Material adicional del Seminario Taller

Riesgo vs. Seguridad de la Información

Gestión del riesgo

Desde hace varias décadas la información ha pasado de ser un producto del desarrollo de las actividades de las organizaciones a ser un insumo de alto valor, fundamental para el cumplimiento de los objetivos y subsistencia de las mismas. En muchas de estas organizaciones, y con el objeto de brindar eficiencia y agilizar la administración, los procesos incorporan la utilización de sistemas automatizados de procesamiento de información.

El auge en el rol que ha tomado la información, sin embargo, no exime a las organizaciones de una serie de peligros, que se han visto incrementados por las nuevas amenazas surgidas del uso de tecnologías de la información y las comunicaciones. De esta manera, toda organización se encuentra constantemente expuesta a una serie de riesgos mientras que resulta imposible establecer un entorno totalmente seguro.

La **gestión de riesgos** se presenta entonces como una actividad clave para el resguardo de los activos de información de una organización y en consecuencia protege la capacidad de cumplir sus principales objetivos. Es un proceso constante que permite a la administración balancear los costos operacionales y económicos causados por la interrupción de las actividades y la pérdida de activos, con los costos de las medidas de protección a aplicar sobre los sistemas de información y los datos que dan soporte al funcionamiento de la organización, reduciendo los riegos que presentan los activos de información a niveles aceptables para la misma.

El proceso de gestión de riesgos involucra cuatro actividades cíclicas:

- la identificación de activos y los riesgos a los que están expuestos
- el análisis de los riesgos identificados para cada activo
- la selección e implantación de controles que reduzcan los riesgos
- el seguimiento, medición y mejora de las medidas implementadas

Esta breve guía se centrará en las primeras dos actividades del proceso de gestión de riesgos, llegando hasta la definición de recomendaciones de controles a implementar que permitan reducir el riesgo al que el sistema en estudio está expuesto.

Antes de continuar definiremos al **riesgo** como función de la probabilidad de que una amenaza aproveche o explote una potencial vulnerabilidad en un activo de información, y de la magnitud del daño resultante de tal evento adverso en la organización.

I. Identificación de activos de información

El primer paso en la gestión de los riesgos es la definición del alcance que tendrá el estudio. En este paso se definen los límites del sistema en estudio a la vez que se detallan los recursos y la información que constituyen el sistema, que se denominarán activos de información, algo esencial para posteriormente definir el riesgo. Desde ya, es necesario un amplio conocimiento del ambiente en cuestión.

El primer concepto a contemplar es el de activo de información. Se denominan **Activos de Información** a todos aquellos recursos de valor para una organización que generan, procesan, almacenan o transmiten información.

Esto comprende:

- funciones de la organización,
- información y datos,
- recursos físicos (equipamiento, edificios),
- recursos humanos,
- recursos de software,
- servicios, etc.

Asociado al concepto de activo está el rol de **Propietario de Información**, quién es responsable de clasificar al activo de información de acuerdo con su grado de criticidad y de definir qué usuarios podrán acceder al mismo.

II. Clasificación de activos de información

Se define la **criticidad** de un activo en función de cuán necesario resulta para las actividades de un área o la misión de la organización. Dado que en una organización no todos los activos de información poseen el mismo valor, a la vez que un mismo activo puede poseer un valor diferente para distintas áreas, se establece una valoración estandarizada donde el propietario de la información clasifica cada activo según las tres características básicas de la seguridad de la información: *la confidencialidad, la integridad, y la disponibilidad* a la que debe estar sometido.

Una posible escala para la clasificación es la siguiente:

CONFIDENCIALIDAD	VALOR
Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera de la Universidad.	**0**
Información que puede ser conocida y utilizada por todos los agentes de la Universidad.	**1**
Información que sólo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo.	**2**
Información que sólo puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio a la Univ. o terceros.	**3**

INTEGRIDAD	VALOR
Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades de la Universidad.	**0**
Información cuya modificación no autorizada puede repararse aunque podría ocasionar un perjuicio para la Universidad o terceros.	**1**
Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para la Universidad o terceros.	**2**
Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades.	**3**

DISPONIBILIDAD	VALOR
Información cuya inaccesibilidad no afecta la actividad normal de la Universidad.	**0**
Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para la Universidad.	**1**
Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades de la Universidad.	**2**
Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la Universidad.	**3**

El valor máximo de las tres características determinará la criticidad del activo de información analizado.

