Desarrollo de Software
8º Semestre

Programa de la unidad didáctica:
Seguridad de la informática

Unidad 3.
Gestión y aplicación de protocolos de seguridad informática

Clave:
15144844

Ciudad de México, febrero de 2026

Universidad Abierta y a Distancia de México

DCEIT

Índice

Unidad 3. Gestión y aplicación de protocolos de seguridad informática

Presentación de la Unidad

En la presente unidad revisarás los conceptos básicos de una gestión de protocolos de seguridad informática, dentro de la cual se tiene como objetivo la supervivencia de la empresa en caso de amenaza por alguna vulnerabilidad.

La gestión o administración de protocolos de seguridad informática son para promover y difundir las medidas de seguridad recomendadas para el manejo estratégico de crisis ante diferentes eventualidades (García, Cervigón y Alegre, 2011).

La seguridad informática es la clave para que toda empresa pueda tener control en su información, y de aquí parte la importancia que tiene la prevención y/o recuperación del sistema en caso de sufrir algún ataque.

Además, conocerás las tendencias de la tecnología en seguridad, pues cabe mencionar que aun con toda la seguridad implementada en la empresa, nunca estará cien por ciento protegida contra todas las amenazas que pudieran existir, pero si es el caso, se minimiza el impacto que éstas puedan generar en la empresa.

Si no se cuenta con un buen control de seguridad es muy posible que al mínimo ataque que se sufra existan pérdidas incontables, hasta causar el cierre de la empresa, sin posibilidad de recuperarse.

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta, y, especialmente, la información contenida o circulante. Para ello existe una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información (García, Cervigón y Alegre, 2011).

Competencia específica

- Evaluar los tipos de amenazas y riesgos en los sistemas informáticos para gestionar la protección de información de acuerdo con las necesidades de la organización o del usuario utilizando la metodología para el desarrollo de proyectos de seguridad informática.

Logros:

Al finalizar la unidad podrás:

- Identificar los mecanismos de seguridad en redes, sistemas operativos y bases de datos.
- Utilizar mecanismos de seguridad en los SI.
- Implementar la metodología de proyectos de seguridad informática.
- Utilizar nuevas tecnologías de seguridad informática.

3. 1. Mecanismos de seguridad en los sistemas informáticos: redes, sistemas operativos, bases de datos

Un sistema informático se conforma por hardware, software y datos; respecto a la seguridad, son los componentes hacia los cuales puede ir dirigido un ataque informático (Sarubbi y Blanqué, 2008). Estos ataques informáticos pueden clasificarse en: interrupción, intercepción, modificación y fabricación. Para revisar en qué consisten, es necesario que consultes el documento *U3. Seguridad en los sistemas informáticos*, mismo que se encuentra en los *Materiales de desarrollo de la Unidad 3*.

Para establecer mecanismos de seguridad en los componentes de un sistema informático, es necesario establecer políticas de seguridad que se sustenten en algunas metodologías fundamentales: prevención, detección y respuesta. Para revisar en qué consisten, es necesario que consultes el documento *U3. Seguridad en los sistemas informáticos*, que se ubica en los *Materiales de desarrollo de la Unidad 3*.

Algunos mecanismos de seguridad en redes, sistemas operativos y bases de datos, los puedes revisar en el documento *U3. Seguridad en los sistemas informáticos*, en los *Materiales de desarrollo de la Unidad 3*.

Para revisar las instrucciones de protección a bases de datos, consulta el sitio de MDSN (2015) *Seguridad de bases de datos*

3.2. Metodología para el desarrollo de proyectos de seguridad informática

Existen diversas metodologías para integrar en el desarrollo de proyectos de seguridad informática. Algunas de ellas se explicarán a continuación.

La metodología del Instituto Internacional de Recuperación de Desastres DRII (por sus siglas en inglés, *Disaster Recovery Institute International*) para el desarrollo del Proyecto de BCP se fundó en 1988 con el nombre de *The Disaster Recovery Institute*, DRII, y proporciona programas de educación y servicios de certificación para profesionales de la planificación de recuperación de desastres (Hiles, 2004, p. 315). Básicamente sigue estas etapas:

1. Inicio y administración del proyecto
2. Evaluación y control del riesgo
3. Análisis de impacto al negocio (BIA)
4. Desarrollo de estrategias de continuidad del negocio
5. Respuesta a la emergencia y estabilización
6. Desarrollo e implementación de planes de continuidad del negocio
7. Programas de concientización y entrenamiento
8. Prueba y mantenimiento de los planes de continuidad del negocio
9. Relaciones públicas y coordinación de la crisis
10. Coordinación con las autoridades públicas

A continuación, se explica cada una de las etapas de la metodología del DRII:

1. Inicio y administración del proyecto

Objetivos:

- Establecer la necesidad de desarrollar e implementar un Plan de Continuidad del Negocio.
- Obtener el soporte directivo.

