UNIVERSIDAD NACIONAL DE SALTA

Facultad de Ciencias Económicas, Jurídicas y Sociales

Cátedra: SISTEMAS DE INFORMACION PARA LA GESTION – GESTION DE TI

Unidad 5: Seguridad en los Sistemas de Información

Contenidos:

Seguridad en los Sistemas de Información: Seguridad, Privacidad e Integralidad: Objetivos de la seguridad en la información Análisis de Riesgos de los sistemas de información. Tecnologías y herramientas para proteger los recursos de información. Medidas de controles generales, de aplicación, y en comunicaciones. Firma Digital. Plan de Contingencia de los sistemas de información. Plan de reanudación de negocios Medidas de recuperación. Aspecto económico de las medidas de seguridad. Estructura de control: Costos Beneficios.

Objetivos específicos:

- Entender las vulnerabilidades de los Sistemas de Información
- Conocer los componentes de un marco de trabajo organizacional para definir la seguridad y el control adecuados
- Conocer las herramientas y tecnologías para salvaguardar los recursos de información y áreas de TI para el aseguramiento de la disponibilidad la información sistemas
- Analizar y avaluar las políticas y procedimientos relativos a la planificación para la atención de contingencias y devolver a la gestión capacidad de respuesta y retorno a la normalidad

Bibliografía Básica:

- Sistemas de información gerencial / Laudon, Kenneth C. (2012) Sistemas de información gerencial [texto impreso] / Laudon, Kenneth C.; Laudon, Jane P.. - 12a. ed.. - México: Pearson Educación, 2012. ISBN 978-607-32-0949-6. Nota de contenido: Cap. 8. Seguridad en los sistemas de información
- Sistemas de información para la gestión empresaria / Lardent, Alberto R. (2001) Sistemas de información para la gestión empresaria : procedimientos, seguridad y auditoría [texto impreso] / Lardent, Alberto R.. - Buenos Aires : Pearson Educación, 2001. . ISBN 987-9460-51-0. Nota de contenido: II: Seguridad y auditoría informática : 19. Seguridad informática 22. Controles de accesos lógicos y físicos - 23. Seguridad en los sistemas de base de datos - 24. Seguridad de redes y sistemas distribuidos 29. Recuperación de desastres. Continuidad de operaciones.

Índice de Contenido

1. Seguridad en Sistemas de Información: Seguridad, Privacidad e Integralidad..... 3
2. Tecnologías y herramientas para proteger recursos de información 5
3. Plan de Contingencia de los sistemas de información 7
4. Aspecto económico de las medidas de seguridad 9

1. Seguridad en Sistemas de Información: Seguridad, Privacidad e Integralidad

Introducción

Actualmente en el mundo empresarial existe un alto grado de dependencia de los sistemas informáticos para poder operar.
La información que circula en esos sistemas informáticos puede encontrarse en forma impresa, en formato electrónico, magnético u óptico, en el conocimiento de las personas, etc.
Esta situación convierte a la información en un activo fundamental de la empresa, que debe ser *protegida* de manera adecuada en la medida de su valor y exposición.
Por ende, esta protección de los sistemas de información también evoluciona conforme a la dinámica de los negocios.
Antes era suficiente instalar un antivirus que se actualizaba mensualmente hoy esa es una medida con un alto riesgo sobre los sistemas de información debiéndose aplicar medidas adicionales conforme a la complejidad del activo a proteger.

Objetivos de la seguridad de la información

Los objetivos que persigue la protección de los sistemas de información básicamente son tres:

- Confidencialidad: la información crítica o sensible debe ser protegida a fin de evitar su uso no autorizado.
- Integridad: se refiere a la exactitud que la información debe tener, así como su validez acorde con las pautas fijadas por la empresa y regulaciones externas.
- Disponibilidad: los recursos y la información, ante su requerimiento, deben estar disponibles en tiempo y forma.

Otra forma de considerar los objetivos de seguridad es diferenciando dos aspectos:

- Mantener la:
    - integridad,
    - operatividad (disponibilidad),
    - confidencialidad y
    - el no repudio (transmisión segura)

      de la información
- Reducir los riesgos que amenazan a la información

Estos objetivos cuidan la información que soporta los procesos y servicios de una empresa.

