VÍDEO intypedia011es

LECCIÓN 11: ANÁLISIS Y GESTIÓN DE RIESGOS

AUTOR: Dr. José A. Mañas

Universidad Politécnica de Madrid, España

ALICIA

Hola, bienvenidos a Intypedia. Hoy vamos a estudiar cómo gestionar los sistemas de información. ¡Acompáñanos!

ESCENA 1. RIESGOS Y PROTECCIONES EN LOS SISTEMAS DE INFORMACIÓN

ALICIA

En la lección de hoy vamos a analizar la confianza que merecen los sistemas de información con los que trabajamos, ya que dependemos fuertemente de ellos en actividades personales, empresariales o en la administración pública.

BERNARDO

Eso es verdad; pero ¿no basta con ir trabajando y ya veremos qué hacer cuando algo falle?

ALICIA

Puede no ser lo más prudente. Imagina que no funcionaran los sistemas que controlan la red eléctrica, los hospitales, los trenes, etc. Si un día fallan de golpe, no podemos ponernos a improvisar. Y lo mismo pasa con el secreto y la integridad de nuestros datos. Cuando tenemos un incidente es demasiado tarde para evitarlo y podríamos ser culpables de negligencia.

BERNARDO

Vale. Entiendo que el problema puede ser serio. Pero me parece a mí que hay mil situaciones posibles: fallos nuestros, de nuestros proveedores, catástrofes naturales, gente interesada en robar, espionaje, etc.

ALICIA

La responsabilidad no termina porque la culpa sea ajena. Sea quien sea el culpable, hay que intentar atajar las consecuencias. Cuando uno no puede anticiparse a los hechos, lo profesional es preparar planes de acción para mitigar los incidentes y establecer soluciones alternativas.

BERNARDO

Me parece que todo esto es muy relativo.

ALICIA

Cierto. Cada sistema de información atiende a un negocio concreto y sólo el responsable del negocio sabe lo que le interesa proteger y de qué o de quién. Aunque hay medidas generales que prácticamente interesan a todo el mundo, otras habrá que adecuarlas a cada caso. En esta tarea nos puede ayudar el análisis de impacto de los incidentes.

ESCENA 2. ANÁLISIS DE IMPACTO Y ANÁLISIS DE RIESGOS

ALICIA

Se llama análisis de impacto al ejercicio de imaginarnos las consecuencias de que haya un incidente, accidental o deliberado. O sea, responder preguntas del tipo: ¿qué pasaría si se revela un dato confidencial? ¿Qué pasaría si manipulan nuestra información? ¿Qué pasaría si nos quedamos sin servicio durante X horas?

BERNARDO

¡Uf! Y eso, ¿cómo se calcula?

ALICIA

Más que calcularse, hay que preguntar al responsable de la información o el servicio. A efectos del análisis de riesgos, esta estimación del impacto es un dato de entrada.

A veces se sabe porque existe una legislación u obligaciones contractuales que marcan obligaciones. La normativa relativa a la protección de datos de carácter personal puede ser un ejemplo. Otras veces hay obligaciones de servicio, como puede ser el suministro eléctrico o que funcione el teléfono. Otras veces es simplemente la estrategia empresarial que ha determinado la Dirección.

BERNARDO

Eso no resulta muy técnico.

ALICIA

No lo es. Es un tema de gobierno de la organización. Normalmente es más importante saber el daño que podría derivarse de un fallo de seguridad que saber lo que cuesta el sistema de información en sí mismo.

BERNARDO

Muy bien, ahora que ya sabemos qué es lo que nos pasaría si algo falla, ¿qué hacemos?

ALICIA

Analizar situaciones. Es lo que se llama análisis de riesgos.

No es fácil. Cuanto menos, es muy laborioso porque los sistemas son muy ricos en componentes y las posibles situaciones se multiplican. Es curioso; hay gente que añade equipos y equipos, funciones y funciones y no se da cuenta de que lo que es una oportunidad para su negocio, es igualmente una oportunidad para el beneficio ajeno o un posible punto de problemas.

BERNARDO

Comprendo que hay que empezar por un buen inventario e imagino que eso implica entender el negocio, qué información maneja y qué servicios tiene que prestar. Luego habrá que saber qué equipos hemos puesto y quizás las comunicaciones. ¿Voy bien?

ALICIA

Correcto Bernardo. Dentro de los activos no deberías olvidar otras causas de problemas como las instalaciones físicas y las personas relacionadas con el sistema. Lo de considerar a las personas como un activo al principio suena curioso, pero luego la experiencia nos dice que hay más problemas por personal interno que se equivoca, o que directamente quiere causar daño, que por fallos técnicos.

BERNARDO

Perdona, pero más que soluciones parece que te encantan los problemas. ¿No eres un poco agorera?