- Organizar y administrar el proyecto hasta su completa realización y acorde con los límites de tiempo y presupuesto.

Justificaciones para implementar un DRP–BCP

- Sobrevivir a un desastre.
- Cumplir con los *Service Level Agreements* o Acuerdos de nivel de servicios.
- Cumplir con los requerimientos o recomendaciones de auditoría.
- Cumplir con los Requerimientos Legales (Legislaciones de Estados Unidos y de México).
- Reducir los costos de seguros.
- Usar las instalaciones y equipo de respaldo para otros propósitos.
- Promover los objetivos de la cultura corporativa (contar un plan que garantice la disponibilidad de los servicios en un evento de desastre).

Apoyo Directivo. El apoyo de la dirección es clave para el éxito del BCP, pues la aprobación del proyecto de DRP-BCP, por parte de la dirección, es necesaria para fondear tanto el desarrollo del plan como la adquisición de productos y servicios comerciales requeridos por las estrategias del plan.

La emisión de una política o directiva sobre la recuperación y continuidad del negocio facilita la cooperación de todas las partes involucradas en el desarrollo del Proyecto de DRP-BCP, por tanto, el interés de la dirección para desarrollar el DRP-BCP puede surgir de alguna auditoria reciente, de una nueva ley o reglamento, de una institución corporativa, o incluso de una comida del directivo con algún otro empresario que ya tenga implementado un DRP– BCP, etcétera.

Para obtener el apoyo directivo es necesario realizar las siguientes acciones:

- Llevar a cabo un análisis informal de riesgos de desastre.
- Recolectar estadísticas de la industria.
- Investigar historias de casos de desastre.
- Identificar los mandatos legales y regulatorios relevantes.
- Desarrollar la justificación para el proyecto de DRP-BCP.
- Llevar a cabo una sesión ejecutiva de sensibilización de la dirección y de la gerencia.

Para realizar una sesión ejecutiva de sensibilización sobre el Proyecto BCP, es necesario realizar las siguientes acciones:

- Hacer una presentación ejecutiva del proyecto a la dirección para obtener su apoyo.
- Destacar la necesidad de establecer una política de recuperación y continuidad del negocio.
- Determinar el alcance del proyecto.
- Presentar los objetivos del proyecto.
- Identificar candidatos para el comité de dirección.
- Presentar la estructura organizacional del equipo de trabajo requerido para desarrollar el proyecto.
- Solicitar apoyo para integrar el equipo de trabajo.
- Presentar requerimientos y presupuesto preliminares.

De las sesiones ejecutivas se obtienen las políticas de recuperación de negocios, las cuales “establecen los objetivos, principios y planteamiento de la gestión de la continuidad de negocio, qué habrá que producir y cómo, principales funciones y responsabilidades y cómo será dirigida e informada la gestión de la continuidad de negocio.” (Gaspar, 2010, p. 206)

Por ejemplo, una política de continuidad del negocio se identifica cuando la gerencia comparte el interés sobre proporcionar seguridad al personal y poder continuar las operaciones del negocio en caso de desastre y deberá cumplir con los esfuerzos que están siendo emprendidos por la alta dirección en el desarrollo de planes para reaccionar y recuperarse de un desastre.

Comité de dirección. En general cuenta con los siguientes elementos:

- Director general.
- Director de finanzas.
- Director de comercialización.
- Gerente de relaciones públicas.
- Gerentes de las unidades de negocios.
- Gerente de operaciones.

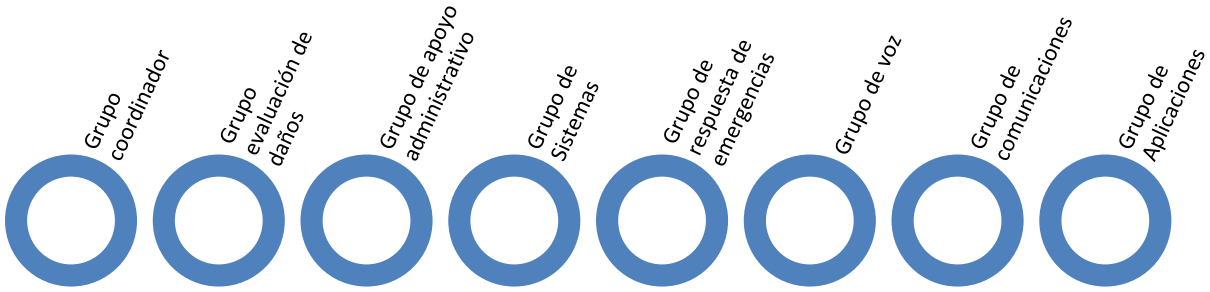
- Gerentes de soporte.
- Gerente de administración del edificio.
- Gerente e IT y comunicaciones.
- Líder del proyecto de continuidad del negocio.