Definición de la seguridad de la información

La seguridad de la información o protección de los sistemas de información es una disciplina que relaciona a diversas técnicas, aplicaciones y dispositivos encargados de

asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.
A la seguridad de la información le conciernen todos los aspectos vinculados con los datos empleados en la empresa y su protección en todos los procesos en los que se generan o consultan dentro de la empresa.

¿Por qué seguridad de los sistemas de información?

Según normas y estándares vinculados a la seguridad de la información porque permite "asegurar la continuidad del negocio *minimizar los daños* a la organización y *maximizar el retorno* de las inversiones y las oportunidades de negocios". También porque es necesario proteger los tres elementos principales en cualquier sistema informático que son: el **software**, el **hardware** y los **datos.**

Gobierno de seguridad de la información (GSI)

El GSI comprende un marco guía para el desarrollo y administración de un programa integral de seguridad de información alineado a los objetivos del negocio. Comprende un plan de gestión de riesgo, estrategia de seguridad del negocio, plan de seguridad del negocio, políticas y procedimientos.

Plan de gestión de riesgo
Es un documento normativo que describe la metodología y procedimiento para identificar, analizar y tratar los riesgos que pueden afectar los sistemas informáticos y a la información.

Estrategia de seguridad del negocio
La estrategia de seguridad depende del negocio o actividad que se esté desarrollando, no obstante, se pueden considerar los siguientes pasos para su diseño:

1- Crear una política integral de seguridad,

2- Realizar un análisis de riesgos y

3- Aplicar las medidas correspondientes.

Política integral de seguridad: se refiere a establecer el estatus de la información para la empresa, objetivos, importancia de la tecnología de la información para la empresa, recursos con que se cuenta, entre otros.

Análisis de riesgos: consiste en enumerar las amenazas a las cuales está expuesta la información y cuáles son las consecuencias de materializarse esas amenazas.

El riesgo se puede calcular por la fórmula riesgo = probabilidad x pérdida, por ejemplo el riesgo de perder un contrato por robo de información confidencial es igual a la probabilidad de que ocurra el robo multiplicado por la pérdida total en pesos de no

hacer el contrato. El riesgo de fraude en transacciones financieras es igual a la probabilidad de que ocurra el fraude por la pérdida en pesos de que llegara ocurrir ese fraude. Si la probabilidad es muy pequeña el riesgo es menor, pero si la probabilidad es casi uno, el riesgo puede ser casi igual a la pérdida total. Si por otro lado la pérdida es menor, aunque la probabilidad de que ocurra el evento sea muy grande tenemos un riesgo menor. Por ejemplo, la pérdida de una transacción de $500 con una probabilidad muy grande de que ocurra al usar criptografía débil, el riesgo llega a ser menor por lo que depende de la política de seguridad para que este riesgo se asuma.

Medidas de seguridad: una vez planteada la política de seguridad y el análisis de riesgo se deben establecer medidas para que cumpliendo con la política de seguridad las pérdidas sean las menores posibles y que esto se transforme en ganancias, ya sean económicas o de imagen.

Plan de seguridad
Es un documento normativo que describe las medidas de seguridad y controles internos adoptados para minimizar los riesgos a los que están expuestos los Sistemas Informáticos de una empresa.

Políticas y procedimientos
Es el conjunto normativo que abarca lineamientos, directivas, estándares, tareas a seguir vinculadas a la seguridad de la información.

Sistema de seguridad
La seguridad vista como un sistema integral se compone de los siguientes elementos:
Seguridad: prevenir o minimizar los riesgos de ocurrencia de un desastre
Contingencia: operar cuando se produce un desastre hasta salir de la crisis
Continuidad del Negocio: continuar con el negocio luego de la crisis

2. Tecnologías y herramientas para proteger recursos de información

Las tecnologías y herramientas para proteger recursos de información en una empresa deben cubrir los siguientes aspectos:

- Organización y Gestión
- Gestión de Riesgos
- Gestión de Activos de información
- Control de Accesos
- Adquisición, Desarrollo y Mantenimiento de sistemas
- Gestión de operaciones y comunicaciones
- Seguridad física y ambiental
- Seguridad de los recursos humanos
- Continuidad del Negocio
- Monitoreo
- Cumplimiento

La combinación de medidas manuales y automatizadas que salvaguardan los sistemas de información y cuidan que funcionen según las normas internas de una empresa, se denomina controles. Los controles consisten en todos los métodos, políticas y procedimientos de la empresa que cuidan la seguridad de sus activos y fiabilidad de sus registros contables, y el cumplimiento operativo de sus normas internas.

