. El plan de respuesta a incidentes también se debe indicar la frecuencia con la que los equipos de respuesta a incidentes deben ser entrenados y los requisitos para los gestores de incidentes.

- Desarrollar procedimientos de respuesta a incidentes. Los procedimientos de respuesta a incidentes proporcionan instrucciones detalladas para responder frente a una intrusión. Los procedimientos deberían abarcar todas las fases del proceso de respuesta a incidentes. Los procedimientos deben basarse en la política y el plan de respuesta a incidentes.

- Establecer políticas y procedimientos relacionados con el intercambio de información relacionada con el incidente. La organización debe comunicar los detalles de incidentes

con terceros, tales como los medios de comunicación, fuerzos y cuerpos de seguridad del Estado, el CNPIC, etc.

- Educación y concienciación. Los usuarios son los principales detectores y notificadores de intrusiones o fugas de datos. Esta formación puede ser realizada a través de muchos medios: talleres y seminarios, sitios web, boletines, carteles, pegatinas e incluso en los monitores.

- Vigilancia Tecnológica. Un equipo puede realizar una función de vigilancia tecnológica, lo que significa que busca las nuevas amenazas a la seguridad de la información. Ejemplos de ello son las listas de seguimiento de correo relacionados con la seguridad, análisis de datos de detección de intrusiones para identificar a un aumento de la actividad de un virus o la investigación de nuevos rootkits que están a disposición del público. El equipo debe hacer recomendaciones para mejorar los controles de seguridad sobre la base de las tendencias que se identifiquen. Un equipo que realiza una función de vigilancia tecnológica también debe estar mejor preparado para manejar los nuevos tipos de incidentes.

- Administración de revisiones. El equipo de respuesta a incidentes tiene la responsabilidad de la administración de revisiones (por ejemplo, la adquisición, las pruebas y la distribución de parches a los administradores y usuarios en todo caso la organización). De hecho, los servicios de gestión de parches a menudo son más necesarios cuando se trata de contener, erradicar, y recuperarse de incidentes de gran envergadura.

4.4.5.2. Políticas y procedimientos de intercambio de información

Una organización debe establecer políticas y procedimientos sobre el intercambio de información con los medios de comunicación y otros terceros.

1. Proporcionar información pertinente sobre los incidentes. La presentación de informes es beneficiosa para todos, ya que estas organizaciones facilitan y proporcionan información a las organizaciones sobre nuevas amenazas o nuevas tendencias de incidentes.

2. Considere los factores pertinentes al seleccionar un modelo de equipo de respuesta a incidentes. Las organizaciones deberían sopesar cuidadosamente las ventajas y desventajas de cada modelo de equipo, posible estructura y el modelo de dotación de personal en el contexto de las necesidades de la organización y los recursos disponibles.

3. Seleccione las personas con las habilidades apropiadas para el equipo de respuesta a incidentes. La credibilidad y competencia del equipo dependerá en gran medida de la capacidad técnica de sus miembros. Una falta de juicio técnico puede socavar la credibilidad y provocar desconfianza. Las competencias técnicas incluyen administración de sistemas, administración de redes, programación, soporte técnico, y detección de intrusiones. Las habilidades de trabajo en equipo y de comunicación también son necesarias para la gestión eficaz de incidentes.

4. Identificar otros grupos dentro de la organización que se necesitan para participar en la gestión de incidentes. Todos los equipos de respuesta a incidentes se basan en la experiencia, juicio y habilidades de otros equipos, incluida la gestión, seguridad de la información, soporte de TI, los asuntos legales, públicos y gestión de las instalaciones.

5. Determinar qué servicios debe ofrecer el equipo. Aunque el principal objetivo del equipo es la respuesta a incidentes, la mayoría de los equipos deben realizar funciones adicionales. Los ejemplos incluyen la difusión de avisos de seguridad, la realización de evaluaciones de vulnerabilidades, la educación de los usuarios en materia de seguridad o la vigilancia de sensores de detección de intrusos.

4.4.5.3. Categorización de incidentes

Los incidentes pueden ocurrir en innumerables formas, por lo que no es práctico desarrollar procedimientos idénticos para el manejo de todos los incidentes. Lo mejor que puede hacer la organización es preparar uno general para manejar cualquier tipo de incidente y, más específicamente, para manejar los tipos más comunes. Las categorías incidente se enumeran a continuación. No son muy exhaustivas ya que la intención no es la de proporcionar la clasificación definitiva de los incidentes, sino proporcionar una base para la prestación de asesoramiento sobre cómo manejar incidentes en función de su categoría principal:

1. Denegación de servicio: un ataque que impida el uso autorizado de redes, sistemas o aplicaciones por una carencia de los recursos de la organización.

2. Código malicioso, virus, gusanos, caballos de Troya, o cualquier otra tipo de código malicioso.

3. Acceso no autorizado a una red, sistemas, aplicaciones, datos u otros recursos de TI.

4. Uso inapropiado: una persona viola el uso correcto de cualquier red o computadora de la organización.

5. Múltiples componentes: un solo incidente que abarque dos o más incidentes.

Algunos incidentes pueden encajar en más de una categoría. El equipo debe clasificarlos.

- Un virus que crea una puerta trasera debe ser manejado como un incidente de código malicioso, no un incidente de accesos no autorizados, ya que el código malicioso fue el mecanismo de transmisión utilizado.

- Un virus que crea una puerta trasera que se ha utilizado para obtener acceso no autorizado debe ser tratado como un incidente de múltiples componentes, ya que se utilizaron dos mecanismos de transmisión.

4.4.5.4. Pasos a seguir antes la existencia de una incidencia

Esta es una lista de las principales medidas que se deben realizar cuando un profesional técnico cree que un incidente grave se ha producido y la organización no tiene una capacidad de respuesta a incidentes disponibles. Esto sirve como una referencia básica de qué hacer para alguien que se enfrenta a una crisis y necesita solventarla de manera rápida e inminente.

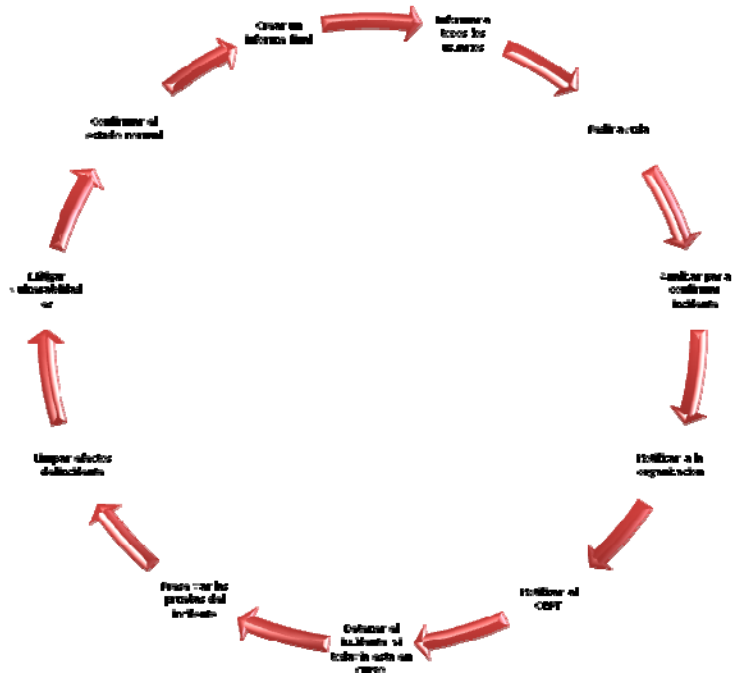

Ilustración 10: Pasos a seguir ante un incidente

1. **Información a todos los usuarios**. Este esfuerzo incluye cada acción que se lleva a cabo, cada pieza de evidencia, y todas las conversaciones con los usuarios, los propietarios de redes, y otros sobre el incidente.

2. Encuentre un compañero de trabajo que pueden proporcionar **ayuda**. El manejo del incidente será mucho más fácil si dos o más personas trabajan juntas.

3. **Analizar las pruebas** para confirmar que ha ocurrido un incidente. Realizar investigaciones adicionales como sea necesario (por ejemplo, los motores de búsqueda en Internet, la documentación de software) para entender mejor las pruebas. Llegar a otros profesionales técnicos dentro de la organización para obtener ayuda adicional.

4. **Notificar** a las personas adecuadas dentro de la organización si se considera que ha ocurrido un incidente. Esto debería incluir al Responsable de Sistemas de Información (CIO), el Responsable de Seguridad de la Información (CISO) y el Responsable de seguridad (CSO). Si el incidente se cree que implica la divulgación no autorizada de la información de identificación personal, notificar a las partes especificadas en la política de la organización de datos de incumplimiento. Sea discreto al discutir los detalles de un incidente con los demás, sólo cuentan las personas que necesitan conocer y utilizar los mecanismos de comunicación que son razonablemente seguros (si el atacante ha

puesto en peligro los servicios de correo, no envíe correos electrónicos sobre el incidente.)

5. **Notifique al CNPIC**, fuerzas y cuerpos de seguridad del Estado y/u otras organizaciones externas para la asistencia en el trato con el incidente, después de consultar con la oficina de asuntos públicos, departamento legal, y / o de gestión para evitar la liberación inapropiada de información confidencial.

6. **Detener el incidente** si todavía está en curso. La forma más común de hacer esto es desconectar los sistemas afectados de la red. En algunos casos, cortafuegos y configuraciones del router posiblemente tengan que ser modificados para detener el tráfico de red que forma parte de un incidente, como una denegación de servicio (DoS).

7. **Preservar las pruebas** del incidente. Hacer copias de seguridad (copias de seguridad de preferencia de imagen de disco, no copias de seguridad de archivos del sistema) de los sistemas afectados. Haga copias de los archivos de registro que contienen datos relacionados con el incidente.

8. **Limpie todos los efectos** del incidente. Este esfuerzo incluye infecciones de códigos maliciosos, los materiales inadecuados (por ejemplo, software pirateado), archivos troyanos y otros cambios introducidos en los sistemas por los incidentes. Si un sistema es plenamente comprometido, debería reconstruirse desde cero o restaurarlo desde una copia de seguridad correcta, no infectada.

9. **Identificar y mitigar** las vulnerabilidades que fueron explotadas. El incidente ocurrió probablemente mediante el aprovechamiento de vulnerabilidades en sistemas operativos o aplicaciones. Es fundamental para identificar las vulnerabilidades tales y eliminar o atenuar lo contrario de modo que el incidente no se repita.

10. **Confirmar que las operaciones han sido restaurados** a su estado normal. Asegúrese de que los datos, aplicaciones y otros servicios afectados por el incidente han sido devueltos a sus operaciones normales.

11. Crear un **informe final**. Este informe deberá detallar el proceso de gestión de incidentes. También debe proporcionar un resumen de lo que sucedió y cómo la capacidad de respuesta a incidentes formales que han ayudado a manejar la situación, mitigar el riesgo y limitar los daños con mayor rapidez.

4.5. PLAN DE CONTINUIDAD DE NEGOCIO / PLANES DE CONTINGENCIAS INFORMÁTICAS

4.5.1. Objetivos

Las empresas y organizaciones dependen del mercado donde se compran sus productos y servicios . Estos son realizados de manera única gracias a los procesos característicos de cada empresa u organización. Así que se debe proteger estos procesos y características frente a factores accidentales, incidentales y humanos. Gracias a los planes de contingencia, las

organizaciones pueden contar con niveles adecuados de seguridad, disponibilidad y confiabilidad en los procesos de la empresa para la continuidad de sus productos y servicios.

Hechos como los atentados del 11 de septiembre en Nueva York o el terremoto y tsunami en Japón (Ilustración 11) han demostrado como la falta de planes de contingencia ante determinados hechos pueden hacer que una empresa fracase, por lo que hay una necesidad de mecanismos y/o técnicas que permitan la continuidad después de que un riesgo posible se convierta en hecho cierto.

Ilustración 11: Efectos del terremoto y tsunami en Japón. Marzo 2011. Fuente: Newstoday.com

4.5.2. Descripción

Un plan de contingencia está compuesto por los mecanismos y/o técnicas que permiten la continuidad de una empresa u organización ante posibles hechos en los que está en riesgo. Una de las partes claves de los planes de contingencia es la recuperación y uso de las infraestructuras, datos vitales, tecnología de la información, equipos… que permiten que la organización siga funcionando.

Hay diferentes estándares que nos pueden ayudar a la elaboración de este tipo de planes y que veremos a continuación.

4.5.2.1. BS 25999

Estándar británico en forma de guía con actuaciones y recomendaciones para asegurar la continuidad de funcionamiento a pesar de los riesgos que pueda tener una organización. Se basa en la existencia de un plan de continuidad de negocio (más conocido por sus siglas en inglés, BCM – Business Continuity Plan) que hace un evaluación de los procesos de la empresa para entender el negocio.

Las principales fases son:

- Inicio y gestión del proyecto
- Evaluación y control de riesgo

- Análisis de impacto de negocio
- Respuesta ante emergencias
- Desarrollo e implementación del BCM
- Programa de concienciación y capacitación
- Mantenimiento
- Comunicación
- Coordinación con Autoridades Públicas

El BCM se caracteriza por involucrar todos los recursos de la organización, analizando y estableciendo las estrategias que ayuden a la continuidad del negocio con los menos recursos posibles.

4.5.2.2. BS 25777

Publicado en 2008, recoge el código de buenas prácticas sobre la Gestión de la Continuidad en TIC y tiene una relación directa con la BS 25999.

Esta norma es importante porque separa la continuidad TIC de la continuidad del negocio. También destaca que en ella se detalla más profundamente la actuación que se debe hacer en una empresa para tener asegurada la continuidad TIC.

En la actualidad ha sido sustituida por el estándar IEC 27031 donde se pone especial atención a la gestión de la información digital así como a su seguridad.

4.5.2.3. IEC 27031

Estándar que sustituye internacionalmente al BS 25777 y que describe las pautas a seguir para asegurar la continuidad del negocio a través de las TIC.

El IEC 27031 pone especial atención en:

- Sugerir una infraestructura y/o sistema principal (con métodos y procesos) para cada organización o empresa.
- Identificación y especificación de todos los aspectos relacionados con el rendimiento. Diseño e implementación de mejoras en la organización que aseguren la continuidad del negocio.
- Preparación de la empresa para controlar su continuidad, seguridad y preparación para sobrevivir a un desastre.

4.5.2.4. ISO/IEC 24762

La ISO/IEC 24762 se centra en proveer un plan de recuperación tecnológico en caso de desastre. El objetivo es seguir dando servicio TIC a la empresa en caso de incidente gracias a una aplicación tanto interna como externamente (empresas relacionadas directamente).

Las fases principales de la norma son:

- Requisitos para su implantación.
- Capacidades de los outsourcing (las empresas subcontratadas deben tener en cuenta la norma para su correcto funcionamiento).
- Directrices para la recuperación y actualización continua de los planes de recuperación.

4.5.2.5. NERC CIP-009

El estándar CIP 009 asegura que, dentro de los planes de recuperación, se tenga en cuenta las medidas de seguridad tecnológicas. El CIP 009 es parte de un grupo de estándares (desde el CIP 002 al 009) y deben ser implantados según cada caso.

Según este estándar, los Planes de recuperación, una vez creados, serán revisados anualmente y contendrán principalmente las siguientes fases:

- Ejercicios, al menos anualmente para comprobación.
- Cambios de control, cambios según el resultado de los ejercicios.
- Infraestructura para copias de seguridad y restauraciones.
- Comprobación de copias de seguridad.

4.5.2.6. NIST SP 800-34

Desarrollado para la protección de las organizaciones federales de EEUU, el SP 800-34 se centra en la continuidad de los servicios TIC en la empresas teniendo en cuenta el impacto de negocio que estas pueden tener en caso de desastre. Para ello establece las pautas a seguir para el diseño de estrategias que permitan evitar el mayor impacto posible. En este estándar toda la infraestructura es analizada al máximo, teniendo en cuenta:

- Sistemas individuales y servidores
- Telecomunicaciones involucradas
- Unidad principal de la infraestructura

En caso de emergencia destaca como el plan contempla la activación (con notificación a responsables) la recuperación total y un sistema de comprobación cuando esté todo reconstituido.

4.5.3. Mejores prácticas

Ilustración 12: Mejores prácticas Continuidad

Según la metodología de la organización DRI (Disaster Recovery Institute International – www.drii.org) son varias las fases a tener en cuenta. En cada etapa habrá un coordinador que haga que cada una sea un éxito. Las etapas son:

4.5.3.1. Inicio y gestión del proyecto

El inicio y la gestión del proyecto se caracterizan por una involucración de todo el personal de la empresa empezando por los directivos. Desarrollar el plan con toda la organización transmite la importancia que este tiene.

Los puntos a definir en esta etapa serían:

- Comité responsable del plan
- Responsabilidades de cada equipo de trabajo
- Actividades de cada una de las fases del proyecto

- Documentación de los procesos
- Presentación de avances
- Obtención de la aprobación por parte de los directivos

Es responsabilidad del coordinador:

- Dirigir la definición de objetivos, políticas y actividades críticas.
- Coordinar y organizar directores de cada fase.
- Controlar el proceso de BCM a través de métodos de control efectivo y gestión del cambio
- Definir y recomendar procesos de estructura de gestión
- Dirigir el proyecto a desarrollar e implementar el proceso del BCM

4.5.3.2. Evaluación y control de riesgos

En esta fase se identificarán las amenazas internas y externas que pueden ser críticas para la continuidad de la organización. Probabilidad, frecuencia y vulnerabilidad son factores a tener en cuenta. Se establecerán prioridades frente a las amenazas, así como una base que permita el control y la acción en caso de incidente.