Seleccionar a los integrantes del equipo de trabajo del proyecto:

- Personal gerencial de unidades de negocio.
- Expertos funcionales del negocio.
- Expertos técnicos.
- Personal administrativo y de soporte.

Los miembros del equipo de trabajo del proyecto cubren las siguientes actividades:
Consultores. Los consultores especializados en DRP pueden ser útiles en el desarrollo del proyecto por su experiencia en otros proyectos de DRP en otras empresas y por el conocimiento que tienen sobre los productos y servicios ofrecidos por proveedores de la industria.

Grupos de recuperación–continuidad. Tienen a su cargo identificar a los participantes que intervienen en el proceso de recuperación y continuidad que harán frente a un evento de desastre en forma organizada y controlada.



Grupos de recuperación–continuidad

Preparar y llevar a cabo *Kick–Off Meeting*, establecer el alcance del proyecto:

- Presentar los objetivos del proyecto de desarrollo del DRP-BCP.
    - Objetivos del DRP-BCP.
    - Objetivos generales del proyecto.
    - Objetivos específicos del proyecto.
    - Entregables del proyecto.
- Presentar el plan del proyecto (metodología).
    - Fases y actividades del proyecto.
    - Calendarización de actividades (diagrama de Gantt).
- Presentar la estructura organizacional del equipo de trabajo.
- Asignar tareas y responsabilidades.
- Presentar otros aspectos de coordinación y control del proyecto.
- Distribuir las herramientas de recolección de datos.

Requerimientos presupuestales:

- Costos fijos.
    - Mobiliario, equipo de cómputo, energía eléctrica, gastos telefónicos, renta de oficina, etc.
- Nómina.
    - Idealmente, considerar como tiempo completo al coordinador del proyecto y a su asistente o secretario. En tiempo parcial, los miembros del equipo de trabajo que serán prestados por otros departamentos.
- Viáticos y gastos de viaje.
- Honorarios de consultores.
- Suministros, accesorios y consumibles.
- Otros gastos imprevistos.

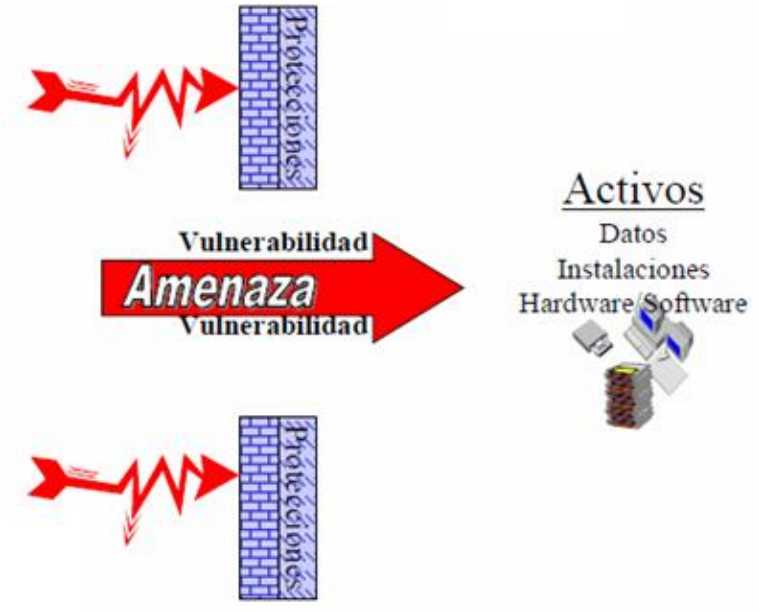
Para consultar los elementos software y hardware que se exponen en un BCP, consulta el documento *U3. Elementos de software y hardware y software para BCP* en los *Materiales de desarrollo de la unidad 3.*

2. Evaluación y control del riesgo

Objetivos:

- Determinar los eventos y circunstancias del ambiente (interrupciones y desastres) que pueden afectar adversamente a la organización y sus instalaciones.
- Determinar el daño que tales eventos pueden causar.
- Determinar los controles necesarios para prevenir o minimizar los efectos de pérdidas potenciales
- Proveer el análisis costo-beneficio para justificar la inversión en controles para mitigar los riesgos

Es riesgo se concibe como el potencial de daño o pérdida que existe como resultado del aparejamiento entre amenaza y vulnerabilidad. “Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye un riego una amenaza cuando no hay vulnerabilidad, ni una vulnerabilidad cuando no existe amenaza para la misma.” (Aguilera, 2010. p. 14)



Las protecciones previenen las amenazas de los activos vulnerables, de no existir una protección adecuada, la vulnerabilidad puede ser aprovechada por una amenaza y los activos estarían en riesgo (Guttman & Roback, 1995, p.62) https://archive.org/stream/introductiontoco80012gutt#page/62/mode/2up/search/vulnerability

3. Análisis de impacto al negocio (BIA)

A: Identificar los impactos que resultan de la interrupciones y escenarios de desastre que pueden afectar a la organización.