Controles generales: son los que controlan el diseño, la seguridad y el uso de los programas informáticos en toda la empresa. Estos controles se ejercen sobre todas las aplicaciones computarizadas y consisten en una combinación de software de sistemas y procedimientos manuales que crea un entorno de control gerencial.
Controles de seguridad de los datos: aseguran que los archivos no sean objeto de accesos no autorizados, cambios o destrucción.
Controles de aplicación: son controles específicos, distintos para cada aplicación informática.
Controles Administrativos: comprende estándares, reglas, procedimientos y disciplinas formalizados para garantizar que los controles se ejecuten y apliquen adecuadamente.
La segregación de funciones es un principio de control interno que divide responsabilidades y asigna las tareas a las personas de modo que las funciones no se traslapan y se minimice el riesgo de los errores y la manipulación fraudulenta de los activos de la organización.
Controles de comunicaciones: asegura que el intercambio de información no sufra modificaciones o intercepciones indebidas.

Tipos de Controles Generales

- Controles de implementación: auditoria que se hace al proceso de desarrollo de sistemas en diversos puntos, para asegurar que se maneje y controle debidamente.
- Controles de software: controles para cuidar la seguridad y fiabilidad del software.
- Controles de hardware: controles para cuidar la seguridad física y el correcto funcionamiento de software.
- Controles de operaciones informáticas: procedimientos que cuidan que los procedimientos programados se apliquen de forma congruente y correcta al almacenamiento y procesamiento de datos.

Tipos de Controles de Seguridad de los Datos

Controles de entrada: verifican la exactitud e integridad de los datos cuando entran en el sistema.
Totales de control: tipo de control de entrada que requiere contar las transacciones o los campos de cantidades antes del procesamiento para efectuar comparaciones y conciliaciones posteriormente.

Controles de procesamiento: comprende rutinas para comprobar que los datos estén completos y sean exactos durante la actualización.
Controles de salida: asegura que los resultados del procesamiento informático sean correctos, estén completos y se distribuyan debidamente.

Desarrollo de una estructura de control: costos y beneficios
Para determinar cuánto control se debe incorporar en un sistema depende de la importancia de los datos.
- La eficacia de costos de los controles también depende de la eficiencia, complejidad y costos de cada técnica de control.
- El nivel de riesgo si no se controla debidamente una actividad o un proceso especifico.
Para decidir que controles usar, los constructores de sistemas de información deben examinar diversas técnicas de control, las relaciones entre ellas y su eficacia de costos relativa. Una deficiencia de control en un punto podría compensarse con un control estricto en otro. Tal vez no sea costeable incorporar controles estrictos en todos los puntos del ciclo de procesamiento si las aéreas de mayor riesgo están seguras o si hay controles compensadores en otros puntos.

3. Plan de Contingencia de los sistemas de información

Plan de Contingencia de los sistemas de información. Plan de reanudación de negocios Medidas de recuperación.

En el apartado 1 mencionamos que un sistema de seguridad integral comprende un plan de seguridad para prevenir, un plan de contingencia para operar ante la ocurrencia de un desastre y salir del mismo y un plan de continuidad del negocio luego de la crisis.

Es decir que si el entorno de seguridad falla corresponde aplicar como recurso complementario los planes de contingencia y continuidad del negocio. Esto es seguir una serie de pasos cuando un sistema entra en crisis a fin de recuperar (al menos en parte) su capacidad funcional y luego continuar con el negocio.

Plan de Contingencia: Es un documento normativo que describe en forma clara, concisa y completa los riesgos, los actores y sus responsabilidades en caso de eventos adversos.

El plan de contingencia debe ser operable y funcional, acorde a los requerimientos del negocio. Debe evidenciar que se han identificado los eventos que puedan ocasionar interrupciones en los procesos críticos; que se elaborado una evaluación de riesgos para determinar el impacto de distintos eventos, tanto en términos de magnitud de daño como del período de recuperación y la vuelta a la normalidad.
Estas actividades deben llevarse a cabo con la activa participación de los propietarios de los procesos y recursos de negocio. La evaluación debe considerar todos los

procesos de negocio y no se limitará sólo a las instalaciones de procesamiento de la información, sino también a todos los recursos relacionados.
Los resultados de la evaluación deben ser el soporte para la selección de mecanismos alternativos de recuperación y adopción de medidas preventivas para la confección del plan de recuperación y vuelta a la normalidad del procesamiento de datos.