ALICIA

Bueno, una cosa es analizar todo lo que anticipemos que puede ocurrir y otra es ponerlo en perspectiva. Tras inventariar activos y amenazas, hay que calificar cada escenario posible para conocer su impacto y su riesgo. El impacto es de lo que hablamos antes: las consecuencias para el negocio que nos traemos. El riesgo va un paso más allá y ordena los incidentes según la probabilidad de que ocurran. Con esas estimaciones podemos priorizar los riesgos y concentrarnos en aquellas cosas más probables y/o que traigan las peores consecuencias.

BERNARDO

Alicia, esas palabras de impacto y riesgo parecen sustanciales.

ALICIA

Y lo son. A veces se llaman indicadores del estado de seguridad y sirven para tomar decisiones. El impacto mide lo que puede pasar. El riesgo mide lo que probablemente pase.

ESCENA 3. GESTIONANDO LOS RIESGOS

BERNARDO

Alicia, supongamos que es posible un cierto escenario cuyo impacto o cuyo riesgo me inquietan. ¿Qué puedo hacer?

ALICIA

Típicamente tienes 4 formas de afrontar los riesgos. La primera es evitar la situación, la segunda mitigar el peligro, la tercera pasárselo a otro y la cuarta aceptar lo que hay.

La primera medida es preguntarnos si necesitamos todo lo que tenemos. Por ejemplo, poner un servidor Web público en nuestro servidor de bases de datos puede ser una forma de dar un servicio espectacular a nuestros clientes, pero también abre la puerta a que haya una fuga o un robo de información: se lo estamos poniendo fácil al ladrón. Podemos separar el servidor de producción del de acceso público y así el escenario de riesgo es otro.

La segunda medida es mitigar el impacto, mitigar el riesgo o ambos. El riesgo lo mitigas con medidas preventivas. Por ejemplo, cifrando el disco duro reduces las oportunidades de que la información acabe en malas manos si pierdes el portátil en un taxi. El impacto se reduce con medidas reactivas o de recuperación. Por ejemplo, si tienes copias de seguridad, no impides que se pierda un fichero o que se averíe el servidor de bases de datos, pero sabes que te recuperas rápidamente y sigues trabajando.

BERNARDO

Antes hablaste de aceptar los riesgos. Suena absurdo. ¿Quién quiere aceptar un riesgo?

ALICIA

Aceptar riesgos es parte de nuestras decisiones rutinarias. Hay que equilibrar riesgos y posibles beneficios. Muchos montamos en avión pese al riesgo de que se desplome. Y ponemos tiendas Web porque el beneficio del comercio elecrónico creemos que compensa el riesgo de fraude. Estas decisiones son una vez más de gobierno del negocio. No las puede tomar un técnico, las tiene que tomar la Dirección. Muchas actividades consisten en buena medida en asumir riesgos para alcanzar unos ciertos beneficios. Lo que el análisis de riesgos proporciona es la información para saber qué nos estamos jugando y tomar decisiones informadas.

BERNARDO

Ya veo. También hablaste de pasarle el riesgo a otro. Suena raro eso ¿no? …

ALICIA

Quizás es por la forma de decirlo. Contratar un seguro es pasarle el riesgo a la aseguradora. Subcontratar un servicio con un acuerdo de niveles de servicio, es pasarle el riesgo al proveedor. Son cosas habituales que funcionan bien cuando todos ganan con el reparto. Date cuenta de que los servicios horizontales diluyen el riesgo al tratar con muchos clientes. Si se quema tu casa, tu pérdida es enorme. Pero para la aseguradora es una casa quemada entre miles de casas aseguradas. Y las cuentas salen para las dos partes.

Es curioso, ahora está de moda hablar de ‘compartir riesgos’ para resaltar que el asunto incumbe a todas las partes y que lo que se busca es ubicar el riesgo en el lugar ideal. Los acuerdos entre partes son también muy ricos en variantes.

BERNARDO

Veo que tenemos cuatro opciones: eliminar, mitigar, traspasar o aceptar. Unas opciones parecen técnicas y otras no, con costes económicos muy diferentes. Al final ¿es una cuestión de dinero?

ALICIA

Es una cuestión de gestión de recursos: técnicos, humanos y económicos. La decisión se toma a la vista de las consecuencias y del coste de la solución. El análisis de riesgos te califica las consecuencias y tú verás cuántos recursos pueden justificarse para la solución. Al final hay que llegar a un equiibrio. La máxima a recordar es que el coste de las medidas de protección no puede superar el bien protegido.

BERNARDO

Muy interesante. En cualquier caso los análisis de riesgos no serán para toda la vida, ¿o sí? En mi empresa hay sistemas de información que no han cambiado en años.