Para la evaluación y el control de riesgos los puntos clave serán:

- Identificación
- Análisis y evaluación
- Gestión y control

Los resultados obtenidos tendrán una identificación y documentación de:

- Probabilidad de ocurrencia
- Concentración de riesgos
- Análisis de impacto en el negocio
- Estrategia de gestión de control y plan de acción
- Enfoque de priorización del BCM y control de riesgos

4.5.3.3. Análisis del impacto en el negocio

En esta fase se usarán las diferentes técnicas y metodologías existentes para cuantificar y cualificar los daños al negocio en caso de pérdida o interrupción de las actividades principales por incidente.

El Análisis de Impacto en el Negocio (conocido por sus siglas en inglés, BIA – Business Impact Analysis) tendrá en cuenta el RPO y RTO que serán establecidos por la organización:

- RPO (Recovery Point Objective): Punto en el tiempo después de un desastre en el cual deben estar recuperados los datos.
- RTO (Recovery Time Objective): El tiempo estimado después de un desastre en el que una empresa recupera los procesos y sistemas que la permitan seguir funcionando.

El análisis de impacto en el negocio tendrá identificadas las actividades indispensables para la organización, también será capaz de cuantificar el impacto que tendría una incidencia y el efecto que provocaría la parada de esas actividades.

Del análisis de impacto de negocio se obtendrá:

- Objetivos y salidas
- Actividades críticas para la organización, dependencias y debilidades
- Impactos y consecuencias (financieros y no financieros)
- Objetivos del BCM para cada actividad
- Priorización mínima de la recuperación de recursos en caso de incidente
- Registro de datos vitales
- Usuarios y clientes claves
- Proveedores

4.5.3.4. Desarrollo de estrategias para la continuidad del negocio

Esta fase se centrará en el desarrollo de estrategias que permitan la recuperación de las actividades en un tiempo definido a través de los siguientes factores:

- Identificación de los requerimientos de continuidad de la organización.
- Evaluación de la compatibilidad de las estrategias con los resultados del BIA.
- Presentación del análisis de costo/beneficio de las estrategias de continuidad.
- Selección de alternativas de lugares y almacenamiento externo.
- Comprensión de los términos contractuales de los servicios de continuidad del negocio.

En algunos casos las estrategias tendrán un componente externo en forma de acuerdos con organizaciones externas, clientes u otras empresas.

4.5.3.5. Repuestas ante emergencia

Esta fase consistirá en el desarrollo e implementación de procedimientos para actuar ante un incidente, así como la creación de un centro de mandos para operaciones ante la emergencia.

Deberá cumplir los siguientes puntos:

- Identificación de componentes para la respuesta de emergencia.
- Procedimientos de respuesta ante emergencia.
- Identificación y procedimientos de control y autoridad.
- Respuesta de emergencia y recuperación de heridos.
- Seguridad y recuperación.

4.5.3.6. Desarrollo e implementación del BCM

En esta fase se hará el diseño, desarrollo e implementación de los planes de continuidad con el objetivo de evitar paradas. Se tendrán en cuenta los RTO y RPO (ver 4.5.3.3)

Los factores que tendrán que aparecer serán:

- Identificación de requisitos de desarrollo de planes.
- Requisitos de control y administración de continuidad.
- Definición de formato y estructura de los planes.
- Elaboración de planes preliminares.
- Definición de procedimientos y gestión de crisis.
- Definición de estrategias de evaluación de daños y puesta en marcha.
- Desarrollo de introducción a los planes.
- Desarrollo de material para los equipos de:
    - Operación de negocio
    - Recuperación de TIC
- Desarrollo del sistema de comunicaciones
- Implementación de planes
- Procedimientos de control y distribución de planes

4.5.3.7. Programa de concienciación y entrenamiento

Debido al desarrollo continuo de la mayoría de las empresas, los cambios internos son normales, aún así, siempre se genera cierta resistencia que debe ser analizada para evitarla en caso de la puesta en marcha del plan de continuidad. El entrenamiento del plan de continuidad por parte de toda la empresa ayudará a crear una mejor reacción en caso de ser necesario.

Los factores a tener en cuenta serán:

- Objetivos de concienciación y entrenamiento
- Desarrollo e implementación de varios tipos de programas de entrenamientos
- Desarrollo de programas de concienciación
- Identificación de otras oportunidades de educación

4.5.3.8. Mantenimiento y ejercicio del BCM

El objetivo de realizar el ejercicio será la evaluación y el continuo mejoramiento del BCM, además de una evaluación casi real de las capacidades de competencia ante la gestión de la crisis. En el mantenimiento y ejercicio se determinarán varios factores:

- Determinación de la madurez del BCM
- Verificación y validación de estrategias, prioridades y capacidades desarrolladas, además del personal que entre en los planes de contingencia
- Concienciación de la organización sobre el plan de contingencia.
- Ensayo y pruebas de infraestructura, planes y todos los factores que participan.
- Documentación y evaluación de resultados.
- Detección de fallos.

La prueba siempre se realizará como si de una emergencia real se tratara

4.5.3.8.1. Mantenimiento

El proceso de gestión de continuidad no termina con el desarrollo de las estrategias a seguir sino que necesita un mantenimiento que asegure que el plan siempre esté actualizado y preparado para entrar en actuación.

Los resultados principales del mantenimiento del BCM serán:

- Pruebas y documentación sobre el estado actual del plan.
- Registro de todos los cambios y actualizaciones.
- Verificación y validación de identidades, cambios, políticas, estrategias y/o de cualquier otro punto que afecte al plan.

- Comprobación de capacidades y personal.

Estos datos serán de gran ayuda para que el plan no se quede obsoleto.

Las TIC tendrán gran importancia en los planes como apoyo, por ello tendrán un análisis propio y se pondrá especial atención dentro del plan. Siempre habrá que tener en cuenta el estándar ISO 17999 ya que trata especialmente sobre la seguridad TIC.

4.5.3.8.2. Auditoria

La auditoria será la fase posterior al ejercicio donde se analizarán la correspondencia del plan desarrollado con las políticas y estándares utilizados.

Los puntos más importantes serán:

- Resistencia.
- Prioridades y objetivos de acuerdo a las políticas y estándares.
- Directrices de buenas prácticas aplicadas.
- Competencia y efectividad del BCM.
- Implementación.
- Documentación.

El seguimiento y las técnicas a aplicar en la auditoría serán las generales a cualquier proceso, teniendo que dejar constancia de las pautas seguidas.

4.5.3.9. Comunicación de crisis

El BCM deberá establecer las pautas a seguir para la comunicación en caso de emergencia. Se establecerá planes de comunicación para todo el personal involucrado, así como, listas de información de contacto de organismos relacionados directamente con la empresa (clientes, proveedores, gobierno,…) Estando así controlado todos los factores de la comunicación en caso de accidente.

4.5.3.10. Coordinación con autoridades públicas

El objetivo de esta última fase será tener un documento donde estén bien definidas las políticas aplicadas y el resultado obtenido con ello. Dentro del documento destacarán varias partes:

- Alcance.
- Declaración de contenidos de las políticas.
- Objetivos.
- Roles, responsabilidades.

- Detalle de material pendiente.

El documento será producto de un desarrollo donde se revisarán las políticas y su aplicación tanto internamente como externamente. Además se identificarán, revisarán y validarán todos los puntos del plan de contingencia.

4.5.4. Herramientas

Además de todos los estandares y políticas (nacionales y/o internacionales) que nos pueden valer de referencia como son el BS 25999, BS 257777, ISO/IEC 24762, SS 507:2008,… también se podrá recurrir a herramientas diseñadas por organizaciones como el NIST, ASIS y otras organizaciones de reconocido prestigio mundial. Incluso empresas como IBM han desarrollado herramientas propias para realizar los planes apropiadamente.

Cabe destacar alguno de los softwares que hay en el mercado para la planificación de la continuidad del negocio como son eBPR, COOP, Mitigator, TAMP, Linus Revive, RecoveryPac,…

4.5.5. Conclusiones

El plan de contingencia tendrá una importancia vital en la empresa, ya que será la guía a seguir en caso de cualquier incidente que afecte gravemente a la empresa.

Algunos puntos generales a la hora de finalizar nuestro plan:

- No será necesario la realización de aquellas fases que no procedan en nuestra empresa.
- Será necesario que los responsables de desarrollo del plan tengan un conocimiento notable de la empresa y sector.
- Se analizarán todos los recursos que forman la empresa.
- Las amenazas pueden cambiar pero nunca desaparecer.
- El análisis siempre será mejor como proceso conjunto, no como funciones individuales.
- Los planes de contingencia nunca deberán ser usados hasta pasar la fase de mantenimiento y ejercicio.
- Las actualizaciones tendrán vital importancia, ya sea por cambios internos, externos o periodicidad.

Cada cierto tiempo, una noticia nos recuerda que un plan de contingencia puede ahorrar muchos recursos y tiempo a una empresa, incluso salvarla de una desaparición que de otro modo sería segura. Sucesos como el terremoto de Japón y su consecuencia en diferentes sectores han dejado patente la importancia de estos planes. Por todo ello, deberemos esforzarnos en desarrollar correctamente los planes de contingencia o BCM.

5. MEDIDAS DE SEGURIDAD FÍSICA

5.1. OBJETIVOS

La seguridad física establece las pautas para el mundo tangible por las que se trata de evitar la concreción de las amenazas posibles sobre una organización. Para ello, para los activos generales de una organización como zonas protegidas, zonas de influencia y personal, establece las obstrucciones o protecciones necesarias, vigilando activamente las zonas protegidas y de influencia; repensando de forma inteligente con la información recopilada las medidas y controles adecuados a las circunstancias con el último objetivo de proteger a las personas en los grados y aspectos que sean necesarios.

5.2. DESCRIPCIÓN

Puesto que no hay que olvidar que una de sus funciones es velar por la salvaguarda de las instalaciones y el personal que en ellas se encuentra, la seguridad física se va integrando con la tecnología, con la que se superpone y en la que se apoyan, cada vez más, los responsables de su gestión.

Por tanto, a la hora de planificar las medidas de seguridad física, cubriremos los siguientes aspectos:

- Protecciones y Obstrucciones
- Vigilancia y Control
- Operación y Personas
- Inteligencia y Evolución

Dentro de las medidas de seguridad a considerar, no debemos olvidar aquellas de tipo físico destinadas a salvaguardar tanto los edificios como a las personas que en ellos trabajan y prevenir el acceso no autorizado a equipos, sistemas, material e información. Determinar las medidas y procesos que se van a implementar en cuanto a la seguridad física puede resultar complicado. En principio, habría que considerar los siguientes parámetros.

- Vallas, puertas y demás barreras que restringen el acceso al perímetro
- Limitar el acceso a personal autorizado
- Medidas de control de accesos para visitantes, comerciales, proveedores, etc.
- Sistemas de alarma interna en zonas o áreas críticas
- Sistemas de alarma perimetral
- Circuito cerrado de televisión controlable en local o remoto

- Patrullas o personal fijo
- Alarma integrada, CCTV y otros sistemas que informan a la autoridad local
- Barreras de vehículos
- Barreras anti-proyectiles para proteger personal o equipos vulnerables
- Informes de seguridad
- Iluminación que permite visibilidad para la observación y una óptima funcionalidad de las cámaras del CCTV
- Señalización
- Programa de concienciación de seguridad
- Los niveles de las medidas de seguridad física pueden incrementarse o relajarse en función de amenazas y riesgos en diferentes categorías.

5.3. PROTECCIONES Y OBSTRUCCIONES

5.3.1. Perímetro de seguridad

Un cierre perimetral es una barrera física que identifica el área o zona que requiere protección. El nivel de protección ofrecido por un cierre dependerá de su altura, construcción, material utilizado y las características empleadas para incrementar su efectividad, así como los elementos instalados en la parte superior del mismo como: Alambradas, Sistemas de Detección de Intrusión, Alumbrado de Seguridad o un Circuito Cerrado de Televisión.

Se debe controlar todo el perímetro de la organización, segmentando aquellas zonas más generales de aquellas otras más vitales donde se ubican los activos más sensibles e importantes para la organización. Asimismo, la segmentación interna deber tener su propio perímetro de seguridad cuando proceda. En cualquier caso es necesario realizar seguimiento y registros de eventos de forma que puedan realizarse estudios sobre los datos de seguridad recabados.

Para controlar una zona desde el punto de vista físico, primero debe dividirse en pequeños espacios bien definidos. Es en éstos donde deben focalizarse los esfuerzos y acciones para crear un espacio seguro o de protección, ya sean zonas de acceso público, semi-público o privadas en función de quien tenga acceso a las mismas.

Anteperímetro

Se deber tener en cuenta la vigilancia y Control de las zonas más externas a la ubicación en las que se deben valorar las amenazas intencionadas que pueden actuar sobre los parámetros ambientales y sociales.

Se debe valorar la necesidad de vigilancia y control de Alcance más allá del perímetro para detectar de forma proactiva posibles amenazas que incurriendo en las zonas circundantes a las instalaciones pueden afectar a éstas.

Daños colaterales por inestabilidad social

Se debe valorar la necesidad de vigilancia y control para las protecciones de infraestructuras las amenazas derivadas de daños colaterales derivados por la inestabilidad social que puede afectar directa o indirectamente a la infraestructura.

5.3.2. Zonificación de seguridad

Ilustración 13: Zonificación de seguridad

Para controlar la seguridad de las distintas áreas y su entorno, es necesario dividir el conjunto en zonas menores claramente definidas a las cuales se aplican los criterios de protección y defensa necesarios en función de los riesgos.

Una posible subdivisión es la siguiente:

- Zonas Generales y Públicas
- Zonas de Soporte (Semi-privadas)
- Zonas Vitales o Privadas

La estructuración de las zonas interiores y exteriores debe realizarse coherentemente de forma que se asegure y vigile en función de los riesgos, sin olvidar aquellas zonas internas vitales que de ser comprometida su seguridad produciría un alto impacto en la organización. Y todo ello sin olvidar la necesidad de protección ambiental.

5.3.2.1. Zonas Generales y Públicas

Las zonas generales se encuentran dentro del área protegida y se corresponden con zonas de uso general cuyo acceso es menos restringido. Se deberán tener en cuenta los siguientes controles:

- Control de accesos de personas y vehículos
- Vallados
- Zonas limpias para facilitar la vigilancia
- Sistemas y equipamiento
- Sistemas de control de acceso de personas
- Sistemas de control de acceso de vehículos
- Sistemas de detección perimetral
- Sistemas de vigilancia por CCTV
- Iluminación

5.3.2.2. Zonas de Soporte (semi PRIVADA)

Estas áreas se componen de las ubicaciones de trabajo y almacenamiento de la organización: oficinas, salas e instalaciones, etc.

Se deberán tener en cuenta los siguientes controles:

- Sistemas de control de acceso de vehículos
- Sistemas de control de acceso peatonales
- Sistemas de detección perimetral
- Sistemas de vigilancia por CCTV
- Iluminación

5.3.2.3. Áreas de acceso público, carga y descarga

Se deberá tener especial control en aquellas áreas de uso general con acceso público y en las áreas destinadas a la carga y descarga de productos.

5.3.2.4. Zonas Privadas y Vitales

Las áreas vitales se encuentran dentro del área protegida, no obstante el acceso a una zona privada supone atravesar al menos dos barreras físicas independientes, lo suficientemente delimitadas.

Existen además sistemas específicos para el control del acceso y la protección estas áreas. Entre los más comunes se incluyen los siguientes:

- Control de accesos
- Televigilancia

5.3.3. Iluminación de seguridad

Una buena iluminación es muy efectiva tanto desde el punto de vista de la seguridad como para prevenir acciones criminales o amenazas. Un buen nivel de luz debe aportar buena visibilidad en las horas o zonas donde no haya luz natural, así como eliminar puntos ciegos o áreas con sombra.

Los sistemas de alumbrado ofrecen un alto grado de disuasión a un potencial intruso, además de proporcionar la iluminación necesaria para una efectiva vigilancia, ya sea directamente por los guardias o indirectamente mediante un Circuito Cerrado de Televisión (CCTV).

Niveles mínimos de iluminación, alumbrado comúnmente utilizado, distancia entre puntos de iluminación.

5.3.4. Protección de áreas

5.3.4.1. Parámetros horizontales y verticales

Los muros, suelos y techos de una Zona de Acceso Restringido serán de construcción permanente y estarán unidos los unos con los otros. Se deberán proteger convenientemente los espacios que dan acceso a falsos suelos y techos.

La construcción debe estar realizada de tal manera que provea evidencia visual inmediata de cualquier intento de penetración no autorizado. En este sentido es conveniente que los paramentos sean visitables exteriormente, para verificar su estado en las rondas de seguridad que se realicen, especialmente si no hay otros medios electrónicos de detección o visualización de intentos de intrusión.

5.3.4.2. Puertas

Las puertas que dan acceso a Zonas de Acceso Restringido estarán compuestas de madera maciza, metal u otro material sólido. Su superficie no presentará huellas de golpes o raspaduras con el objeto de que sea posible detectar un intento de penetración.

Las bisagras y sus correspondientes pivotes se montarán hacia el interior, o bien se soldarán o fijarán con abrazaderas para impedir que la puerta pueda ser arrancada. Los marcos y las fijaciones deberán ser tan sólidos como la misma puerta.

Los dispositivos de cierre de las puertas que dan acceso a las Zonas de Acceso Restringido serán accionados por cerraduras del grupo correspondiente a su grado de clasificación.

Las puertas deberán cerrarse cuando no estén en uso y controlarse cuando se estén utilizando. Se instalarán dispositivos automáticos de cierre de puertas, como por ejemplo muelles telescópicos, que tiendan a mantener las puertas cerradas una vez franqueado el paso por las mismas.