- **Si todos son 0 ==> Criticidad 0-Nula**
- **Si el máximo es 1 ==> Criticidad 1-Baja**
- **Si el máximo es 2 ==> Criticidad 2-Media**
- **Si el máximo es 3 ==> Criticidad 3-Alta**

Ejemplo: Identificación de activos

ACTIVO	CONFIDEN-CIALIDAD	INTEGRIDAD	DISPONI-BILIDAD	CRITICIDAD
Alta de movimientos mensuales	**2**	**2**	**1**	**2**
Base de Datos de Haberes	**2**	**2**	**2**	**2**
Red de Telefonía	**0**	**1**	**1**	**1**
Destructoras de papel	**0**	**0**	**0**	**0**
…	…	…	…	...

III. Identificación de vulnerabilidades y amenazas

El objetivo de este paso es identificar las vulnerabilidades en los activos y compilar un listado de amenazas potenciales que son aplicables al sistema que está siendo evaluado.

Una **vulnerabilidad** es toda debilidad en un activo de información, dada comúnmente por la inexistencia o ineficacia de un control. Una **amenaza** es todo elemento que, haciendo uso o aprovechando una vulnerabilidad, atenta o puede atentar contra la seguridad de un activo de información. Las amenazas surgen a partir de la existencia de vulnerabilidades, e independientemente de que se comprometa o no la seguridad de un sistema.

Son ejemplos de vulnerabilidades, entre muchas otras:

- la falta de mantenimiento en las instalaciones.
- la falta de capacitación al personal.
- la falta de manuales de procedimientos.
- la inexistencia de respaldos de información y equipamiento redundante.
- la falta de políticas de acceso a los sistemas informáticos.
- la divulgación o utilización de contraseñas inseguras.
- la transmisión de información por medios inseguros.
- los errores de programación en las aplicaciones.
- la falta de mobiliario de oficina con llave.
- el acceso irrestricto al lugar de trabajo.
- la eliminación insegura de la información.

Son ejemplos de amenazas:

- de origen natural: eventos tales como inundaciones, terremotos, tornados, incendios, tormentas eléctricas y otros desastres naturales.
- de origen humano: eventos que son permitidos o causados por seres humanos, sean estos actos involuntarios tales como errores en la operatoria, errores de programación, ausencia de personal técnico responsable; o bien acciones intencionales tales como la comisión de robo o fraude, el acceso no autorizado a la información, la suplantación de identidad, etc.
- del entorno: tales como interrupciones prolongadas de servicios eléctricos o de comunicaciones, fallas por obsolescencia o mal funcionamiento de equipamiento, etc.

Ejemplo: Identificación de vulnerabilidades

ACTIVO	CRITICIDAD	VULNERABILIDAD
Alta de movimientos mensuales	**2**	Inexistencia de copias de respaldo
		Eliminación insegura de la información
		Errores de programación en el sistema
…	…	…

Ejemplo: Identificación de amenazas

ACTIVO	CRITICI-DAD	VULNERABILIDAD	AMENAZA
Alta de movimientos mensuales	**2**	Inexistencia de copias de respaldo	Fallo en el disco rígido Borrado accidental de la información
		Eliminación insegura de la información	Divulgación no autorizada de la información
		Errores de programación en el sistema	Robo de información Fraude electrónico
…	…	...	...

IV. Valoración de amenazas y determinación del impacto

El paso siguiente para la medición del nivel de riesgo es la determinación del impacto adverso como resultado de la ejecución de una amenaza. Este impacto se puede describir en términos de pérdida o degradación de alguna de las tres características básicas: confidencialidad, integridad y disponibilidad.

Para cada activo y amenaza debe estimarse la **degradación**, es decir el porcentaje en que la amenaza daña al activo en estudio estableciendo un valor entre 0 % (no lo daña) y 100 % (lo daña absolutamente) para cada una de las características de confidencialidad, integridad y disponibilidad.

- **Pérdida de Integridad:** Se refiere al requerimiento de que el activo o la información sea protegido contra la modificación no autorizada. Se pierde integridad si se realizan cambios no autorizados en los sistemas o se pierde parte de los datos almacenados sea por un evento accidental o intencionado.

- **Pérdida de Disponibilidad:** El hecho de que la información o un sistema no esté disponible para sus usuarios, ya sea por la pérdida de datos o la destrucción de elementos necesarios, puede afectar a la efectividad operacional y consecuentemente al cumplimiento de la misión de una organización.

- **Pérdida de Confidencialidad:** La confidencialidad hace referencia a la protección de la información contra la divulgación no autorizada. El impacto producido por un evento de estas características, sea en forma no autorizada, intencional o inadvertida, puede variar entre la pérdida de confianza en la institución hasta la posibilidad de acciones legales contra la misma.

