Servicio Nacional de Aprendizaje SENA

CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN
- CASO DE ESTUDIO -

CASO DE ESTUDIO

La unidad objeto de estudio no es de nueva creación, sino que lleva años tramitando expedientes de forma local, antes manualmente, ahora por medio de un sistema informático propio. A este sistema informático se le ha añadido recientemente una conexión a un archivo central que funciona como "memoria histórica": permite recuperar datos y conservar los expedientes cerrados. La última novedad consiste en ofrecer un servicio propio de la administración electrónica, en el que los usuarios pueden realizar sus tramitaciones vía web, usando su Número de Identificación Fiscal (NIF) como identificación, más una contraseña personal. El mismo sistema de tramitación es usado localmente por un funcionario que atiende a los ciudadanos que se presentan en las dependencias de la unidad.

El responsable del proyecto de administración electrónica, alarmado por las noticias aparecidas en los medios sobre la inseguridad de Internet, y sabiendo que un fallo en el servicio conllevaría un serio daño a la imagen de su unidad, asume el papel de promotor. En este papel escribe un informe interno, dirigido al director de la unidad, en el que da cuenta de:

- Los medios informáticos con que se está trabajando y los que se van a instalar.
- Las incidencias ocurridas desde que la unidad existe.
- Las incertidumbres que le causa el uso de Internet para la prestación del servicio.

Con base en dicho informe argumenta la conveniencia de lanzar un proyecto ASEGURA. La dirección, convencida de la necesidad de tomar medidas antes de que ocurra una desgracia, crea un comité de seguimiento formado por los responsables de los servicios involucrados: atención a usuarios, asesoría jurídica, servicios informáticos y seguridad física.

Se determina que el alcance del proyecto será el servicio de tramitación electrónica, presencial y remota. También se estudiará la seguridad de la información que se maneja: expedientes.

Respecto del equipamiento, se analizarán equipos y redes de comunicaciones. Se toma la decisión de dejar fuera del estudio elementos que pudieran ser relevantes en un análisis más detallado como pudieran ser los datos de identificación y autenticación de los usuarios de los sistemas, las áreas de trabajo del personal que los maneja, la sala de equipos (centro de proceso de datos) y las personas relacionadas con el proceso. Está previsto lanzar un futuro proyecto ASEGURA más detallado que profundice en dichos aspectos.

Explícitamente se excluirá la evaluación de la seguridad de los servicios subsidiarios que se emplean. El análisis es local, circunscrito a la unidad que nos ocupa. Dichos servicios remotos se consideran, a efectos de este análisis, "opacos"; es decir, que no entraremos en analizar cómo se prestan.

El lanzamiento del proyecto incluye una reunión de la dirección con el comité de seguimiento en la que se exponen los puntos principales del análisis somero realizado por el promotor que queda habilitado como director del proyecto ASEGURA en el que participaran dos personas de su equipo junto con un contrato de asesoría establecido con una empresa consultora externa.

Uno de los miembros del equipo interno tendrá un perfil técnico: ingeniero de sistemas. A la consultora externa se le exige identificar nominalmente a las personas que van a participar y firmar un acuerdo de confidencialidad.

El proyecto se anuncia internamente mediante comunicación general a todo el personal de la unidad y notificación personal a aquellas personas que se verán directamente afectadas. En estas comunicaciones se identifican las personas responsables del proyecto.

Para la valuación de los activos nos podemos apoyar en varias metodologías dispuestas para este propósito, para este ejemplo trabajaremos con SP-830:

NIST SP 800 – 30 (National Institute of Standards and Technology)

La guía de gestión de riesgo para sistemas de tecnología de la información – Recomendaciones del Instituto Nacional de Estándares y Tecnología; es una guía que propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información. Sin embargo, esto no es suficiente, pues se necesita del apoyo de toda la organización para que los objetivos y alcance de la gestión de riesgos concluyan con éxito.

Esta metodología abarca 9 pasos:

1. Caracterización del sistema.
2. Identificación de amenazas.
3. Identificación de vulnerabilidades.
4. Análisis de controles.
5. Determinación de probabilidades.
6. Análisis del impacto.
7. Determinación del riesgo.
8. Recomendaciones de controles.
9. Documentación de resultados.

A. Objetivos

El objetivo de desempeño de la gestión de riesgos es habilitar la organización para cumplir su misión mejorando el aseguramiento del sistema TI que almacena, procesa o transmite información organizacional.

Adicional permite la gestión de riesgos para tomar decisiones bien fundamentadas de gestión y justificar los gastos que forman parte de un presupuesto de TI para asistir a la administración en lo que se autoriza (o acredita) de los sistemas de TI sobre la base de la documentación de soporte a partir de los resultados de la gestión de riesgos.

A manera de ejemplo se realizará una parte de cada uno de los pasos propuestos por SP- 830, para este caso utilizaremos las dos primeras actividades que incluye la caracterización de los activos y su valuación de acuerdo a los principios de la seguridad.

I. Caracterización del sistema

La primera parte consiste en identificar cuáles son los activos con que cuenta la empresa, para esta parte tomaremos como ejemplo los propuestos en el caso de estudio, para realizar de manera más ordenada y clara se recomienda caracterizar los activos de acuerdo a categorías que entre otras pueden ser:

Instalaciones, comunicaciones, equipamiento, aplicaciones, personal, activos esenciales, entre otros que se consideren nos faciliten su clasificación y posterior valuación de los activos.

Podemos crear tablas que nos facilitan el agrupamiento de activos en cada una de las categorías antes mencionadas.

Tabla 1. Clasificación de Activos

Instalaciones	Comunicaciones	Equipamiento	Aplicaciones	Personal	Activos esenciales
Edificio empresa	Conexión a Internet Conexión de red LAN Servicio de Correo electrónico	Servidor Computadores de escritorio Impresora Fotocopiadora	Software tramitación de archivos	Operador software	Bases de Datos

II.Valuación de activos

Dentro de la etapa de caracterización de la infraestructura, luego de la identificación y clasificación de los activos por categorías se realiza la valuación de estos. Esta valuación se hace teniendo como punto de partida los pilares de la seguridad informativa y para cada uno de ellos se definen diferentes niveles de cumplimiento como se consigna en la tabla siguiente. El nivel más alto indicaría que se cumple a cabalidad con un determinado pilar de la seguridad informática.

Tabla 2. Valores de valuación de activos

Criterios de valuación de los activos	
Muy alto	5
Alto	4
Medio	3
Bajo	2
Muy bajo	1

Para determinar el valor de la valuación de los activos se debe de considerar los siguientes criterios de acuerdo a los pilares de la seguridad de la información.

Tabla 3. Pilares de seguridad - Criterios de valuación

Criterios de valuación de los activos		
Confidencialidad	**Integridad**	**Disponibilidad**
Los componentes del sistema TI serán accesibles sólo por aquellos usuarios autorizados.	Los componentes del sistema TI sólo pueden ser creados y modificados por los usuarios autorizados.	Los usuarios deben tener disponibles todos los componentes del sistema TI cuando así lo requieran.

Para determinar el valor de la valuación de los activos se debe de considerar los siguientes criterios de acuerdo a los pilares de la seguridad de la información.

Tabla 4. Valuación de activos

Proceso de valuación de Activos Categoría: Equipamiento				
Activo	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor del activo**
Servidor	5	5	5	15
Computador de escritorio	4	4	3	11
Impresora	3	1	1	5
Forocopiadora	1	1	1	3

Como se puede evidenciar en la tabla anterior se concluye que el activo llamado servidor que aloja la aplicación de tramitación de archivos es el más crítico de la categoría seleccionada.