5.3.4.3. Puertas de emergencia

Se deberá controlar el uso de las puertas de emergencia en las Zonas de Acceso Restringido, limitando el acceso y salida por las mismas exclusivamente a los casos de emergencia o ensayo. Siempre que sea posible, se utilizarán puertas del tipo “antipánico”, de composición y fortaleza equivalente a las puertas habituales de acceso a la zona. Para abandonar el recinto, los usuarios deberán presionar en la barra antipánico retrayendo el pestillo para la apertura de la puerta.

Se instalarán dispositivos magnéticos que permitan detectar una inapropiada apertura de las puertas. Estos sistemas deberán dotarse de sistemas antisabotaje.

5.3.4.4. Conductos

Los conductos de ventilación o cualquier otra apertura que pueda existir en los paramentos de una Zona de Acceso Restringido, cuando sean de tamaño tal que supongan una vulnerabilidad de acceso no autorizado, deberán protegerse con barras de acero soldadas formando cuadro, sujetas firmemente con pernos a la estructura en el interior de la abertura.

5.3.4.5. Ventanas

Las ventanas existentes en la propia Zona de Acceso Restringido, estarán provistas de un sistema de alarma contra apertura, rayado o rotura. Los cristales deberán ser opacos o translúcidos, de forma que se impida cualquier visión nítida desde el exterior.

Cuando los mismos muros del edificio constituyen en parte o por completo el perímetro de seguridad, todas las ventanas y conductos situados a menos de 5,5 metros por encima del nivel del suelo, en zonas no controladas, así como a igual distancia de los tejados, cornisas o bajantes de agua, deberán protegerse con barras de acero soldadas formando cuadro, sujetas firmemente con pernos a la estructura en el interior de la ventana o abertura.

5.4. VIGILANCIA Y CONTROL

5.4.1. Sistema de Detección de Intrusión

Los Sistemas de Detección de Intrusión se constituyen de acuerdo con el principio de “defensa en profundidad”. Pueden ser utilizados en perímetros para aumentar el nivel de seguridad o en las propias Zonas de Acceso Restringido. Se instalan camuflados o de manera visible como elemento disuasorio. Estos sistemas son propensos a las falsas alarmas por lo que normalmente sólo son utilizados junto con sistemas de verificación de alarmas, como CCTV. En áreas o edificios en los que hay guardia de seguridad o personal de servicio permanentemente presente, se podrá prescindir de estos sistemas de detección de intrusión.

Para ser efectivos, deberán coexistir con una fuerza de repuesta ó fuerza de apoyo que actúe en un tiempo razonable en caso de alarma.

Los sistemas de detección de intrusión han alcanzado un nivel de desarrollo y especificidad muy alto. Dado que se encuentran en constante evolución, resulta necesario que el responsable de seguridad preste atención a las innovaciones tecnológicas que puedan mejorar este control en sus instalaciones.

Algunos de estos son:

- **Detectores de presencia**: Existe una gran variedad de tecnologías y formas de sensores de este tipo. Los más utilizados se basan en variaciones del campo magnético o detectores de infrarrojo pasivos. Tienen en común el alertar cuando una persona se encuentra en su radio de acción.

FIGURA 10: Ejemplo de detector por infrarrojos pasivo

- **Perimetrales:** En este grupo se incluyen equipos que detectan el cruce de una línea perimetral. Los más comunes se basan en microondas e infrarrojos activos. En este caso se detecta cuando un objeto cruza la línea. Debido a su escasa especificidad tienden a producir falsas alarmas, por lo que se recomienda que se utilicen en zonas interiores y con escaso movimiento de cargas o personas.

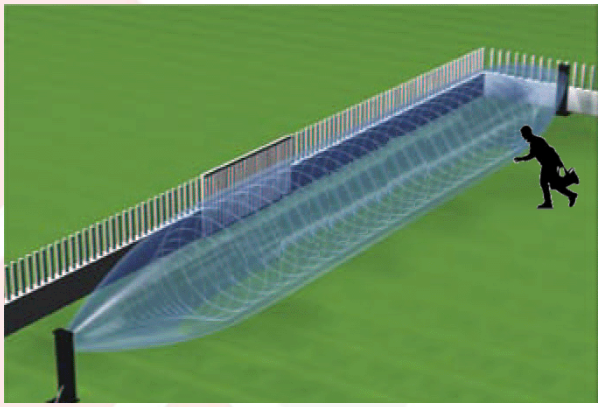

FIGURA 11: Ejemplo de detección por microondas

- **Radares:** Recientemente han aparecido radares de corto alcance con aplicación para la detección de intrusión. Por ejemplo el radar DIO, fabricado por Indra, es capaz de detectar personas e indicar su posición en un radio de dos kilómetros. Además de detectar una intrusión con un ratio de falsas alarmas mucho menor, permiten realizar un seguimiento de esa intrusión.

FIGURA 12: Radar DIO

5.4.2. Control de accesos

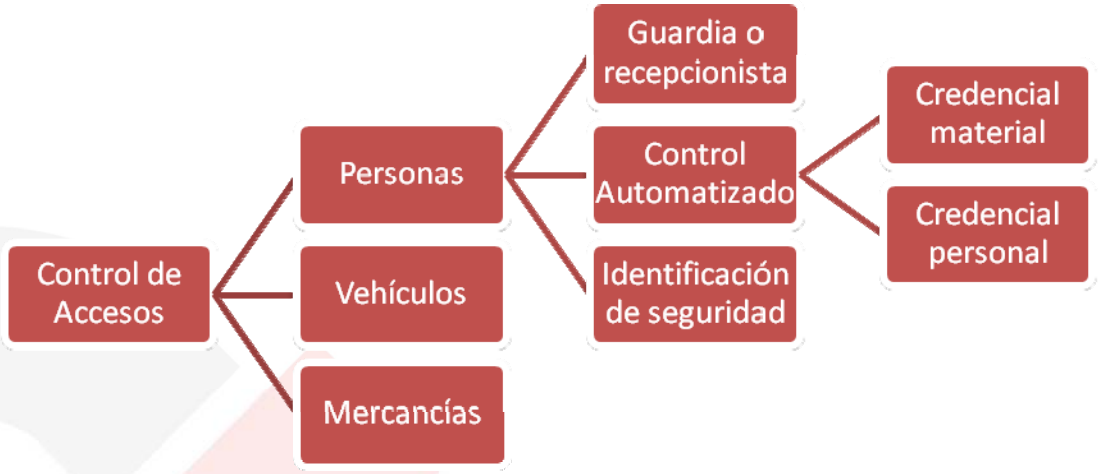

Ilustración 14: Tipos de controles de acceso

El control de acceso puede aplicarse a un lugar, a un edificio o varios edificios de un lugar, o bien a zonas o salas dentro de un edificio. El control podrá ser electrónico, electromecánico, mediante guardia o recepcionista. Debe permitir la separación de accesos en función de la "necesidad de conocer".

5.4.2.1. Personas

En el control de accesos de personas resulta imprescindible establecer mecanismos sencillos por los que se verifique que sólo las personas que puedan entrar en un área determinada lo

hagan. Pero además resulta importante controlar que no porten objetos que puedan poner en peligro la seguridad de la infraestructura, como explosivos o armas de fuego.

Para el control de las personas que pueden acceder o no se pueden utilizar:

- Recepcionista: Debe comprobar quiénes pueden acceder y llevar un registro de entrada y salida.
- Tarjetas de identificación: En edificios con varias entradas o mucha variedad de zonas con distinto nivel de acceso resultan una ayuda indispensable las tarjetas de identificación, que de forma automatizada y centralizada autorizan los accesos y registran los movimientos.
- Sistemas biométricos: Una persona con una tarjeta de acceso convencional de otra persona puede tener acceso a zonas restringidas para él. Para evitar esto se utilizan medios biométricos como lectores de huellas dactilares, iris, reconocedores faciales, etc.

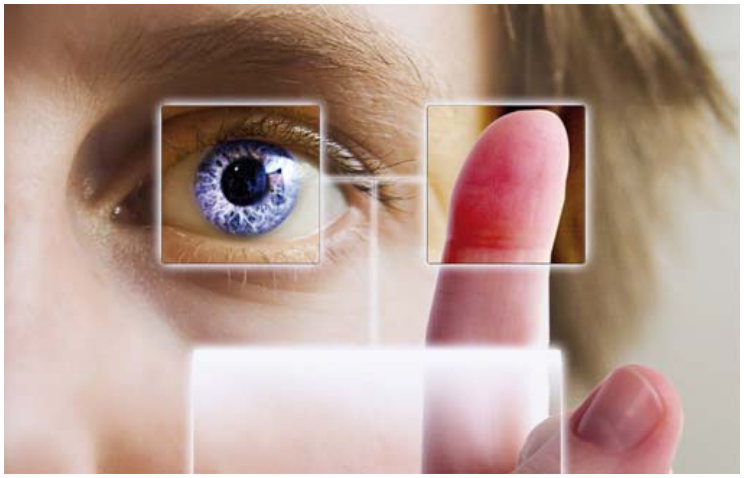

FIGURA 13: Los sistemas biométricos aumentan la seguridad del control de accesos

Para el control de los objetos que portan las personas que acceden a las instalaciones se han desarrollado equipos que permiten niveles variables de inspección.

- Detectores de metales: Detectan armas metálicas, pero no explosivos ni otras amenazas no metálicas. Los últimos modelos tienen sensibilidad ajustable e indican la zona de la detección.

FIGURA 14: Detector de metales

- Escáneres corporales: Detectan cualquier elemento ajeno al cuerpo que se lleve escondido entre la ropa. Pueden ser de ondas milimétricas, con menor resolución de imagen, o de rayos X por retrodispersión.

FIGURA 15: Escáner corporal de retrodispersión

- Escáneres de maletas: Las maletas y bolsos pueden ser escaneados en equipos de rayos X para analizar si ocultan amenazas.

FIGURA 16: Escáner de inspección de bultos

- Detectores de radiactividad: Equipos capaces de encontrar muestras radiactivas portadas por la persona.

5.4.2.2. Guardia de Seguridad o Recepcionista

Organización de los recursos humanos para control de accesos, rondas de vigilancia, inspección de paquetería, supervisión de los sistemas (CCTV, detección de intrusión), etc.

El empleo de guardias adecuadamente habilitados, entrenados y supervisados proporciona un elemento valioso de disuasión frente a aquellas personas que puedan planear una intrusión encubierta.

Las obligaciones de los guardias y la necesidad y frecuencia de las patrullas se decidirán teniendo en cuenta el nivel de riesgo y cualesquiera otros sistemas o equipos de seguridad que pudieran estar en el lugar. Por otra parte, a los guardias se les proporcionarán directrices adecuadas por escrito para asegurarse de que las tareas que les han sido específicamente asignadas se llevan a cabo de acuerdo con las necesidades.

Los guardias habrán de contar con un medio de comunicación con su Centro de Control de Alarmas.

5.4.2.3. Control de Acceso Automatizado

Un sistema de control de acceso automatizado deberá ser capaz de identificar al individuo que trata de entrar en la zona de seguridad, verificando su autorización para entrar en la misma.

Los sistemas de control de acceso automatizado se dividen en:

- Sistemas de credencial material:
    - Llaves: mecánica, eléctrica, electrónica, magnética, mixta, etc.

- Tarjetas: con código de circuito eléctrico, con banda magnética, mecánica, holográfica, con código magnético, con código capacitivo, con código óptico, con código electrónico, mixtas.

- Emisores: de radiofrecuencia, de infrarrojos, de ultrasonidos.

- Sistemas de credencial de reconocimiento y personal.

    - Credencial de reconocimiento: teclado digital, cerradura de combinación, escritura.

    - Credencial personal: huella digital, voz, geometría de la mano, rasgos faciales, iris de ojos, etc.

Los sistemas de control de acceso deben incluir también dispositivos en los que se mantengan registros de las entradas y salidas del personal, tanto en horario de trabajo como, especialmente, fuera de dicho horario.

El sistema más común de doble tecnología es la tarjeta o pase de seguridad, que se acompaña de un número de identificación personal (PIN). El PIN deberá ser introducido en el sistema por cada individuo utilizando un teclado numérico. El PIN deberá consistir en cuatro o más dígitos, seleccionados aleatoriamente, sin conocimiento o asociación lógica con el individuo. El PIN deberá ser cambiado cuando exista cualquier duda sobre una violación o riesgo del mismo.

5.4.2.4. Identificación de Seguridad (pases)

Es necesario un sistema eficaz de identificación del personal, que facilite la circulación al personal autorizado para acceder a los distintos entornos de seguridad, practicar diferenciaciones entre los usuarios e impedir accesos no autorizados.

Los pases deberán colocarse de manera bien visible dentro de los entornos de seguridad, con el fin de que el titular pueda ser reconocido e identificado. Deberán ocultarse cuando se abandone el Entorno Global de Seguridad.

5.4.2.5. Vehículos

Para el control de acceso de los vehículos, el concepto general es similar al de las personas. Por un lado se trata de identificar el vehículo y el conductor, y por otro comprobar si porta objetos peligrosos.

5.4.2.6. Mercancías

Para comprobar la carga del vehículo han tomado protagonismo los equipos de inspección por rayos X, que permiten detectar explosivos y otros materiales peligrosos. También los equipos detectores de trazas de explosivo, más reducidos, permiten reconocer si un vehículo ha podido ser manipulado para introducir explosivos.

FIGURA 17: Inspección por rayos X de vehículos

5.4.3. Circuito Cerrado de Televisión (C.C.TV.)

El CCTV representa una valiosa ayuda para los guardias de seguridad a la hora de verificar incidentes y alarmas en lugares o perímetros extensos. Sin embargo, la eficacia de este sistema dependerá de la selección de un equipo adecuado, de su instalación y de la supervisión que se ejerza desde el Centro de Control de Alarmas.

Resulta fundamental también el correcto mantenimiento y la comprobación periódica de su ubicación, visibilidad y conexión.

5.4.4. Tecnologías

A las cámaras convencionales, o del espectro visible, se han unido recientemente las cámaras térmicas. Si bien resultan un poco más costosas que las visibles, tienen la posibilidad de funcionar día y noche, así como la capacidad de discriminar entre personas y otros objetos móviles.

El trabajo de supervisión de la instalación de videovigilancia resulta pesado para el operador. Además resulta difícil orientarse y saber qué se está viendo a través de esa cámara si no se ha permanecido cierto tiempo en la instalación. Herramientas como la videovigilancia 3D ayudan a mejorar estos aspectos.

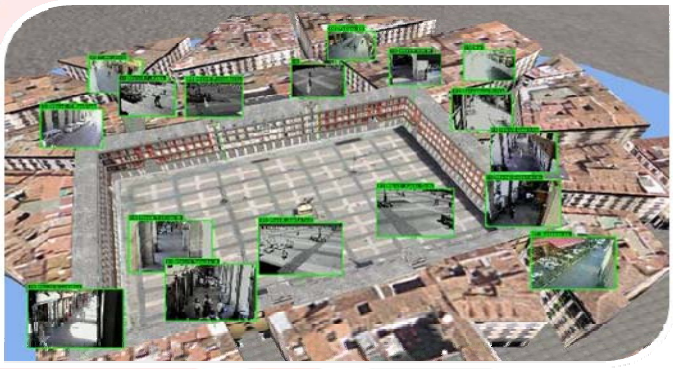

FIGURA 18: Ejemplo de videovigilancia sobre modelo 3D

5.4.5. Protección contra incendios

Para que se produzca un incendio, hacen falta tres factores: calor, combustible y oxígeno. Si se elimina cualquiera de los tres, el fuego no ocurrirá.

Por otra parte, cuando el incendio es provocado, necesita tres componentes: Inclinación, activos y oportunidad. Si prevenimos cualquiera de estos tres componentes, evitaremos que se produzca el mismo.

Inclinación: Entendemos por inclinación el deseo o motivación de alguien para provocar un incendio. Es el factor más difícil de prevenir ya que interviene la voluntad del prójimo.

Activos: Éstos pueden ser tangibles o intangibles, y sería el beneficio que obtendría un tercero tras la consecución de un incendio. Al igual que el factor anterior, prevenir en este punto no sería realista ni práctico.

Oportunidad: Son las circunstancias y condiciones que permiten que ocurra un incendio cuando éste es provocado. Generalmente son de dos tipos: Acceso a los activos y mínimo riesgo para el que provoca el incendio. Es en este punto en el que hay que incidir en las medidas de seguridad

5.4.6. Guardia de Seguridad

Además de lo comentado en el punto 5.4.2.2, es preciso contar con una fuerza de respuesta que proporcione un mínimo de dos personas a cualquier punto en el que se produzca un problema de seguridad, sin debilitar la protección local de otras zonas. Se comprobará la respuesta de los guardias ante las alarmas o las señales de emergencia y se garantizará que dicha respuesta se produce dentro de un plazo que se considere adecuado para impedir el acceso de intrusos.

Los inmuebles, urbanizaciones, polígonos o cualquier tipo de infraestructura que no disponga de un servicio de vigilancia propio en el entorno de sus instalaciones contará con un servicio de vigilancia externo contratado, como mínimo, en horario fuera de la jornada laboral.

Debe organizarse la seguridad en la organización de forma que la transversalidad de las funciones y responsabilidades de seguridad pueda ser transmitido a toda la organización a través de una oficina de seguridad encargada de la seguridad operativa integral.

5.4.6.1. Organización funcional

Deberá establecer y mantenerse una organización de seguridad para proteger a la organización de los riesgos a los que se haya expuesta. Las dependencias orgánicas y funcionales de la organización de seguridad, con la organización general de la organización y sus emplazamientos deberán estar debidamente identificadas y documentadas.

Se deberán establecer niveles de seguridad tanto permanentes como provisionales adecuados a las situaciones de riesgos y en función del incremento del riesgo y/o la evolución de un incidente.