ALICIA

Pues en un mundo dinámico, el análisis de riesgos ha de ser tan dinámico como el mundo. El contexto suele cambiar. El riesgo no es sólo asunto tuyo, el riesgo analiza lo que puede ocurrirle a tu sistema enfrentado a un cierto entorno. Los cambios del entorno hay que seguirlos con cuidado, no sólo porque hay atacantes; cada cambio de legislación o de prácticas sectoriales obliga a analizar de nuevo. Hay que ser muy ágiles y muy rápidos. Más vale un análisis de riesgos de trazos gruesos, que un análisis perfecto. La gestión de riesgos es para tomar decisiones estructurales. Los detalles son para combatir los incidentes concretos.

BERNARDO

Alicia, vamos a ver si puedo resumirlo. Primero, inventariamos los activos que tenemos. Segundo, analizamos los incidentes que pudieran ocurrir. Tercero, añadimos las medidas de seguridad. Y después calculamos el impacto y el riesgo. Con eso tomamos alguna decisión que puede ser aceptarlo, o modificar algún aspecto del sistema, lo que nos lleva a hacer otro análisis. Y eso es recurrente. Por una parte hay que tomar decisiones para ya; y por otra hay que irse adaptando a los cambios que vayamos percibiendo, sean por nuestra parte o por el entorno.

ALICIA

Lo has resumido muy bien Bernardo. Ahora hay que ser metódicos para que no se nos pase nada. No olvides que todo lo imprevisto es un riesgo oculto ante el que no estaremos preparados.

ESCENA 4. RECOMENDACIONES. METODOLOGÍAS

BERNARDO

Alicia, hay un tema que me inquieta. Parece que los análisis de riesgos sean como ejercicios de muy alto nivel, en donde abstraemos los detalles funcionales y nos centramos en el valor del sistema para el negocio. ¿Estoy en lo cierto?

ALICIA

Efectivamente. Los análisis pueden ser de detalle, pero no suelen serlo. Por ejemplo, supongamos que montamos un sistema con recuperación de sesiones en un equipo alternativo si falla el principal. Técnicamente es un montaje complejo; pero desde el punto de vista de seguridad se simplifica muchísimo: la confidencialidad y la integridad de la información debe mantenerse igual en todos los equipos. Y la disponibilidad se limita a imponer un tiempo máximo de interrupción del servicio.

BERNARDO

Es lo que imaginaba. Pero la consecuencia de lo anterior es que dependemos mucho del arte del analista. Y a mí … no sé … las cosas artesanas en materia de seguridad me dan un cierto vértigo.

ALICIA

Y no te falta razón Bernardo. No creo que el análisis de riesgos sea 100% independiente del analista. Se trata de una actividad de consultoría donde hay un factor humano no despreciable. Lo que hay que hacer es seguir un método de forma que el análisis sea homologable y estar siempre preparados para poder explicar el porqué de las conclusiones.

BERNARDO

¿Y existe un método universal para ello?

ALICIA

Pues sí, hay bastante consenso alrededor de las normas de análisis de riesgos de ISO que establecen una serie de marcos de nomenclatura y actividades. Por cierto, estas normas no se limitan sólo a seguridad de la información, sino que unifican riesgos de diferentes tipos para poder tomar decisiones combinando riesgos laborales, riesgos financieros, riesgos técnicos, riesgos medioambientales, etc.

BERNARDO

Muy bien, ya me voy enterando. Entiendo entonces que esa creatividad del analista puede estar encauzada, por ejemplo, usando herramientas que impongan una metodología. ¿Eso es posible?

ALICIA

Sí, claro. De hecho, hacer un análisis de riesgos sin herramientas raya en lo heroico. En todo caso, sería imposible de mantener y de hacer los análisis marginales pertinentes para los cambios constantes del sistema y del entorno.

En España, la Administración Pública lleva varios años liderando actividades para analizar y gestionar riesgos en los sistemas de información. El motivo no es otro que el proceso administrativo y las actividades de la administración.

Como resultado de esta inquietud podemos citar Magerit y Pilar. Magerit es una guía práctica para analizar y gestionar riesgos dentro del marco ISO. Y Pilar es una herramienta que ayuda a gestionar el volumen de información que requiere un análisis de riesgos profesional. Ambos instrumentos han trascendido del ámbito público y se

aplican en todo tipo de escenarios, simplemente adecuando el tipo de información y servicios a cada caso concreto.

BERNARDO

Muy interesante, he aprendido bastante sobre riesgos. Parece que esto de anticiparse a los incidentes va a hacernos pensar mucho. En la página Web de intypedia hay información adicional a esta lección. ¡Hasta luego!

ALICIA

¡Adiós!

Guión adaptado al formato intypedia a partir del documento entregado por el Dr. José A. Mañas de la Universidad Politécnica de Madrid.

Madrid, España, noviembre de 2011

http://www.intypedia.com

http://twitter.com/intypedia