Por ejemplo, podría estimarse que tras un incendio controlado, un archivo de legajos se vería afectado un 50 % en su integridad. En el caso de un sistema informático, una falla eléctrica podría afectar en un 100 % la disponibilidad del mismo, sin afectar (0 %) su confidencialidad.

El **impacto** se calcula en base al máximo valor de degradación que la amenaza produce sobre un activo, y la criticidad del activo definida en los pasos anteriores, por ejemplo, mediante la multiplicación de tales valores.

Ejemplo: Valoración de amenazas

AMENAZA	DEGRADACIÓN			IMPACTO (TOTAL)
	CONFID.	INTEG.	DISP.	
Fallo en el disco rígido de la PC	0,00%	40,00%	50,00%	2 x 50% = **1**
Borrado accidental de información	0,00%	100,00%	70,00%	2 x 100% = **2**
…	…	…	…	…

V. Determinación del riesgo

El propósito de este paso es establecer el nivel de **riesgo** que cada amenaza conlleva al sistema. La determinación del riesgo que cada par activo/amenaza resulta como función de:

- la **probabilidad** de que ocurra el evento, es decir, que la amenaza explote la vulnerabilidad, y
- la **magnitud** del impacto que el evento produce sobre el activo en estudio.

El cómputo de la probabilidad suele basarse en los valores históricos de frecuencia con la que ocurre (o podría ocurrir) un evento en forma anual. Por ejemplo, si ocurren fallas eléctricas al menos una vez al mes, la frecuencia de dicha amenaza será 12; si ocurre una inundación cada cuatro años, la frecuencia de dicha amenaza será 1/4. El riesgo al que está expuesto un activo surge de la multiplicación de la frecuencia anual por el impacto estimado en el paso anterior.

Ejemplo: Determinación del riesgo

ACTIVO	AMENAZA	FREC. (ANUAL)	IMPACTO (TOTAL)	RIESGO
Alta de movimientos mensuales	Fallo en el disco rígido de la PC	1	1	1 x 1 = **1**
	Borrado accidental de la información	3	2	3 x 2 = **6**
…	…	…	…	...

VI. Recomendación de controles

La salida del paso anterior constituye un detalle de los riesgos a los cuales el sistema está expuesto, a la vez que brinda un orden de prioridades de los riesgos a tratar: aquellos activos con un alto nivel de riesgo son los que probablemente deberán ser tratados en el corto plazo, buscando la forma de contrarrestar las vulnerabilidades y amenazas; los riesgos de nivel medio también son relevantes pero suelen tratarse a más largo plazo; finalmente los riesgos de bajo nivel suelen aceptarse directamente en los casos donde la implementación de controles implica un mayor coste que el costo de la pérdida producida por el evento adverso.

La recomendación de controles comprende la identificación de medidas adecuadas que mitiguen o eliminen los riesgos encontrados previamente. Un **control** o **salvaguarda** contribuye reduciendo el impacto que produce una amenaza o bien la frecuencia con la que ésta sucede. El objetivo es reducir el nivel de riesgo al que el sistema en estudio está expuesto, llevándolo a un nivel aceptable, y constituye la base inicial para la actividad siguiente de selección e implantación de controles.

A la hora de determinar las recomendaciones de controles y alternativas de solución deben de tenerse en cuenta ciertos factores tales como:

- la efectividad de las opciones recomendadas
- la adecuación a leyes y normas existentes
- el impacto operacional de las modificaciones
- la confiabilidad de tales controles

Por ejemplo, la incorporación de energía a baterías permitiría reducir la frecuencia de los cortes de energía eléctrica a sólo 3 por año; la incorporación de alarmas contra incendios permitiría detectar tal evento en forma temprana reduciendo la degradación que se produzca sobre los activos afectados.

Ejemplo: Recomendación de controles

ACTIVO	VULNERABILIDAD	AMENAZA	SALVAGUARDAS
Alta de movimientos mensuales	Inexistencia de copia de respaldo	Borrado accidental de la información	-Copias de seguridad -Capacitación al usuario -Restricción de permisos
		Fallo en el disco rígido de la PC	-Copias de seguridad -Mantenimiento preventivo
…	…	…	...

Finalmente, la documentación elaborada en el transcurso de esta serie de pasos constituirá un reporte de suma utilidad para la toma de decisiones en lo que respecta a cambios operacionales y administrativos en políticas, procedimientos, presupuestos y de utilización de sistemas informáticos.