5.4.6.2. Niveles de Seguridad

En función del nivel se podrán aplicar medidas de seguridad física progresivas o medidas compensatorias en caso de no operatividad de los sistemas de seguridad.

5.4.7. Centro de Control de Seguridad

El Centro de Control de Seguridad es un ambiente seleccionado dentro de las instalaciones de una empresa que está a cargo de un grupo de operadores que se encargan de mantener un constante enlace, coordinación, supervisión y control por medios radiales y/o electrónicos con los elementos de seguridad.

Una vez creado el Centro de Control de Seguridad, se debe formular un plan de reacción inmediata como parte del plan general de seguridad integral. La Organización del Centro incluye establecer una asignación de personal con una estructura adecuada, lo que implica una definición lógica de perfiles.

Para operar el Centro de Control será necesario desarrollar manuales de procedimientos, llevar a cabo programas de capacitación y formación, así como realizar auditorías de gestión y técnicas de seguridad periódicamente para detectar áreas de mejora.

La misión principal del Centro es:

- Detectar los riesgos
- Realizar las comunicaciones oportunas
- Dar respuesta inmediata

Aunque el Centro de Control puede reunir también otras funciones:

- Aviso técnico de fallos de funcionamiento
- Realización de maniobras sencillas de cambio de estado.
- Control de alarmas por omisión o error de procedimientos
- Análisis de datos para mejorar el rendimiento de los sistemas operativos.

5.4.8. Contenedores de Seguridad

Se utilizan para almacenar en su interior la Información Clasificada de grado “CONFIDENCIAL o equivalente” o superior, cuando no está en uso. En determinadas condiciones, también para grado “DIFUSIÓN LIMITADA o equivalente” podrá requerirse su almacenamiento en estos contenedores.

Se deberá mantener un control de los nombres de las personas que conocen las combinaciones o están en posesión de las llaves de cajas fuertes, armarios blindados y contenedores de seguridad.

Las cajas fuertes, armarios blindados y otros contenedores de seguridad autorizados por la Autoridad Nacional, se deberán mantener cerrados cuando no estén bajo la supervisión de una persona autorizada.

No se almacenarán en los mismos valores distintos a la propia Información Clasificada, que puedan actuar como un reclamo de intentos de intrusión (joyas, dinero, armas, etc.). Las combinaciones y llaves deberán ser almacenadas de acuerdo con el mayor grado de clasificación del material o información almacenada en ese contenedor.

5.5. OPERACIÓN Y PERSONAS: PROCEDIMIENTOS OPERATIVOS

Ilustración 15: Procedimientos operativos de seguridad

5.5.1. Identificación de Seguridad (pases, tarjetas, etc.).

Es necesario un sistema eficaz de identificación del personal, que facilite la circulación al personal autorizado para acceder a los distintos entornos de seguridad, practicar diferenciaciones entre los usuarios e impedir accesos no autorizados.

Los pases deberán colocarse de manera bien visible dentro de los entornos de seguridad, con el fin de que el titular pueda ser reconocido e identificado. Deberán ocultarse cuando se abandone el Entorno Global de Seguridad.

5.5.2. Control de visitas.

5.5.2.1. Generalidades

Toda Zona de Acceso Restringido dispondrá de una Lista de Personal Autorizado (Anexo III), donde figurarán las personas que están permanentemente autorizadas a acceder a dicha zona.

Cuando otra persona distinta, que no figura en la citada lista, ha de acceder a la zona, tendrá la consideración de Visita. Existirá un libro de registro de visitas, en formato papel o electrónico, donde se controlen todas las visitas recibidas y los detalles relevantes de las mismas.

La nacionalidad del visitante, su habilitación de seguridad, la necesidad de conocer y el tipo de local, determinan que a un visitante se le permita acceder con o sin escolta a un establecimiento clasificado, sin perjuicio de lo establecido con carácter general respecto a personal que ha de acceder a Zonas de Acceso Restringido configuradas como Área Clase I o Área Clase II.

En los siguientes apartados se describe el tipo de control a llevar sobre los visitantes a estas zonas.

5.5.2.2. Visitas con escolta

Los visitantes que necesiten escolta dentro de una zona, irán acompañados en todo momento. Si necesitan visitar departamentos diferentes o a miembros diferentes del personal, pasarán oficialmente de un escolta al siguiente junto con la documentación que les acompañe.

Puede exigirse llevar un pase que identifique a estas personas como visitantes.

La escolta podrá ser realizada específicamente por guardias de seguridad, especialmente cuando las condiciones de seguridad así lo aconsejen por ser mayor el riesgo que supone la visita.

En condiciones de menor riesgo, la escolta podrá ser realizada por el propio personal con acceso autorizado en la zona. En dicho caso, quien realice la escolta deberá ser consciente de que está desarrollando dicho cometido y de la responsabilidad que asume.

5.5.2.3. Visitas sin escolta

Los visitantes a los que se les permita la estancia sin escolta en una zona, por ser personal controlado, con necesidad de conocer y la oportuna habilitación de seguridad, deberán llevar un pase permanentemente visible que les identifique como visitantes. El sistema de pases para las visitas sólo será eficaz si a todo el personal habitual se le exige igualmente que lleve pase.

5.5.3. Control de llaves y combinaciones.

5.5.3.1. Control de llaves

Para establecer una efectiva política de control de llaves es preciso realizar un exhaustivo examen e inventario de todas y cada una de las llaves de todas las cerraduras de la instalación.

Ante cualquier duda de existencia de llaves no controladas, será necesario cambiar el bombín de todas las cerraduras del emplazamiento que sean afectadas.

A continuación se indican una serie de medios y pautas convenientes para obtener y mantener un efectivo control de llaves:

- Armario de Llaves: un armario de seguridad que permita asegurar cada llave individualmente, programable para entregar las llaves solo a usuarios autorizados y durante un lapso de tiempo determinado. Deberá contar con alarma, tanto para los distintos componentes del armario contenedor, como para las llaves.

- Registro de Llaves: se procederá al registro administrativo de las llaves. En el mismo se indicará el número de serie y marca de la misma, así como la cerradura a la que pertenece.

- Llaves Ciegas: Las llaves utilizadas para la generación de réplicas deberán marcarse convenientemente, asegurando que ningún empleado puede generar sus propios duplicados. Las llaves originales serán depositadas en contenedores dedicados y protegidos, accesibles sólo por personal autorizado, cuando no estén en uso. Los originales sólo serán distribuidos, bajo firma de un recibo, a las personas autorizadas para la realización de réplicas y por un tiempo limitado. Las llaves dañadas en el proceso de replicado deberán ser devueltas a efectos de su contabilidad.

- Inventario: se realizarán inventarios periódicos, personales, de las copias y de las llaves originales.

- Auditoria: además de los inventarios, se deberán realizar auditorias sin previo aviso de los registros y procedimientos de control de llaves. Durante el transcurso de estas auditorias se realizará un inventario de todas las llaves.

- Informe diario: se deberá confeccionar un informe diario indicando los empleados que han abandonado o van a abandonar la zona de seguridad. A partir de este informe se iniciarán las acciones pertinentes para recuperar las llaves e identificaciones de seguridad.

Las llaves de armarios, cajas de seguridad y cámaras acorazadas que almacenen Información Clasificada, así como las llaves de puertas, alarmas y sistemas de seguridad, no abandonarán el Entorno Global de Seguridad establecido. Las llaves y claves serán depositadas en contenedores dedicados y protegidos, accesibles sólo por personal autorizado, cuando no estén en uso.

Las llaves de las cajas fuertes y de las cámaras acorazadas deberán guardarse de forma segura, en distinto lugar de donde se custodien las claves de combinación para la apertura de las mismas.

5.5.3.2. Combinaciones

Sólo tendrán conocimiento de los códigos del sistema de acceso a las Zonas de Acceso Restringido, de las claves de control de la central de alarmas, así como de las combinaciones de los lugares de custodia de las materias clasificadas, el Jefe o Responsable de Seguridad y las personas que él designe, que serán las mínimas imprescindibles.

Las claves de combinación para la apertura de las cajas fuertes o cámaras acorazadas, y los códigos de control de la central de alarmas no deben conservarse en claro, debiendo ser modificados obligatoriamente en los siguientes casos:

- Al recibirse los contenedores de seguridad e instalarse la central de alarmas, modificando las claves y códigos que traen de fábrica.
- Cada seis (6) meses.
- Cuando se produzca un cambio en las personas que hayan tenido acceso a las mismas.
- Cuando personas no autorizadas hayan podido tener acceso a las mismas, incluido el personal de las empresas mantenedoras.

Se llevará un libro de registro de los cambios realizados.

Deberá ocultarse la identificación del fabricante, modelo, año de construcción u otros datos que puedan facilitar un conocimiento de las características de las cajas fuertes o cámaras acorazadas.

5.5.4. Registros de entrada/salida

Se realizarán registros aleatorios a la entrada y a la salida, concebidos para que actúen como elemento de disuasión para la introducción no autorizada de material o para la retirada no autorizada de Información Clasificada de una zona o de un edificio.

Los registros en entradas y salidas podrán convertirse en condición para la entrada a un lugar o edificio.

Se colocará un aviso en el que se indique que se pueden realizar registros a la entrada o salida de un determinado establecimiento o local.

5.5.5. Control de Rondas

La supervisión y control de las rondas de seguridad llevadas a cabo por el personal de seguridad, deberá estar diseñado para crear alarmas ante cualquier incidencia que se pueda

declarar durante el transcurso de las mismas, por ejemplo que el guarda llegue tarde (o demasiado temprano) a lugares determinados. El diseño de las mismas se puede realizar desde la empresa de seguridad o ser planificado por la entidad, predefiniendo itinerarios, variando las mismas día a día…. es decir, llevando a cabo las acciones necesarias para que éstas sean realmente efectivas y una herramienta útil para mejorar la seguridad física.

5.5.6. Evacuación

En caso de que se declare cualquier situación de peligro, es necesario tener preestablecido un sistema eficaz de evacuación, conocido por todos los miembros de la organización. Se trata de un conjunto de elementos que se relacionan de manera dinámica entre sí, diseñados para salvaguardar la vida, movilizando personas de un punto de riesgo a un lugar seguro a través de rutas señalizadas, minimizando todos riesgos personales y materiales posibles.

5.6. INTELIGENCIA Y EVOLUCIÓN: PLANIFICACIÓN Y EVALUACIÓN DEL PLAN

Los sistemas de inteligencia surgen como la forma más clara de analizar la información resultado de las actividades anteriormente descritas. En ellos la obtención de datos, la gestión del conocimiento y la integración hacia un objetivo común son la base fundamental de la prevención.

La inteligencia no solamente recaba información del ambiente donde se encuentra, sino indaga más allá de sus límites para hacer mejores estimaciones que permitan tener ventaja táctica y operativa ante los cambios generales de la sociedad y del entorno en particular, que provocan nuevos riesgos basados en la evolución de las amenazas existentes o en la aparición de nuevas.

La función de inteligencia muestra la capacidad del factor humano, para prever y simular, basado en la experiencia y el procesamiento asistido de información, escenarios, para tomar decisiones clara ante situaciones no previstas por la organización, pero probables en el contexto de su entorno de riesgo.

5.7. HERRAMIENTAS

Para la elaboración de un manual de Medidas de Seguridad Física, hay que tener en cuenta las siguientes herramientas:

- BOE núm. 121 de 21 de mayo de 2011: Real Decreto 704/2011 por el que se aprueba el Reglamento de Protección de Infraestructuras Críticas. En él se regula la seguridad de las más de 3.500 instalaciones “sensibles” existentes en España, cuya perturbación supondría un grave impacto sobre los servicios públicos esenciales.

- BOE núm. 102 de 29 de abril de 2011: Ley 8/2011 por la que se establecen las medidas para la protección de las Infraestructuras Críticas. Contempla el desarrollo de un catálogo reservado de esas 3.500 infraestructuras críticas, como centrales nucleares,

embalses, medios de transporte, los sistemas sanitario y financiero o las redes de telecomunicaciones.

En esta norma se establece la puesta en marcha de un Plan Nacional con medidas concretas para hacer frente a las amenazas que se ciernen sobre estas infraestructuras, con participación de las Comunidades Autónomas.

Estas medidas se complementarán con un Plan de Apoyo Operativo elaborado por la Fuerza de Seguridad -estatal o autonómica- que ostente las competencias en la demarcación en la que se encuentre la instalación y que será supervisado por la Delegación del Gobierno.

Ya en noviembre de 2007 el Gobierno creó el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), encargado de controlar, las 24 horas del día, la seguridad de estas infraestructuras.

El CNPIC, que depende de la Secretaría de Estado de Seguridad del Ministerio del Interior, vigila la integridad de estas instalaciones, no sólo ante la amenaza de atentados terroristas, sino también ante la posibilidad de catástrofes naturales.

6. REFERENCIAS

- Real Decreto 3/2010, Esquema Nacional de Seguridad
- MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administración Española http://www.csi.map.es/csi/pg5m20.htm, http://www.ccn.cni.es - http://www.ar-tools.com
- NORMAS UNE: UNE-71501-1, UNE-71501-2, UNE-71501-3 y UNE-71504 en relación al análisis de riesgos de sistemas de información.
- European Network and information Security Agency (ENISA: Risk Management & Information Security Management Systems, http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-isms, http://rm-inv.enisa.europa.eu/rm_ra_methods.html
- Método MOSLER de análisis de riesgos
- Guideline Risk & Crisis Management, Metodología para hacer análisis de riesgos y organización de sistemas de gestión basados en mejora continua
- Critical infrastructure protection report, Government Accountability Office, Washington, DC, May 2005. [Online]. Available: http://www.gao.gov/new.items/d05434.pdf
- Information Security: Technologies to Secure Federal Systems, Mar. 2004,Report to Congressional Requesters, GAO-04-467. [Online]. Available: http://www.gao.gov/new.items/d04467.pdf
- NERC Tech. Rep. Cybersecurity Standards. [Online]. Available: http://www.nerc.com/filez/standards/Cyber-Security-Permanent.html [52] User Manual for the Workshop, North Amer. Electric Rel. Council (NERC), Minneapolis, MN, Sep. 2006. Cybersecurity Standards Workshop
- John Moteff, Paul Parfomak. Standards for Security Categorization of Federal Information and Information Systems. CRS Report for Congress, http://fas.org/sgp/crs/RL32631.pdf. (October 1 2004), accessed march 2010
- National Institute of Standards and Technology (NIST). SP800-53 Recommended Security Controls for Federal Information Systems and Organizations, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf, accessed march 2010 Decima Research, Cyber Security Practices in Canada, Final Report, February 2008] <http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx>
- ISO/IEC 27001, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información
- ISO/IEC 27002, Information Technology. Security Techniques. Code of Practice for Information Security Management.

- ISO/IEC 27005, Information Technology. Security Techniques. Information Security Risk Management.
- ISO/IEC 27006, Information Technology. Security Techniques. Requirements for bodies Providing Audit and Certification of Information Security Managements Systems
- ISO/IEC 27799, Information Technology. Security Techniques. Health Informatics – Information Security Management in Health using ISO/IEC 27002
- ISO/IEC 24762 Guidelines for information and communications technology disaster recovery services
- ISO/IEC CD 27000, Information Technology. Security Techniques. Introduction with Principles, concepts and vocabulary
- ISO/IEC CD 27003, Information Technology. Security Techniques. Implementation guidance for 27001 and 27002
- ISO/IEC CD 27004, Information Technology. Security Techniques. Measurement and metrics for ISM
- ISO/IEC CD 27007, Information Technology. Security Techniques. Guidelines for Information Security Management systems auditing.
- ISO/IEC CD 27008, Information Technology. Security Techniques. Guidelines for auditors on ISMS controls
- ISO/IEC CD 27035, Information Technology. Security Techniques. Information Security Incident Management.
- ISO 19011 Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental
- UNE 66175 Sistemas de gestión de la Calidad. Guía para la implantación de sistemas de indicadores
- NIST 800-53 Recommended Security Controls for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
- NIST 800-82 Guide to Industrial Control Systems http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf
- NIST 800-83 Guide to Malware Incident Prevention and Handling http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
- NIST 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
- NIST 800-34 Contingency Planning Guide for Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

- NIST 800-88 Guidelines for media Sanitization http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
- NIST 800-86 Guide to integrating Forensic Techniques into Incident Response http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
- NIST 800-61 Computer Security Incident Handling Guide http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
- NIST 800-30 Risk Management Guide for Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- NIST 800-100 Information Security Management for Managers http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf
- NIST 200-27 RA Engineering Principles for Information Technology Security http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf
- NIST 800-68 R1 Guide to Securing Microsoft Windows XP Systems for IT Professionals http://csrc.nist.gov/itsec/SP800-68r1.pdf
- NIST 800-41Guidelines for Firewalls and Firewalls Policy http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
- NIST 800-50 Building and Information Technology Security Awareness and Training Program. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
- NIST 800-54 Border Gateway Protocol Security http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf
- NIST 800-123 Guide to General Server Security http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
- NIST 800-115 Technical Guide to Information Security Testing and Assessment http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
- NIST 800-63 Electronic Authentication Guideline http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- NIST 800-64 Security Considerations in the System Development Life Cycle http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
- NIST 800-92 Guide to Computer Security Log Management http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
- FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems
- FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems

- NERC-CIP: el conjunto está constituido por ocho estándares de obligado cumplimiento para la industria del subsector eléctrico de la alta tensión. Los listamos traducidos a continuación:

  - CIP-002-1 Identificación de activos cibernéticos

  - CIP-003-1 Controles en la gestión de la seguridad

  - CIP-004-1 Personal y formación/capacitación

  - CIP-005-1 Perímetros de seguridad electrónica

  - CIP-006-1 Seguridad física

  - CIP-007-1 Gestión de la seguridad de sistemas

  - CIP-008-1 Notificación de incidentes y respuesta

  - CIP-009-1 Plan para la recuperación de activos cibernéticos de carácter crítico

- BS 25999 Business Continuity Management Norma Británica de la Gestión de Continuidad del Negocio
- BS 25777 Information and communications technology continuity management
- FRANCIA: Protección de cadena alimentaria 2007
- UK: Protecting against terror (2nd edition)
- Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (30 de julio de 2002)
- PCI-DSS 2.0, “Payment Card Industry – Data Security Standard), 2010

ANEXO I – SEGURIDAD EN SISTEMAS SCADA

INTRODUCCIÓN Y ÁMBITO

Los Estados modernos se enfrentan actualmente a diferentes desafíos que confieren a la seguridad nacional un carácter cada vez más complejo. Estos nuevos riesgos generados en parte por la globalización, entre los que se encuentran el terrorismo internacional, crimen organizado, empleo y proliferación de armas de destrucción masiva, se suman a los ya existentes entre los que el terrorismo tradicional en el caso de España, era ya un exponente.