Los contenidos mínimos que debe contener un plan de contingencia son:

1) Procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente. Estos deben incluir disposiciones con respecto a la gestión de vínculos eficaces a establecer con las autoridades públicas pertinentes, por ej.: entes reguladores, policía, bomberos y otras autoridades.
2) Los nombres, direcciones, números de teléfono y "localizadores" actuales del personal clave.
3) Las aplicaciones críticas y su prioridad con respecto a los tiempos de recuperación y regreso a la operación normal.
4) El detalle de los proveedores de servicios involucrados en las acciones de contingencia / emergencia.
5) La información logística de la localización de recursos claves, incluyendo: ubicación de las instalaciones alternativas, de los resguardos de datos, de los sistemas operativos, de las aplicaciones, los archivos de datos, los manuales de operación y documentación de programas / sistemas / usuarios.
6) Los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales a las ubicaciones transitorias alternativas, y para el restablecimiento de los procesos de negocio en los plazos requeridos.
7) La inclusión de los planes de reconstrucción para la recuperación en la ubicación original de todos los sistemas y recursos.
8) Todo otro recurso definido como soporte de los procesos de negocio a recuperar.

Mantenimiento y actualización del plan
El plan debe mantenerse por medio de revisiones y actualizaciones periódicas para garantizar su eficacia permanente. Deben existir procedimientos escritos a fin de asegurar que cambios en los procesos de negocio y en su tecnología relacionada se reflejen en las actualizaciones sobre el plan.

Pruebas del plan
El plan debe ser probado periódicamente. Las pruebas deben permitir asegurar la operatoria integral de todos los sistemas automatizados críticos –de acuerdo con los análisis de riesgo previos-, a efectos de verificar que el plan está actualizado y es eficaz. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente del plan mencionado.

Plan de Continuidad del Negocio (PCN)

Un PCN, se enfoca en sostener las funciones del negocio de una empresa durante y después de una interrupción a los procesos críticos del negocio.
La continuidad es considerada como un proceso que se inicia con la recuperación durante la contingencia, y concluye con la vuelta a la normalidad una vez controladas las causas que generaron dicha contingencia.
Gestionar la Continuidad de Negocio es un proceso integral de gestión que identifica los posibles impactos que amenazan a una empresa y ofrece un marco para proporcionar robustez y disponer de una respuesta efectiva que salvaguarde los intereses de los principales proveedores, clientes y demás partes interesadas, la reputación, la marca y las actividades creadoras de valor.
EL PCN se interrelaciona con una serie de planes complementarios:

- Plan de Comunicaciones de Crisis: documento que contiene los procedimientos internos y externos que las organizaciones deben preparar ante un desastre.
- Plan de Evacuación de Edificio: contiene los procedimientos que deben seguir los ocupantes de una instalación o facilidad en el evento en que una situación se convierta en una amenaza potencial a la salud y seguridad del personal, el ambiente o la propiedad.
- Plan de Contingencia de TI: orientado a ofrecer un método alterno para sistemas de soporte general y para aplicaciones importantes
- Plan de Continuidad de Operaciones: orientado a restaurar las funciones esenciales de una sede de la empresa (ej: una agencia, la fábrica, el almacén de ventas) en una sede alterna y realizar aquellas funciones por un período máximo antes de retornar a las operaciones normales.
- Plan de Recupero de Desastres (DRP): Orientado a responder a eventos importantes, usualmente catastróficos que niegan el acceso normal por un período extendido.

Medidas de recuperación

Back Up de información crítica: copias de seguridad de la información crítica.

Sistema ininterrumpido de energía.

Líneas de comunicación redundantes.

4. Aspecto económico de las medidas de seguridad

El aspecto económico de las medidas de seguridad se refiere a la relación costo/beneficio de implementar controles o medidas de seguridad para proteger un activo de información.

La pregunta a responder es ¿Cuánto y cuándo invertir en medidas de seguridad?

La respuesta consiste en implementar una medida de seguridad cuando el costo sea menor al nivel de riesgo (probabilidad por impacto). De lo contrario la medida es antieconómica.

El control debe tener menos costo que el valor de las pérdidas debido al impacto de la misma si se produce el riesgo.

Ley básica: el costo del control ha de ser menor que el activo que protege.