En este contexto, es cada vez mayor la dependencia que las sociedades tienen del complejo sistema de infraestructuras que dan soporte y posibilitan la actividad normal de los sectores productivos, de gestión y la vida ciudadana en general. A su vez estas infraestructuras suelen ser interdependientes ente sí, con lo que los problemas de seguridad que puedan desencadenarse en cascada dentro de un sistema, tienen la posibilidad de afectar y ocasionar fallos inesperados cada vez más graves en servicios básicos para la población.

Debido a las ventajas ineludibles que proporcionan los sistemas de información, estos forman parte ya y están integrados dentro del sistema de infraestructuras que sustentan y apoyan nuestra sociedad, convirtiéndose en una pieza clave en la misma.

Infraestructuras de información entre distintos entornos públicos y privados comparten varias tecnologías comunes relacionadas con el uso y las comunicaciones de datos. Esto sucede especialmente en los entornos de sistemas de control.

Una gran parte de sistemas utilizan arquitecturas sólidas y robustas para avanzar en sus negocios o mejorar su rentabilidad, reduciendo costes al incrementar su integración con redes externas de negocio y sistemas de control.

Sin embargo, el empleo de estrategias de integración entre redes, suelen conducir a la aparición de vulnerabilidades que reducen enormemente la seguridad en una organización o infraestructura crítica y puede dejar expuestos sistemas de control muy importantes a amenazas en la red (pudiéndose producir ciberataques).

Por tanto, la protección correcta de sistemas de supervisión y control (Sistemas SCADA) es una pieza angular más a tener en cuenta en materia de seguridad nacional dentro del tejido de infraestructuras críticas para la sociedad.

Este apartado, pretende presentar una serie de prescripciones y recomendaciones como punto de partida, medidas de "defensa en profundidad" que permita a un operador crítico u organización que emplee redes de sistemas de control, seguir los pasos necesarios para asegurar sus entornos SCADA, contactando con su fabricante para desarrollar y aplicar estas medidas.

SISTEMAS SCADA Y CLASIFICACIÓN POR SECTORES

PALABRA CLAVE. DEFINICIONES

SCADA

Según en el libro de Aquilino Rodríguez Penin – Sistemas SCADA[1] damos el nombre de SCADA (Supervisory Control And Data Acquisition o Control con Supervisión y Adquisición de Datos) a cualquier software que posibilite el acceso a datos remotos de un proceso y permita, utilizando las herramientas de comunicación necesarias en cada caso, el control del mismo.

Por parte del NIST 800-82 – Guide to Industrial Control Systems (ICS) Security[2]: Los sistemas SCADA integran sistemas de adquisición con transmisión de datos y software de control para facilitar un sistema de monitorización y control centralizado para distintos flujos de comunicación.

Con lo que podemos definir como SCADA a una aplicación software especialmente diseñada para funcionar sobre ordenadores en el control de producción, proporcionando comunicación con los dispositivos de campo (controladores autónomos, autómatas programables, etc.) y controlando el proceso de forma automática desde la pantalla del ordenador.

OPERADOR CRÍTICO

Empresa, entidad u organismo responsable de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica con arreglo al proyecto de ley 101-1[3].

Una **infraestructura crítica** está designada como tal de acuerdo con el proyecto de ley pero se puede describir según el Plan Nacional de Protección de Infraestructuras Críticas:

“Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas”.

Un **Sistema de Gestión de la seguridad de la Información (SGSI)** es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001.

El término se denomina en Inglés "Information Security Management System" (ISMS).

1 Aquilino Rodríguez Penin – Sistemas SCADA – 2ª edición MARCOMBO 2007 - 448 pags.

2 NIST 800-82 – Guide to Industrial Control Systems (ICS) Security – U.S. Department of Commerce -September 2008- 156 pags.

3 Ministerio del interior - Proyecto de Ley 101-1 por la que se establecen medidas para la protección de las infraestructuras críticas – BOE – 19 de noviembre de 2010.

El concepto clave de un SGSI es para una organización del diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

SISTEMAS SCADA. VISIÓN GENERAL.

Los sistemas SCADA se emplean en infraestructuras e industrias como el sector eléctrico, distribución de agua, depuración, gestión de residuos, carburantes, gas natural, químicas, transporte, farmacéuticas, productos manufacturados… Estos sistemas de control tal como se indica en el primer punto son críticos dentro del funcionamiento del día a día en nuestra sociedad, suelen estar interconectados y ser dependientes entre sí. En esta sección se describe brevemente una visión general de un sistema SCADA incluyendo su distribución típica y componentes. También se ofrece una visión de arriba abajo del mismo dentro del esquema de una organización.

Los sistemas SCADA son sistemas altamente distribuidos utilizados para controlar puntos geográficamente dispersos, con frecuencia expandidos por miles de kilómetros, donde la toma de datos centralizada o el control de una instalación son críticos para el funcionamiento de un sistema.

Un centro de control de SCADA realiza actividades de monitorización y control en zonas de campo, sobre redes de comunicación de larga distancia, incluyendo alarmas de monitorización y gestión del estado de los datos adquiridos. Basados en la información recibida de las estaciones remotas, órdenes de comprobación automáticas o guiadas por un operador, se pueden emitir de nuevo a los dispositivos de control de dichas estaciones, a los que se suelen llamar dispositivos de campo. Estos controlan operaciones tales como abrir o cerrar compuertas, válvulas, recoger datos de los sistemas de sensores o monitorizar la situación del entorno en función de unas condiciones de alarma preestablecidas.

Dos conceptos muy importantes en un sistema SCADA y que en el mercado se confunden es la distinción clara de un sistema en tiempo real y de tiempo real.

Un sistema SCADA es siempre de tiempo real. Esto es debido a que el sistema interactúa de forma dinámica con un entorno continuo. En tiempo real es por ejemplo, una aplicación de bolsa, en la que el usuario quiere ver los datos rápido, pero trabaja en un entorno discreto (lo contrario de continuo) y la reacción es totalmente manual.

Funcionamiento lógico de un Sistema SCADA. Niveles.

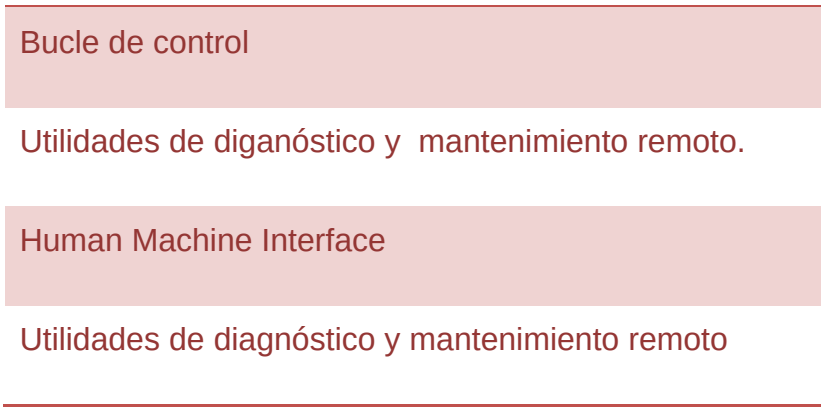

Figura 10: Componentes fundamentales

Como se describe en la figura previa, el funcionamiento básico de un sistema SCADA se basa en los siguientes tres componentes lógicos fundamentales:

- Bucle de control: un bucle de control consiste en sensores de mediciones, hardware de control como PLCs, dispositivos activos como válvulas de control, interruptores, switches, motores y la transmisión de los datos de comunicaciones que emplean.
- Human Machine Interface (HMI). Interfaz hombre-máquina. Técnicos e ingenieros utilizan HMIs para monitorizar y configurar indicadores, algoritmos de control, y ajustar y establecer parámetros de control. El HMI además informa del estado de los procesos en curso e información histórica almacenada.
- Utilidades de diagnóstico y mantenimiento remoto. Utilizadas para prevenir, identificar y recuperar información de un fallo de funcionamiento o incidencia.

Un Sistema SCADA típico tiene combinaciones de estos elementos construidos en torno a una matriz de protocolos de red dispuestos en una arquitectura en distintas capas.

Dentro de una organización desde el punto de vista de la seguridad, podemos representar un ejemplo de esquema eficaz distribuido en zonas de seguridad y la ubicación de un sistema SCADA dentro de la misma.

Así en el anterior esquema organizativo, iremos representando en, zonas de arriba abajo en orden creciente de seguridad, e izquierda a derecha desde el punto de vista del usuario en orden de relevancia en rol de trabajo.

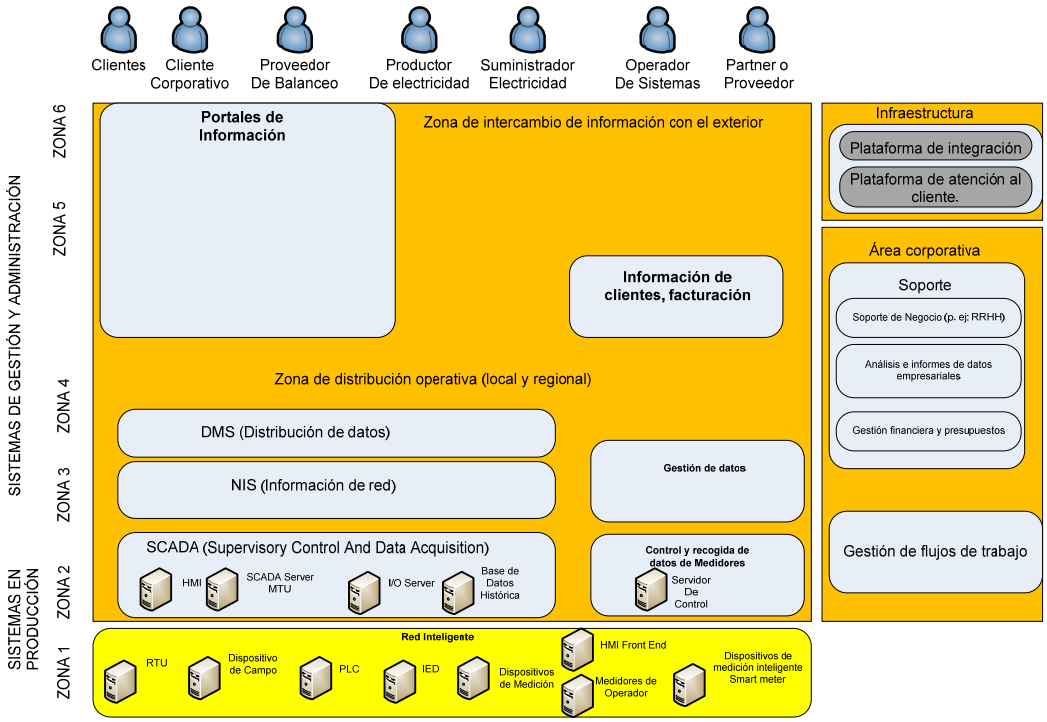

Ilustración 16: Esquema funcionamiento SCADA.

Componentes de control en un Sistema SCADA.

Servidor de Control
SCADA Server or Master Terminal Unit (MTU)
Remote Terminal Unit (RTU)
Controlador Lógico programable (PLC)
Dispositivos de Electrónica Inteligente (IED)
Human-Machine Interface (HMI)
Base de datos Histórica
Input/Output (IO) Server.

Figura 11: Componentes de control

- Servidor de Control. El servidor de control gestiona el software de control de supervisión de PLC diseñado para comunicarse con dispositivos de control de un nivel inferior. El servidor de control accede por debajo a módulos de control en una red SCADA.

- SCADA Server o Master Terminal Unit (MTU). El servidor SCADA es el dispositivo que actúa como maestro en un sistema SCADA. Los terminales remotos y los dispositivos PLC (como se indica más abajo) localizados en zonas de campo remotas suelen funcionar como esclavos.

- Remote Terminal Unit (RTU). El RTU también denominado unidad de telemetría remota, es una unidad de control y adquisición de datos diseñada proporcionar soporte a las estaciones remotas de los sistemas SCADA. RTUs son dispositivos de campo equipados muchas veces con interfaces de comunicación inalámbrica que para dar soporte a situaciones en donde no se dispone de comunicación por cable. A veces los PLC se instalan como dispositivos de campo para funcionar como RTUs; en este caso, el PLC es referido con frecuencia como RTU.

- Controlador Lógico programable (PLC) el PLC es un ordenador industrial pequeño, diseñado para realizar las funciones lógicas ejecutadas por el hardware eléctrico (relays, switches, y temporizadores/contadores mecánicos). PLCs han evolucionado adquiriendo la capacidad de controlar procesos complejos en sistemas SCADA. Otros dispositivos de control a nivel de campo, son controladores de procesos y RTUs; Estos dispositivos ofrecen el mismo control que los PLCs pero diseñados para aplicaciones de control específicas. En entornos SCADA los PLCs se suelen utilizar con frecuencia como dispositivos de campo por su economía, versatilidad, flexibilidad y capacidad de configuración que los RTUs de uso más específico.

- Dispositivos de Electrónica Inteligente (IED). Un IED es un sensor/activador inteligente utilizado para obtener datos, comunicarse con otros dispositivos y realizar procesos a nivel local y tareas de control. Estas tareas en un SCADA pueden ser llevadas a cabo de forma automática.

- Human-Machine Interface (HMI). Un HMI es software y hardware que permite a un operador humano monitorizar el estado de un proceso que está bajo control, modificar ajustes para cambiar el objetivo de control, y tomar el control manual de operaciones automáticas de control en caso de emergencia. El HMI permite también a un ingeniero de control u operador configurar puntos de control y parámetros en el controlador. Un HMI además muestra información de estado de un proceso, información histórica, informes y otra información a operadores, administradores, gestores, proveedores de negocio y otros usuarios autorizados. La localización, plataforma e interface puede variar mucho. Por ejemplo, un HMI puede ser una plataforma dedicada en el centro de control, un portátil en una LAN Wifi, o un navegador en cualquier sistema conectado a Internet.

- Base de datos Histórica. El histórico de datos es una Base de Datos centralizada que almacena toda la información de procesos en un SCADA. Se puede acceder a la

información almacenada en esta base de datos para dar soporte a distintos análisis, desde procesos de control estadístico a planificaciones de nivel empresarial.

- Input/Output (IO) Server. El servidor de entrada y salida es un componente de control responsable de recoger y proveer acceso a procesos de información provenientes subcomponentes de control como PLCs, RTUs e IEDs. Un Servidor IO, puede residir en el servidor de control o en una plataforma de información separada. Son utilizados además como interfaz entre componentes de control de terceras partes, como el HMI y el servidor de control por ejemplo.

Componentes de Red en un Sistema SCADA.

Red de datos de campo.
Red de control.
Routers de Comunicaciones.
Cortafuegos
Modems
Puntos de Acceso Remoto

Figura 12: Componentes de red

Aunque las redes de sistemas de control se han integrado cada vez más con las redes corporativas con el objeto de facilitar su gestión y mantenimiento, se describe aquí una serie de componentes pertenecientes a la red de un sistema de control independientemente de su configuración:

- Red de bus de campo. Conecta sensores y otros dispositivos a un PLC u otro controlador.
- Red de control. Conecta el nivel de control de supervisión con módulos de control de más bajo nivel.
- Routers de Comunicaciones. Interconectando distintos tipos de redes. En un sistema SCADA se utiliza para conectar MTUs y RTUs en una red larga distancia por ejemplo.
- Cortafuegos. Protegiendo dispositivos en una red, monitorizando y controlando paquetes de comunicaciones utilizando políticas de filtrado y restricción de acceso. Su utilización es muy importante dentro de un sistema SCADA en estrategias de segmentación de red en zonas de seguridad.

- Módems. Un módem es un dispositivo utilizado para convertir datos digitales en señal adecuada para la transmisión a través de línea telefónica convencional. En infraestructuras críticas SCADAs se utilizan para comunicar dispositivos de campo remotos y MTUs en larga distancia. Se emplean también en distintos dispositivos, DCS y PLCs para obtener acceso remoto y poder realizar operaciones de mantenimiento como introducción de comandos, modificación de parámetros, diagnósticos y chequeos…

- Puntos de Acceso Remoto. Son distintos dispositivos, áreas y ubicaciones de una red de control a través de los que se accede para realizar configuraciones en remoto así como acceder a datos de procesos. Por ejemplo, el empleo de una PDA o un portátil para acceder remotamente a datos de la red del sistema de control a través de WIFI.

SISTEMAS SCADA POR SECTORES.

Las recomendaciones y medidas de seguridad aquí descritas son adecuadas para organizaciones y entidades que utilicen sus redes de sistemas de control y a la vez mantengan una arquitectura de sistemas de información organizada en varias capas que requiera:

- Mantenimiento de diversos dispositivos de campo, recogida de telemetría, y/o sistemas de procesos industriales.

- Acceso a instalaciones mediante acceso remoto o módem.

- Servicios de atención al público. Por ejemplo, sistemas de control que informen de una caída de corriente en un tramo de vía de un tren, o la detección de un objeto extraño en la vía que pueda provocar un accidente...

- Un sistema de negocio sólido que necesite acceso al sistema de control, acceso externo a internet o acceso directo a otras organizaciones.

Así mismo, estas medidas son aplicables a sistemas SCADA que por sus características, quedan clasificados dentro de sectores estratégicos según el Plan Nacional de Protección de Infraestructuras Críticas. Por tanto, se contempla la inclusión de éstas, en 12 Sectores Estratégicos, subdivididos a su vez en Subsectores, Ámbitos y Segmentos:

- Administración
- Alimentación
- Energía
- Espacio
- Sistema Financiero y Tributario
- Agua
- Industria Nuclear

- Industria Química
- Instalaciones de Investigación
- Salud
- Tecnologías de la Información y las Comunicaciones
- Transporte

GESTIÓN DE LA SEGURIDAD.

ESTABLECIMIENTO DE ROLES.

El factor humano es el que realmente determina la efectividad de cualquier sistema de seguridad. Los problemas de seguridad en redes se pueden achacar a:

- Errores en el manejo del equipo.
- Acciones efectuadas por personal desleal.
- Descuidos en el tratamiento de los equipos.
- Intrusiones exteriores.
- Fallos de equipamiento.

Las tres primeras causas atañen directamente al factor humano y, en parte, son fáciles de tratar. Parte del remedio consiste en promover un sentimiento de pertenencia al grupo, basado en la claridad de los objetivos de seguridad que se persiguen y en la política de apoyo antes que la intimidación.

El establecimiento de roles y funciones para las personas implicadas en un sistema SCADA y más aún en el caso de infraestructuras críticas permite afrontar estos problemas de seguridad de una forma organizada.

Los roles no tienen por que ser personas únicas, sino que pueden ser un equipo de trabajo que decide y actúa de forma solidaria o que una misma persona puede tener varios roles.

Para ello es esencial introducir los roles más significativos en función del sistema SCADA a describir.

Este punto se describe con más profundidad en el apartado siguiente.

Definir funciones y responsabilidades.

Directores, administradores de sistemas, personal de mantenimiento y usuarios deben tener claramente definidas sus obligaciones y responsabilidades en relación con la seguridad del sistema SCADA.

Los planes de seguridad deben definir la jerarquía de seguridad dentro de la empresa. Desde los directores de departamento hasta los usuarios, deben tener definidas sus funciones y posiciones dentro del esquema de seguridad.

Aquellas áreas para las que los individuos tienen asignadas responsabilidades deberían quedar claramente establecidas, en particular en relación a los siguientes aspectos:

- Identificar y definir los activos o elementos de responsabilidad dentro del Sistema SCADA y los procesos de seguridad asociados con cada sistemas específico.

- Asignar una entidad responsable para cada activo y documentar los detalles de esta responsabilidad. Respecto a esta, es recomendable nombrar un propietario que para cada activo que se haga responsable de la protección del día a día.
- Documentar y definir claramente los niveles de autorización dentro del sistema.

Así mismo, hay que tener en cuenta el nombrar a un responsable de seguridad para el sistema de Control con el objeto de asumir la responsabilidad completa del desarrollo e implantación de la seguridad y para dar soporte a la identificación de los controles.

Por último, la mejor forma de progresar es colaborar. Por tanto una buena práctica es también crear grupos de trabajo en el que se permita una colaboración activa por parte de las personas. De estos grupos saldrán propuestas de mejora, encaminadas a eliminar las debilidades del sistema o establecer protocolos de actuación frente a situaciones de crisis.

Referencias:

- ISO/IEC 27002, Information Technology. Security Techniques. Code of Practice for Information Security Management.

CONTROL DE ACCESOS.

El administrador de la red de comunicaciones (no solo de la que accede al SCADA) debe de tener siempre una visión clara y absoluta de sus dominios. De esta manera podrá colaborar en la definición de las políticas de seguridad y actuar rápidamente y en consecuencia ante cualquier alteración de los parámetros preestablecidos en el sistema.

Para incrementar la seguridad en las comunicaciones, pueden establecerse múltiples niveles de seguridad, de manera que si se atraviesa una barrera, quedarán otras. Por ejemplo, se pueden implementar alarmas ante intrusiones, encriptación de datos o jerarquías de usuarios. Este tipo de protección es efectiva frente a intrusiones tanto externas como internas.

Un claro ejemplo son las conexiones wi-fi, generalmente sin protección, o con protecciones muy débiles (programas de escaneado de redes wi-fi permiten a un usuario provisto de una tarjeta de red wifi y un portátil, descubrir las contraseñas de acceso a redes supuestamente protegidas).

Es conveniente que los accesos al sistema sean requeridos desde dentro para minimizar los riesgos (programas específicos de llamada automática se utilizan para encontrar nombres de usuario y contraseñas de los sistemas a los que llaman).

Las puertas traseras permiten el acceso al sistema de manera indetectable o insospechada (por ejemplo, con una tarjeta de red y un portátil).

Por tanto, una conexión abierta es susceptible de cualquier uso. La red Scada es tan resistente a intrusiones como lo sea el más débil de sus puntos de acceso.

Es recomendable establecer una serie de políticas y procedimientos de uso en los recursos del sistema Scada para sólo usuarios autorizados, accesos al software del sistema, procesos etc.

Es especialmente recomendable consultar las guías en el siguiente apartado de referencias para profundizar en estas medias:

Referencias:

NIST SP 800-53 Access Control (AC) family.

Información adicional acerca de controles de acceso se pueden encontrar en los siguientes documentos del NIST:

- NIST SP 800-12 proporciona una guía en políticas de seguridad y procedimientos.
- NIST SP 800-63 proporciona una guía en autenticación electrónica remota.
- NIST SP 800-48 proporciona una guía en seguridad inalámbrica haciendo énfasis en los estándar IEEE 802.11b y Bluetooth.
- NIST SP 800-97 proporciona una guía en el estándar de seguridad de red inalámbrica IEEE 802.11i.
- FIPS 201 Requerimientos para identificación del personal interno y subcontratado.
- NIST SP 800-96 proporciona una guía en la interoperabilidad de los lectores de tarjetas personales.
- NIST SP 800-73 proporciona una guía de interfaces para los sistemas de verificación de identidad personal.
- NIST SP 800-76 proporciona una guía de sistemas biométricos para sistemas de verificación de identidad personal.
- NIST SP 800-78 proporciona una guía de algoritmos criptográficos y dimensionamiento de claves para sistemas de verificación de identidad personal.

GESTIÓN DE CAMBIOS

La implantación de cambios en un sistema SCADA debe controlarse mediante procedimientos formales (documentados) de control de cambios.

Estos procedimientos deberían aplicarse para minimizar la corrupción de los sistemas de información.

La introducción de nuevos sistemas o de cambios importantes en los sistemas existentes, debería seguir un proceso formal de documentación, especificación, pruebas, control de calidad e implantación controlada. Estos dos últimos puntos son de especial importancia debido principalmente a la relevancia de los Sistemas SCADA en infraestructuras críticas donde se intenta evitar en lo posible cualquier impacto dañino que pueda afectar la estabilidad del sistema.

Por tanto, este proceso debería incluir una evaluación de riesgos, un análisis de los efectos de los cambios y una especificación de los controles de seguridad necesarios. Este proceso debería garantizar que los procedimientos de seguridad y control existentes no se pongan en peligro, que los técnicos de la asistencia realizada sólo tengan acceso a aquellas partes del sistema necesarias para su trabajo y que se obtenga un consentimiento y aprobación formales para cualquier cambio.

Referencias:

- ISO/IEC 27002, Information Technology. Security Techniques. Code of Practice for Information Security Management.

GESTIÓN DE LA CALIDAD

La gestión de la seguridad en un sistema SCADA y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos de seguridad), deberían someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.

La revisión independiente, debería comenzar por la Dirección e ir bajando de nivel hasta alcanzar todos los objetivos de control del sistema de seguridad del SCADA.

Una vez generado el informe de la revisión de la que el operador o entidad debe quedar informado de sus resultados, si la revisión independiente identifica que el enfoque para implantar la gestión de la seguridad de la información no es el adecuado o no es el conforme con los compromisos adquiridos en política de seguridad, la Dirección que inició la revisión debería considerar el adoptar las acciones correctivas que correspondan.

A modo de sugerencia, los controles de seguridad propuestos en el documento NIST SP 800-53 Certificación, Acreditación, and Security Assessments (CA) family, proporcionan las bases para realizar revisiones periódicas, proporcionan los medios de certificación necesarios para determinar si los controles de seguridad están implementados correctamente en el sistema SCADA, comprobando que funcionan tal como se han diseñado, y produciendo los resultados deseados para cumplir los criterios de seguridad del sistema. Se debería establecer como responsable un técnico senior de la organización o entidad que gestione los riesgos fuera del alcance de estos controles así como autorizar las distintas intervenciones en el sistema.

Adicionalmente, se deberán monitorizar de forma continua todos los controles de seguridad. Estas actividades de monitorización deben abarcar al menos la gestión de la configuración y componentes de control de información (p.e.: sensores de control, servidores de información, terminales remotos o RTU, PLC s…), análisis de impacto ante cambios en el sistema, revisión continua de controles de seguridad e informes de situación.

Estándar

No sólo para la seguridad de un Sistema SCADA, en general para toda la infraestructura de control es importante tener en cuenta todas las normativas de aplicación, para la misma. El

objeto de alcanzar unos niveles de cumplimiento en características, calidad y seguridad de la instalación.

En este sentido es importante distinguir entre los conceptos de estándar o norma y buenas prácticas.

- Estándar: Son acciones puestas en común y acordadas entre cientos de organizaciones, que habiendo sido probadas en la práctica, su efectividad ha sido contrastada y reconocida por todas.
- Buenas prácticas: como las prescripciones recogidas en este documento, son medidas y acciones de efectividad contrastada por diversas experiencias recogidas en distintas organizaciones pudiendo ser recomendadas. No cuentan con una experiencia y un acuerdo tan amplio como la norma o estándar, pero sí se ha comprobado su efectividad.

En el caso particular de un SCADA estos estándares deben cubrir:

- El rendimiento de equipamiento electrónico.
- Rendimiento del equipo de comunicaciones.
- Prácticas de instalaciones.
- Construcción técnica y mecánica.
- Impacto ambiental.
- Rendimiento para un entorno determinado.
- Requerimientos de Alto y bajo voltaje.
- Medidas para la salud y seguridad de los trabajadores implicados.
- Reglas y regulaciones que son aplicables en el lugar de trabajo.
- Diseño de producción.
- Generación de documentación.

Referencias

- NIST 800-53 Recommended Security Controls for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
- NIST 800-82 Guide to Industrial Control Systems http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

Formación y concienciación.

A pesar de estandarizar procedimientos, el personal debe ser consciente como medida permanente de prevención y compromiso, que la aplicación de los protocolos de seguridad recae en sus manos. Una buena política de seguridad enseña al personal una serie de pautas de comportamiento y además, explica las razones de su conveniencia. Por ejemplo, entrenar al personal para que no faciliten información comprometida como contraseñas, detalles del sistema de control, etc.

Una organización, u operador crítico, debe identificar, documentar y entrenar a todo el personal que tenga responsabilidad o juegue un rol relevante en el Sistema SCADA.

Es recomendable establecer estrategias de seguridad comunes y coordinadas, de manera que se minimicen los casos de iniciativa propia, que suelen acabar en estrategias irracionales y poco efectivas.

Por ejemplo, ciertos equipos deberían ser utilizados únicamente por personal cualificado. No solamente por motivos evidentes de seguridad, sino por la complejidad que suele ir pareja con este tipo de elementos.

Referencias:

- NIST 800-53 Recommended Security Controls for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
- NIST 800-82 Guide to Industrial Control Systems http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

MEDIDAS DE SEGURIDAD EN SISTEMAS SCADA

- Medidas de tipo físico.
- Medidas sobre los sistemas de información.
- Seguridad Perimetral.
- CPC-Primary Control Center.
- CCR-Backup Control Center - CCOUR - Disaster recovery Operational Control Center.
- CCD'S-Communication Management Centers.
- Red de datos.
- Puntos de control.
- Almacenamiento y proceso de información.
- Otros elementos del sistema SCADA.

Sistemas de Información y sistemas SCADA.

El desarrollo de sistemas SCADA ha sido paralelo a la evolución de los microprocesadores, los ordenadores personales y los sistemas de redes y comunicaciones durante la década de los ochenta y noventa. Tecnologías basadas en internet han ido entrando en los diseños de los sistemas SCADA a finales de los 90. Este tipo de tecnologías han dejado a los sistemas SCADA expuestos a nuevos tipos de amenazas.

Es importante prescribir y describir por tanto, las características de seguridad que requieren un tratamiento específico en SCADAs con respecto los sistemas de información, las amenazas y medidas que deben adoptar en su implementación.

Inicialmente, los sistemas SCADA proporcionaban un buen grado de seguridad debido a que se encontraban aislados respecto a otros sistemas y utilizaban hardware, software y protocolos de comunicación específicos para ellos. Debido a la expansión de tecnologías de desarrollo y comunicación a bajo coste (hardware genérico, software con librerías comunes, protocolos de red extendidos, de bajo coste y uso extendido como TCP/IP) ha propiciado que se vean expuestos a múltiples amenazas e incidentes que pueden comprometerlos.

Los sistemas SCADA tienen distintas características que los distinguen de los sistemas de información tradicionales enfrentándose por tanto, a diferentes riesgos y necesitando de daños serios al medioambiente y problemas económicos como interrupción o pérdida de producción y daños económicos graves para el país.

Los Sistemas SCADA tienen requisitos de rendimiento y fiabilidad diferentes y utilizan sistemas operativos y aplicaciones que pueden considerarse poco convencionales para personal con

formación IT convencional. Es más los objetivos de eficiencia de un sistema SCADA puede entrar en conflicto con la seguridad y el diseño de los sistemas de control.

Por tanto, se deberían tener en cuenta las siguientes características en cuanto a la seguridad para un sistema SCADA con respecto a un sistema IT convencional:

- **Requerimientos de rendimiento:** Los sistemas SCADA suelen requerir disponibilidad crítica en tiempo real (teniendo en cuenta y adaptándose a los niveles de retardo e interrupciones definidos por los criterios aplicados para la instalación).

- **Disponibilidad:** Muchos procesos en un sistema SCADA funcionan de forma continua por definición. Interrupciones inesperadas en el suministro eléctrico, no son aceptables dentro del contexto de un SCADA perteneciente a una infraestructura crítica. De producirse, deberían poder planificarse con antelación.

Se debería planificar un testeo exhaustivo del Sistema Crítico antes de que entre en producción para asegurar su alta disponibilidad.

Hay que tener en cuenta que muchos sistemas de control no se pueden detener y rearrancar sin afectar al correcto funcionamiento del sistema.

Por tanto, es recomendable emplear en el despliegue de un sistema SCADA, componentes redundantes que puedan funcionar en paralelo en función de su uso, para proporcionar continuidad de servicio en caso de indisponibilidad.

- **Requerimientos de Gestión de Riesgo:** En un sistema IT típico, la confidencialidad de la información y su integridad son normalmente las principales preocupaciones. En un Sistema de Control la protección humana y la tolerancia a fallos para prevenir pérdidas (p.ej fallo en un sistema de fluido eléctrico en pleno invierno) o poner en peligro la salud pública, pérdida de bienes, daño de productos (una planta de proceso de alimentos p.ej.) son las principales preocupaciones. El personal responsable de operar y proteger un sistema crítico de control debe entender la importancia fundamental que tiene el vínculo entre seguridad y protección

- **Foco en Arquitectura de Seguridad:** En un sistema IT genérico, el foco principal se centra en proteger los activos IT, ya sea centralizado o distribuido y la información almacenada o transmitida entre dichos activos. En ciertas arquitecturas, la información almacenada y procesada en los sistemas centrales es más crítica y es donde necesitan más protección. Para un sistema SCADA, los dispositivos clientes, remotos, PLC, estación de operaciones, control DCS, etc, deben ser protegidos cuidadosamente debido a su responsabilidad final en el control de procesos. La protección del servidor central es también muy importante en un sistema SCADA, debido a la posibilidad de sufrir un impacto no deseado en cada dispositivo remoto.

- **Interacción física:** En un Sistema IT genérico, no hay interacción física con el entorno. Los sistemas de control pueden sin embargo, tener interacciones muy complejas con procesos físicos (p.ej.: un sistema de esclusas en la distribución de agua para una ciudad) y consecuencias en el dominio del SCADA que se puede manifestar en sucesos

físicos. Todas las funciones de seguridad de un sistema crítico de control deben ser probadas antes (p.ej en un entorno de desarrollo y pruebas en un SCADA similar) para demostrar que no comprometen el funcionamiento habitual del sistema SCADA.

- **Respuestas en tiempo crítico:** En un Sistema IT, el control de acceso se puede implementar sin afectar el flujo de datos de forma significativa. Para algunos SCADA, respuestas automatizadas y o respuestas de sistema provocadas por la interacción humana son críticas (p.ej el cierre de un tramo de autopista en caso de saturación de tráfico). Por ejemplo, requerir acceso y autenticación mediante contraseña en un HMI no debe interferir con el protocolo de emergencia que tiene designado el SCADA. El flujo de datos no se debe interrumpir ni ver comprometido. El acceso a estos sistemas debe ser restringido por controles de seguridad física rigurosos.

- **Operación del sistema:** Los sistemas operativos de un SCADA (OS) y sus aplicaciones pueden no aceptar prácticas de seguridad habituales en un sistema IT. Los sistemas heredados son especialmente vulnerables a la caída de recursos o indisponibilidad temporal de los mismos. Las Redes de control suelen ser con frecuencia más complejas y requieren un nivel diferente de experiencia (por ejemplo, redes de control que son gestionadas por ingenieros y no personal IT). El software y hardware es mucho más difícil de actualizar en la red de un sistema de control crítico operacional. Muchos sistemas pueden no tener las funcionalidades deseadas incluidas capacidades de encriptación, registro de errores y protección de claves de acceso.

- **Limitaciones de Recursos:** Un SCADA y su sistema operativo en tiempo real son con frecuencia sistemas limitados en recursos que no suelen incluir funcionalidades típicas de los sistemas IT. Puede no ser posible actualizar los sistemas y componentes de un sistema SCADA con las medidas de seguridad más modernas. En algunos casos, no se permiten soluciones de seguridad de terceros debido a las licencias de uso del SCADA y los acuerdos de servicio, pudiendo perderse el servicio de soporte si aplicaciones de terceros se instalan sin la aprobación o acuerdo previo del vendedor.

- **Comunicaciones:** Los protocolos de comunicaciones y medios utilizados en entornos SCADA para control de campo y comunicaciones entre procesos internos son diferentes de un sistema IT genérico y pueden ser propietarios.

- **Gestión del cambio:** Una adecuada gestión del cambio es fundamental de cara a mantener la integridad de un sistema SCADA y un sistema IT. Software sin parchear o actualizar es uno de los mayores puntos débiles de un sistema. Las actualizaciones de software en un sistema IT incluyendo parches de seguridad, se realizan de acuerdo a procedimientos y políticas de seguridad. Además estos procedimientos suelen utilizar herramientas de actualizaciones centralizadas en un servidor. Las actualizaciones de software no siempre se puede aplicar en un tiempo razonable para un SCADA debido a que necesitan ser testeados en profundidad por el proveedor de la aplicación de control, así como el usuario del sistema en la infraestructura crítica en la que se ubica el SCADA en cuestión. Una vez pasadas estas validaciones, se requiere planificar con mucha antelación (días/ semanas) el momento de interrupción del SCADAD que se va a proceder a actualizar. También pueden requerirse comprobaciones adicionales como

parte del proceso de actualización. Otra dificultad es que muchos sistemas SCADA utilizan versiones anteriores de SO que no se soportan por parte del vendedor. En consecuencia, los parches más recientes pueden no ser aplicables. Esta gestión de actualizaciones se puede aplicar a hardware y a firmware. Un proceso de gestión del cambio cuando se aplica a un sistema SCADA, requiere ser llevado a cabo por expertos en el sistema SCADA (p.ej. ingenieros de control) trabajando con personal de IT y seguridad.

- **Gestión del soporte.** Un sistema típico IT permite distintos tipos de soporte a sistemas dispersos pero interconectados a través de distintas arquitecturas tecnológicas. Un sistema SCADA suele contar con un servicio de soporte a través de un único proveedor, normalmente sin contar con alguna otra solución de soporte de otro proveedor.
- **Ciclo de vida de los componentes:** Un sistema IT típico tiene una vida breve de 3 a 5 años, debido a la rápida evolución de la tecnología. Para un sistema SCADA, su tecnología ha sido desarrollada en muchos casos de forma específica con una implementación completa, su ciclo de vida puede llegar al orden de 15-20 años y en algunos casos más aún.
- **Acceso a componentes:** los componentes de un sistema IT típico suelen ser de fácil acceso y mantenimiento, localizados en lugares muy concretos. Mientras, los componentes de un sistema crítico de control SCADA pueden estar aislados, ubicados en sitios remotos, y requieren de un gran esfuerzo físico para conseguir acceder a ellos.

Requerimientos de rendimiento
Disponibilidad
Requerimientos de Gestión de Riesgo
Foco en Arquitectura de Seguridad
Interacción física
Respuestas en tiempo crítico
Operación del sistema
Limitaciones de Recursos
Comunicaciones
Gestión del cambio

Gestión del soporte
Ciclo de vida de los componentes
Acceso a componentes

Figura 13 :Resumen que resalta las características de un sistema IT frente a un SCADA desde el punto de vista de la seguridad.

INCIDENCIAS, AMENAZAS Y VULNERABILIDADES.

Incidencias en Sistemas SCADA críticos:

Las incidencias posibles que pueden afectar un sistema SCADA perteneciente a una infraestructura crítica incluyen lo siguiente según el caso:

- Bloqueo o retraso en el flujo de datos a través de la red SCADA que puede interrumpir su funcionamiento.
- Cambios no autorizados a instrucciones, órdenes, código, sistemas de alarma, que pueden dañar, desconectar o apagar equipo, impactar en el entorno, medioambiente o poner en peligro la vida de seres humanos.
- Información poco precisa enviada a los operadores del sistema, tanto para encubrir cambios no autorizados o provocar que se lleven a cabo acciones inapropiadas, que podrían tener varios efectos negativos.
- Software del SCADA o valores de configuración modificados, o Software SCADA infectado con malware, que puede tener varios efectos dañinos.
- Interferencia con la operación de sistemas de protección pueden poner en peligro vidas humanas.

Perfiles de seguridad. Amenazas. Vulnerabilidades y Vectores de Ataque.

Las redes de los sistemas de control han pasado de ser islas separadas a redes interconectadas que coexisten con entornos IT corporativos, estando expuestos a amenazas de seguridad. Por ejemplo, código compacto transportable en forma de virus, gusanos y código parásito pueden manifestarse tanto en las redes de sistemas de control (SCADA) como en las redes estándar corporativas. Para dispositivos con firmware incorporado, como controladores o relés, el código malicioso no suele tener impacto a través de la propagación en la red. No obstante, puede contagiar a dichos dispositivos remotos a través de una descarga de datos rutinaria pudiendo ocasionar graves daños.

Adicionalmente, hay que prestar atención a los siguientes amenazas de seguridad críticas, incluidas las relacionadas con:

- Puertas traseras y agujeros en el perímetro de red.
- Vulnerabilidades en protocolos comunes.
- Ataques en dispositivos de campo o remotos.
- Ataques a bases de datos.
- Interceptación de comunicaciones y ataques "Man in the middle" (MitM).[4]

Entendiendo esos vectores de ataque se pueden aplicar medidas y estrategias de mitigación bastante efectivas. El nivel de conocimientos acerca de estos vectores por parte del personal relacionado con el SCADA perteneciente a la infraestructura crítica debe de adaptarse para poder mitigar estas amenazas. La seguridad eficaz del sistema de control depende de cómo los operadores de sistemas y proveedores entienden las arquitecturas que pueden verse comprometidas.

Aislando y protegiendo Sistemas SCADA en infraestructuras críticas: Estrategias de defensa en profundidad

Los objetivos principales en seguridad para la implementación de un sistema SCADA como parte de una infraestructura crítica deberían abarcar los siguientes puntos:

Restringir el acceso lógico a la red del Sistema de Control y monitorizar la actividad de red
Restricción del acceso físico a los dispositivos y redes del Sistema SCADA
Protegiendo componentes individuales del SCADA contra intrusiones
Manteniendo el sistema en funcionamiento durante condiciones adversas
Restaurando el sistema después de una incidencia

Figura 14: Objetivos principales

- **Restringir el acceso lógico a la red del Sistema de Control y monitorizar la actividad de red.** Esto incluiría utilizar una zona desmilitarizada (DMZ) en la

[4] Un **ataque *man-in-the-middle o JANUS*** (**MitM** o *intermediario*, en español) es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

arquitectura de red con cortafuegos que filtren el acceso entre la red corporativa y la red del SCADA, y teniendo mecanismos de autenticación separados para usuarios de la red corporativa y la red del sistema de control. Se debería contar también con un IDS (Intrusión detection system) cuya función es monitorizar el tráfico y la actividad de la red del sistema sin impactar en la misma. El sistema SCADA debería utilizar una topología de red organizada en múltiples capas, con las comunicaciones más críticas dentro de la capa más segura y fiable.
De esta manera, se propone un modelado de zonas de seguridad asociado al principio de defensa en profundidad en el que se van añadiendo distintos niveles de seguridad cuanto más crítico es el elemento dentro del sistema SCADA a proteger.

- **Restricción del acceso físico a los dispositivos y redes del Sistema SCADA.** El acceso físico no autorizado a componentes del sistema puede producir una interrupción grave en la funcionalidad del SCADA. Se deben usar una combinación de controles de acceso como, cierres de seguridad, blindajes, lectores de tarjetas y / o vigilancia.

- **Protegiendo componentes individuales del SCADA contra intrusiones.** Esto incluye el despliegue de parches de seguridad de forma regular después de haberse testeado en condiciones reales, desconectando todos los puertos no utilizados y servicios, restringiendo privilegios de acceso al SCADA en función de los roles de cada persona, siguiendo y monitorizando trazas de auditoría, y utilizando controles de seguridad como software de antivirus y de integridad de ficheros donde sea posible para prevenir, disuadir, detectar y mitigar el malware.

- **Manteniendo el sistema en funcionamiento durante condiciones adversas.** Esto implica diseñar el SCADA de forma que cada componente tenga su contrapartida redundada. Adicionalmente, si un componente falla, debe caer de forma que no genere tráfico innecesario en el SCADA y otras redes, y que no cause mayores problemas como un fallo en cascada.

- **Restaurando el sistema después de una incidencia:** Las incidencias son inevitables y debido a ello, es esencial un plan de respuesta. Una característica fundamental de un buen programa de seguridad es su capacidad y rapidez ante la recuperación de desastres.

Para gestionar la seguridad adecuadamente en un SCADA, es fundamental para un equipo multifuncional especializado en seguridad informática, compartir su conocimiento y experiencia mitigando así riesgos. El equipo de seguridad informática debe consistir en un miembro del personal IT de la entidad u organización, un ingeniero de control, un operador del sistema de control, un experto en redes y sistemas, un miembro del equipo de gestión y un miembro del departamento de seguridad física como mínimo. Para que sea más completo y de cara a la continuidad, el equipo de seguridad informática debería consultar al proveedor del sistema de control así como el integrador del mismo. El equipo de seguridad informática debería informar directamente a la dirección del sitio o el CIO/CSO de la compañía, que en respuesta debe aceptar la responsabilidad y auditoría de seguridad del SCADA crítico a monitorizar.

Un programa de seguridad efectivo para un SCADA crítico sería aplicar estrategias de defensa en profundidad consistentes en distribuir distintos mecanismos de seguridad en capas de tal forma que el impacto o fallo en uno se vea minimizado.

Defensa en profundidad en un sistema SCADA.

Por tanto en un sistema SCADA perteneciente a una infraestructura crítica, una estrategia de defensa en profundidad debe consistir en:

- Desarrollar políticas de seguridad, procedimientos, entrenamiento, material de referencia y formación que se apliquen específicamente al SCADA.
- Considerar las políticas de seguridad en el SCADA y procedimientos teniendo en cuenta la normativa vigente publicada por el Ministerio del Interior para infraestructuras críticas. Se deberá destacar las siguientes normativas: NISTIR 7628, IEC 62351, NERC 1300 (CIP 002 - CIP 009), IEEE 1686 – 2007, NIST 800 – 82, NIST 800-53, ISO/IEC 27002.

Es importante tener en cuenta así mismo que las normativas NERC 1300 (CIP 002 - CIP 009) son fundamentales de cara a las terminales y dispositivos remotos dado que son medidas de seguridad específicamente desarrolladas para las mismas (ver figura resumen CIP).

Se desplegará además mayores niveles de seguridad a medida que el nivel de riesgo o amenaza aumente.

- Dirigir la seguridad durante todo el ciclo de vida del SCADA, desde el diseño de arquitectura, a la instalación, el mantenimiento y finalmente, su retirada del servicio.
- Implementar una topología de red para el SCADA que tenga múltiples capas, con las comunicaciones más crítica ubicadas en la capa más segura y fiable.
- Proporcionar separación lógica entre las redes del SCADA y corporativa (p.ej. inspección completa mediante cortafuegos entre zonas.
- Utilizar arquitecturas de red en DMZ (para prevenir el acceso directo entre la red corporativa y el SCADA por ejemplo)
- Asegurar que los componentes críticos son redundantes y están ubicados en redes redundantes y balanceadas.
- Diseñar sistemas críticos para una degradación benigna (tolerante a fallos) que prevenga una catástrofe en cascada.
- Desconectar puertos sin utilizar y servicios en el sistema SCADA después de hacer las pertinentes comprobaciones para que no impacten en la operación del SCADA.
- Restringir el acceso físico a la red SCADA y sus dispositivos.

- Restringir privilegios de acceso en función de la tarea específica de cada persona. Utilizar un control de acceso basado en Roles y configurando cada Rol basado en el principio de facilitar el menor número de privilegios posible.
- Considerar la utilización de mecanismos de autenticación y proporcionar credenciales de forma separada para usuarios de la red corporativa y la red del sistema SCADA (por ejemplo, las cuentas de red del SCADA no utilizan cuentas de usuarios de la red corporativa).
- Utilizando tecnología avanzada, como tarjetas inteligentes para la verificación de la identidad del personal.
- Implementar controles de seguridad como software de detección de intrusiones (IDS), Unified Threat Management (UTM) software, antivirus, validación de integridad de ficheros , cuando sea posible para prevenir, disuadir, y mitigar la introducción, exposición y propagación de software malicioso, hacia y desde el SCADA.
- Aplicar técnicas de seguridad como cifrado y/o tablas criptográficas en el almacenamiento y comunicaciones del SCADA cuando se considere apropiado. Por ejemplo, emplear dispositivos de campo (RTU) con tecnología criptográfica, que usen contraseñas cifradas, políticas de contraseñas, diferentes perfiles de acceso, registro, protocolos de seguridad SSH y SSL para las comunicaciones y el control de acceso, y protocolos de control (DNP, IEC101, IEC104, etc) según la norma IEC-62351.
- Desplegando de forma obligatoria y regular parches después de haber sido comprobados en condiciones de campo o en un test del sistema si es posible, antes de instalarlo en el ICS.
- Seguimiento y monitorización de trazas de auditoría en áreas críticas del SCADA.

Por último se adjunta un esquema de zonas de seguridad aplicable a un sistema SCADA:

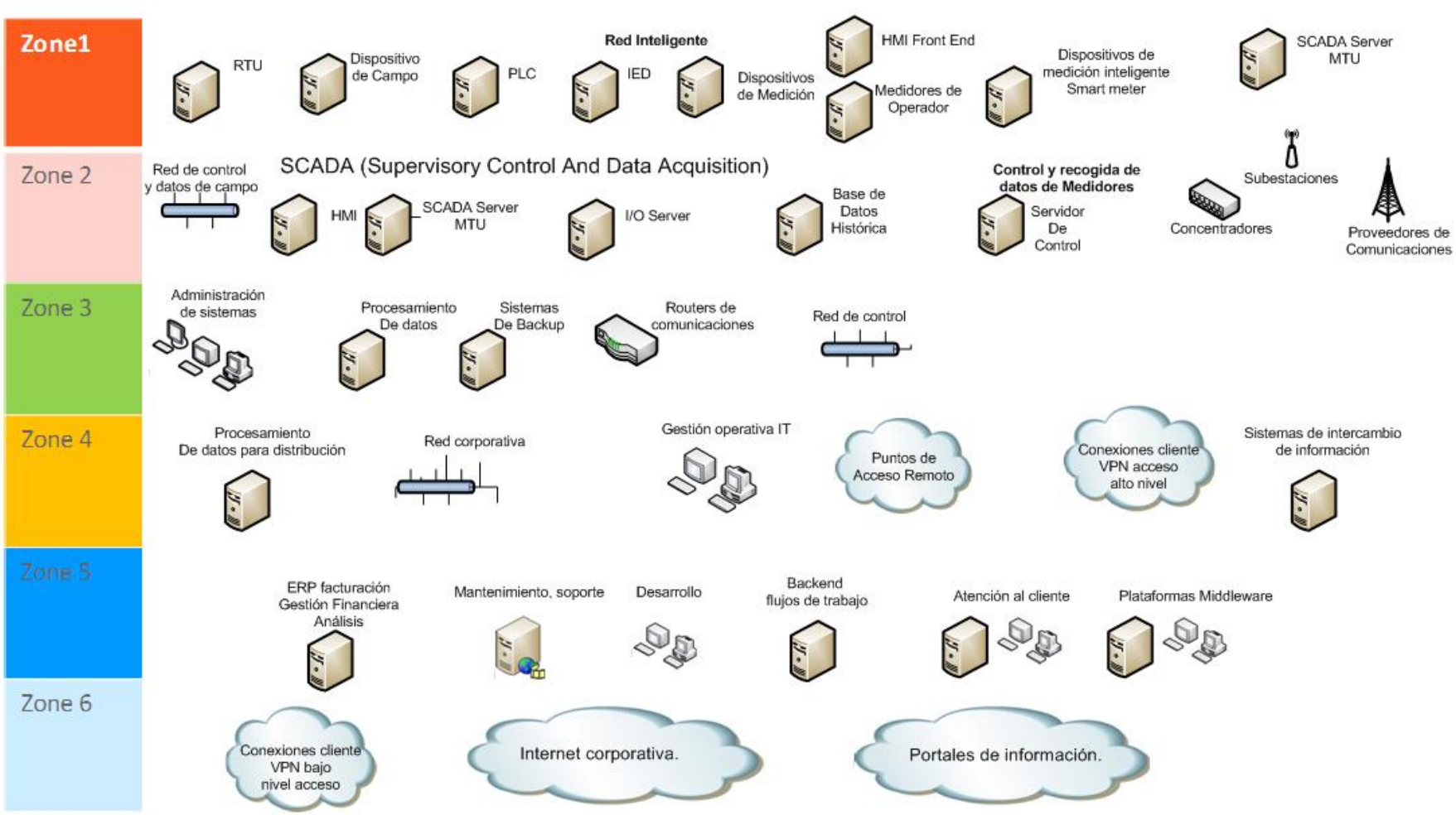

Ilustración 17 :Esquema de zonas de seguridad aplicables a SCADA

IDENTIFICACIÓN Y GESTIÓN DE INCIDENCIAS.

DISASTER RECOVERY.

Un plan de recuperación de desastres es fundamental en la continuidad y disponibilidad de un Sistema SCADA debido a la criticidad de procesos que puede acometer (sobretodo si forma parte de una infraestructura crítica).

Un plan de recuperación de desastres (PRD) para un sistema SCADA debe incluir los siguientes elementos:

- Requiere reaccionar a eventos o condiciones de duración variable que provoquen su activación.
- Procedimientos para operar el SCADA en modo manual a pesar de tener graves daños en su electrónica externa hasta que se pueda volver a operar de forma segura.
- Tener claras las funciones y responsabilidades del personal.
- Procedimientos y procesos de respaldo y almacenamiento seguro de la información.
- Diagrama lógico de la red del sistema completo y actualizado.
- Lista de personal autorizado al sistema SCADA.
- Procedimiento de comunicación y lista de personal para contactar en caso de emergencia incluyendo el fabricante del sistema, administradores de red, soporte del SCADA etc.
- Información actualizada de la configuración de todos los componentes.

El plan debe definir tiempos de respuesta para sustitución de componentes o piezas dañadas en caso de emergencia. Si es posible, las piezas críticas difíciles de obtener deberían almacenarse en inventario (en reserva).

El plan de seguridad debe definir una política completa de respaldo y recuperación que debe tener en cuenta:

- La criticidad del sistema para determinar el tiempo de restauración del mismo. Este requerimiento puede justificar la necesidad de un sistema redundante, un equipo de reserva, o copias del sistema de ficheros.
- La frecuencia en que cambia información de datos críticos y configuraciones. Este punto marcará la frecuencia y alcance de las copias de respaldo.
- La seguridad del almacenamiento interno y externo de las copias de respaldo realizadas. Por ejemplo si se trasladan a otra instalación por seguridad.

- Almacenamiento seguro de los medios de soporte, licencias en información de configuraciones.
- Identificación del personal responsable de realizar, comprobar almacenar y restaurar los respaldos.

Gestión de Riesgos.

Su objetivo es conocer el riesgo y el nivel de impacto.

Para ello es fundamentar tener en cuenta las siguientes iniciativas:

- Identificar los activos y valorar su criticidad.
- Extraer información de los activos (por ejemplo, a través de los registros que éstos generan)
- Procesar la información de los distintos sistemas y correlacionarla para detectar posibles riesgos y generar las alertas de seguridad pertinentes.
- Definir flujos de trabajo para la gestión de estas alertas de seguridad.
- Definir un conjunto de indicadores de seguridad que permitan determinar en cada momento el nivel de riesgo del sistema de control.

Análisis Forense.

Se centra principalmente en conocer que ha sucedido.

Se basa en Localizar el incidente y sus causas, garantizando la trazabilidad y recuperación parcial o total de la información perdida. Este punto es especialmente importante en un Sistema SCADA por el valor crítico de la información y su papel como infraestructura dentro de un sistema crítico. Se puede facilitar su elaboración si se han seguido las políticas de seguridad adecuadas, manteniendo sistema de trazas eficaz en el SCADA. Hay que tener en cuenta, que debido a la disparidad de tecnologías y funciones de estos sistemas, así como su antigüedad en algunos casos, supone una dificultad adicional en esta tarea.

AUDITORÍA DE SEGURIDAD

Su fin es detectar las vulnerabilidades y amenazas del Sistemas de Control de Infraestructuras Críticas (SCIC).

Una auditoría es un examen y revisión independiente de registros y actividades para evaluar la idoneidad de los controles del sistema, asegurar el cumplimiento de las políticas y procedimientos operativos establecidos, y recomendar los cambios necesarios en controles, políticas o procedimientos.

La Auditoría de la seguridad en un sistema SCADA abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. El auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

Por su parte, la seguridad lógica se refiere a la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

Para poderla llevar a cabo, deben instalarse herramientas de registro (auditoría) para todas las redes y equipamientos del sistema.

Estas acciones permiten identificar todos los elementos de red, su actividad, estado operativo y efectividad. De esta manera, es posible identificar puntos débiles y obrar en consecuencia.

Siempre se debe saber con certeza qué es lo que hay conectado a una red SCADA, cómo se conecta a la misma, y qué hace con exactitud para determinar si su configuración es la adecuada.

RECOMENDACIONES PARA SISTEMAS SCADA.

Es necesario determinar que el sistema está funcionando tal como se ha planeado. Auditorías periódicas sobre el sistema SCADA deben llevarse a cabo para validar los siguientes puntos:

- Los controles de seguridad presentes durante el test de validación del sistema (p.ej.: test de aprobación de fábrica, o test de aprobación del emplazamiento) continúan instalados y operando correctamente en el sistema en producción.
- El sistema en producción está libre de situaciones que comprometan su seguridad y proporciona información de la naturaleza y alcance de estas situaciones en caso de que se produzcan.
- El programa de gestión del cambio sigue con rigurosidad un circuito de auditorías con análisis y aprobaciones para todas las modificaciones.
- Los controles de seguridad presentes durante el test de validación del sistema (p.ej: test de aprobación de fábrica, o test de aprobación del emplazamiento) continúan instalados y operando correctamente en el sistema en producción.

- El sistema en producción está libre de situaciones que comprometan su seguridad y proporciona información de la naturaleza y alcance de estas situaciones en caso de que se produzcan. l programa de gestión del cambio sigue con rigurosidad un circuito de auditorías con análisis y aprobaciones para todas las modificaciones.

- Los resultados de cada auditoría periódica deben ser expresados en un formato de desempeño contra un conjunto de de métricas predefinidas apropiadas que muestren el nivel de seguridad conseguido y las pautas a seguir. Se deben enviar las métricas de desempeño en seguridad a las a todas las partes interesadas, junto con una visión de las tendencias en desempeño de la seguridad.

- Almacenamiento de registros. Tradicionalmente, las auditorías de seguridad se han basado siempre en los registros guardados. Utilizar las herramientas apropiadas en un sistema SCADA requiere un conocimiento profundo de un profesional IT familiarizado con el SCADA, sistemas críticos e implicaciones de seguridad de la instalación. Muchos de los dispositivos de control de proceso que forman parte del SCADA, llevan instalados muchos años y no tienen la capacidad de suministrar los registros para auditar descritos aquí. Por tanto, la aplicación de estas herramientas más modernas de auditoría, depende de las capacidades y componentes del sistema SCADA.

- En una operación eficiente y segura, las tareas críticas que gestionan la red en un entorno SCADA, están garantizando fiabilidad y disponibilidad. En sistemas industriales sometidos a una regulación, la necesidad de cumplir esta, añade complejidad a la gestión de la seguridad y autenticación, gestión e instalación de registros y todas las funciones que pueden aumentar el umbral de operatividad de la infraestructura.

- La utilización eficaz de herramientas de auditoría y gestión de logs proporciona una ayuda valiosa en mantener y demostrar la integridad de un sistema SCADA desde su instalación y durante su ciclo de vida.

- El valor de estas herramientas en el entorno, se puede calcular por el esfuerzo requerido en recualificar o volver a testear el SCADA, cuando su integridad ha quedado en duda por un ataque, un accidente o un error.

- El sistema SCADA debe proporcionar información fiable sincronizada en fechas en apoyo a las herramientas de auditoría.

- La monitorización de sensores, logs, IDS, antivirus, gestión de actualizaciones, gestión de políticas de software y otros mecanismos de seguridad debe hacerse en tiempo real cuando sea posible. Un servicio de monitorización de primer nivel recibiría alarmas, tomaría una decisión inicial ante el problema y emprendería acciones al personal apropiado de la instalación, para alertar e intervenir.

- Utilidades de auditoría de sistema deben incorporarse siempre en proyectos de sistemas SCADA nuevos y existentes. Estas herramientas, se deben testear (p.ej. en un SCADA parecido fuera de servicio) antes de ser desplegadas en el sistema SCADA en producción. Son capaces de proporcionar registros sólidos de situación e integridad del sistema.

- Además, utilidades de gestión de logs, pueden señalar un ataque o una incidencia en curso proporcionando localización y trazas del mismo para ayudar solucionar la incidencia. Siempre debe de haber medios para rastrear las trazas del operador en la consola del sistema, tanto manualmente (p.ej. entrar en la sala de control) o de forma automática (al entrar en la aplicación o al logarse en el sistema operativo).

- Deben desarrollarse políticas y procedimientos sobre lo que queda registrado, cómo se graba (o imprime), cómo queda protegido, quién tiene acceso a los logs y cómo/cuando deben revisarse. Estas políticas y procesos dependerán del sistema SCADA y la plataforma en la que trabaje. Sistemas antigüos por ejemplo, utilizan registros impresos que son revisados por personal de administración de sistemas, operadores de sala o expertos en seguridad. Los log almacenados por el sistema SCADA pueden ser almacenados en varias ubicaciones y pueden estar o no encriptados.

Deben desarrollarse **políticas y procedimientos** sobre lo que queda registrado, cómo se graba (o imprime), cómo queda protegido, quién tiene acceso a los logs y cómo/cuando deben revisarse. Estas políticas y procesos dependerán del sistema SCADA y la plataforma en la que trabaje. Sistemas antiguos por ejemplo, utilizan registros impresos que son revisados por personal de administración de sistemas, operadores de sala o expertos en seguridad. Los registro almacenados por el sistema SCADA pueden ser almacenados en varias ubicaciones y pueden estar o no encriptados.

Siempre debe de haber medios para rastrear las trazas del operador en la consola del sistema, tanto manualmente (p.ej. entrar en la sala de control) o de forma automática (al entrar en la aplicación o al logarse en el sistema operativo).

Referencias

Los controles de seguridad descritos en el “NIST SP 800-53 Audit and Accountability (AU) family” proporcionan políticas y procedimientos para generar registros de auditoría y sus requerimientos de contenido, capacidad y conservación. Los controles proporcionan también protección para reaccionar a problemas tales como un error de auditoría o una limitación de capacidad en los registros de auditoría. Los datos auditados deben estar protegidos de modificaciones y diseñados con capacidad para no ser repudiados.

Orientación adicional de controles de auditoría se pueden encontrar en los siguientes documentos:

- NIST SP 800-12 proporciona orientación en políticas de seguridad y procedimientos.

- NIST SP 800-61 proporciona orientación para controlar incidencias de seguridad informática y conservación de datos de auditoría.

- NIST SP 800-92 proporciona orientación en gestión de registros (incluyendo registros de auditoría).

- NIST 800-82 Guide to Industrial Control Systems
  http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

MEJORA CONTINUA.

PLAN DE MEJORA CONTINUA.

Todo plan de mejora continua debe planificar, hacer, verificar y actuar.

Para un Sistema SCADA es completamente factible la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) estando incluido este como ciclo de mejora continua de un sistema.

Dicho ciclo se suele representar a través del círculo de Deming:

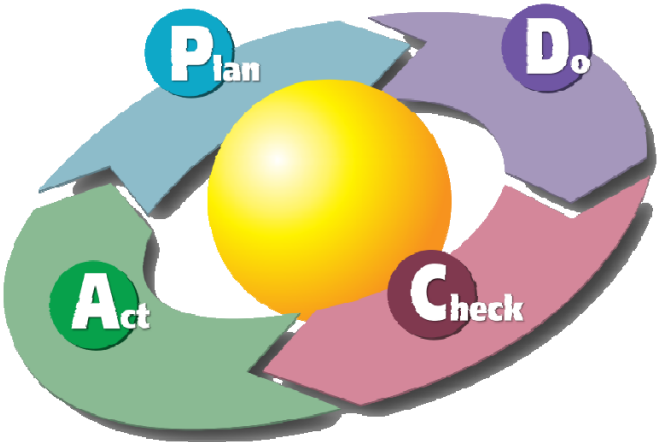

Ilustración 18: Ciclo de Deming

En este apartado incluiremos dentro de lo que supone un plan de mejora continua los procesos de gestión continua, mantenimiento y escalabilidad de un Sistema SCADA como paso fundamental para la evolución del mismo.

Referencias:

- Guideline Risk & Crisis Management, Metodología para hacer análisis de riesgos y organización de sistemas de gestión basados en mejora continua.
- ISO/IEC 27001, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información .
- ISO/IEC 27002, Information Technology. Security Techniques. Code of Practice for Information Security Management.

GESTIÓN CONTINUA

La gestión continua de la seguridad de un sistema SCADA tiene la responsabilidad de mantener las capacidades del mismo operativas en todo momento.

Todo plan de gestión continua debe:

- Planificar los puntos de control definidos para el sistema de seguridad del SCADA a proteger.
- Monitorizar los puntos de control definidos para el sistema con el objeto de cumplir con los requisitos del plan de Seguridad definidos para el mismo.
- Informar de cualquier suceso anómalo o incidencia que pueda producirse.
- Revisar en procesos periódicos de revisión las anomalías que se produzcan con el objeto de adoptar medidas correctoras. Se incluirán estas de nuevo en el primer punto.

Los resultados de la gestión continua del sistema serán auditados periódicamente revisando los SLA s establecidos en cada caso que permiten mantener y actualizar los parámetros del servicio.

MANTENIMIENTO

Los tiempos de mantenimiento pueden reducirse al mínimo si el sistema está provisto de unas adecuadas herramientas de diagnóstico que permitan realizar tareas de mantenimiento preventivo, modificaciones y pruebas de forma simultánea al funcionamiento normal del sistema. En un sistema SCADA la disponibilidad de datos y su integridad es esencial con lo que es necesario contar con este tipo de medidas para garantizar su seguridad y correcto funcionamiento.

ESCALABILIDAD. EJEMPLOS DE MEJORA.

Este concepto está básicamente relacionado con la posibilidad de ampliar el sistema con nuevas herramientas o prestaciones y los requerimientos de tiempo necesarios para implementar estas ampliaciones.

La aplicación de control debe poder evolucionar, adaptándose al entorno que controla, de manera que funcione de forma eficiente sin importar el tipo de equipamiento o el volumen de datos. Del mismo modo los puntos de control y seguridad establecidos en el mismo, deben poder mantenerse y ser igualmente ampliables sin verse comprometidos.

Un sistema SCADA debe poder ampliarse y actualizarse. Puede empezar con un único servidor para todas las tareas (SCADA, archivo, alarmas, comunicaciones..). El problema aquí, reside en que todo pasa por un único punto que es el talón de Aquiles del sistema.

Un planteamiento correcto, permitirá un mejor aprovechamiento de los recursos, creará una mayor disponibilidad y aumentará la seguridad del sistema. Por ejemplo, si se decide implementar los sistemas de control de las instalaciones de forma centralizada, será más costoso realizar una ampliación posterior, pues habrá que acabar modificando el hardware, cambiando el servidor aquel que debe ser más rápido, debido a las nuevas exigencias, o el software, modificando la aplicación.

Sin embargo, de forma distribuida, la ampliación posterior siempre será más sencilla, pues se podrá empezar con único servidor que realice todas las tareas y, cuando la situación lo requiera, ir añadiendo más servidores (de menor coste, dado que las tareas serán más concretas) que sirvan de apoyo al inicial, compartiendo tareas del primero.

Aquí tendremos el problema principal de la centralización, un fallo en el servidor (el único) provocará una caída del sistema entero, mientras que si hay varios servidores compartiendo tareas, el sistema será más tolerante a fallos.

La tendencia es la de atomizar los grandes sistemas de supervisión y control en multitud de componentes, distribuyendo los sistemas de control y las aplicaciones en diferentes máquinas distribuidas a lo largo de la red y con capacidad para comunicarse entre ellas (servidores de datos y de alarmas, generadores de informes, de gráficas de tendencia, etc.).

En un caso típico por ejemplo, un sistema SCADA que disponga de servidores redundantes que proporcionan un sistema seguro y resistente a fallos pueden contar con las siguientes características:

- Si cae la pasarela a un proceso, el control de Campo sigue operativo gracias al panel de operador.
- El sistema de comunicaciones está duplicado . Uno o varios switches se ocupan de la gestión de la red corporativa.
- Varios terminales SCADA permiten acceso al control de la instalación (Incluyendo al panel de Operador).
- Los servidores redundantes toman el control en caso de problemas en los principales, etc.

REFERENCIAS Y BIBLIOGRAFÍA

- Centro Nacional para las infraestructuras Críticas - ¿Qué es una infraestructura crítica? –Ministerio del Interior
  http://www.cnpic-es.es/preguntas_frecuentes/infraestructura_critica/

- David Kuipers, Mark Fabro - Control Systems cyber Security: Defense in depth Strategies-INL-May 2006.

- Ministerio del interior - Proyecto de Ley 101-1 por la que se establecen medidas para la protección de las infraestructuras críticas – BOE
  http://www.congreso.es/public_oficiales/L9/CONG/BOCG/A/A_101-01.PDF – 19 de noviembre de 2010

- Jaime Montoya Estándar Internacional ISO/IEC 27002
  http://www.monografias.com/trabajos67/estandar-internacional/estandar-internacional.shtml

- NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations Access Control (AC) family - U.S. Department of Commerce - August 2009 -141 pags.
  http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

- NIST 800-82 Guide to Industrial Control Systems (ICS) Security - U.S Department of Commerce - September 2008 -
  http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

ANEXO II - ÍNDICE DE TABLAS

ANEXO III - ÍNDICE DE FIGURAS

ANEXO IV - ÍNDICE DE ILUSTRACIONES