B: Identificar las técnicas que pueden ser usadas para cuantificar y calificar tales impactos.

C: Determinar las funciones críticas, sus prioridades de recuperación y sus interdependencias, de tal manera que se pueda establecer el Tiempo Objetivo de Recuperación (RTO = *Recovery Time Objective*).

El BIA analiza el impacto financiero y operacional de desastres sobre las áreas de negocio y los procesos de una organización.

El impacto financiero se refiere a las pérdidas monetarias tales como; ventas perdidas, inversiones perdidas, multas, penas o sanciones contractuales, etc.

El impacto operacional representa las pérdidas no monetarias relacionadas con las operaciones del negocio, y pueden incluir: pérdida de ventaja competitiva, daño a la confianza de los inversionistas, mal servicio a clientes, bajo estado de ánimo (moral) del personal y daño a la reputación de la empresa.

El proceso de desarrollo del BIA implica los siguientes pasos:

- Definir objetivos, alcance y suposiciones del BIA.
- Identificar las funciones del negocio y sus procesos.
- Evaluar los impactos financieros y operacionales.
- Identificar los procesos críticos.
- Evaluar los MTD y priorizar los procesos críticos.
- Identificar los sistemas y aplicaciones informáticas críticas.
- Identificar los recursos no-informáticos que son críticos.
- Determinar el RTO.
- Determinar el PRO.
- Identificar los procedimientos alternativos.
- Generar reporte BIA.

4. Desarrollo de estrategias de continuidad del negocio. Consiste en determinar y guiar la selección de estrategias funcionales alternativas para recuperar el negocio y el servicio informático dentro del tiempo objetivo de recuperación (RTO), al tiempo que se establecen las funciones críticas de la organización.
Las estrategias articuladas para la recuperación de los sistemas y de los usuarios finales no tendrían éxito si no se hacen previsiones para recuperar las redes que enlazan los sistemas con los usuarios, o los sistemas y usuarios a entidades externas, incluyendo clientes, agencias de gobierno, instituciones financieras, etc.

Sin la recuperación de las instalaciones de red que son claves, el DRP no puede tener éxito.

5. Respuesta a la emergencia y estabilización
Objetivos:

- Desarrollar e implementar procedimientos para responder y estabilizar la situación inmediata siguiente a un incidente o evento.
- Establecer y administrar un centro de operaciones de emergencia para ser usado como un centro de mando durante la emergencia.

6. Desarrollo e implementación de planes de continuidad del negocio
Objetivo:

- Diseñar, desarrollar e implementar el BCP que provea la recuperación dentro del Tiempo Objetivo de Recuperación (RTO).

7. Programas de concientización y entrenamiento
Objetivos:

- Preparar un programa para crear conciencia corporativa.
- Preparar un programa para mejorar las habilidades requeridas para desarrollar, implementar, mantener y llevar a cabo el BCP.

8. Prueba y mantenimiento de los planes de continuidad del negocio

Objetivos:

- Pre-planear y coordinar las pruebas del BCP.
- Evaluar y documentar los resultados de las pruebas.
- Desarrollar procesos para mantener la vigencia de capacidades para mantener la continuidad y la vigencia del documento del plan de acuerdo con la dirección estratégica de la organización.
- Verificar la efectividad del plan comparándolo con un estándar adecuado.
- Reportar los resultados de manera clara y concisa.

9. Relaciones públicas y coordinación de la crisis

Objetivos:

- Desarrollar, coordinar, evaluar, y ejercitar planes para manejar a los medios de comunicación durante las situaciones de crisis.
- Desarrollar, coordinar, evaluar, y ejercitar planes para comunicar y, según sea necesario, proveer asesoramiento sobre el manejo de traumas, a los empleados, sus familiares, clientes clave, proveedores críticos, dueños/accionistas de la empresa, y a la gerencia corporativa durante la crisis.
- Asegurar que a todos los *stakeholders* se les mantenga informados según sea necesario.

10. Coordinación con las autoridades públicas

- Establecer las políticas y procedimientos aplicables para coordinar las actividades de respuesta, continuidad y restauración, con las autoridades respectivas, de manera que se cumpla con los estatutos y reglamentos aplicables.

3.2.1. Plan de continuidad de negocio (BCP)

Un plan de continuidad de negocio (o BCP por sus siglas en inglés) es un plan de emergencia, el cual tiene como objetivo el mantener la funcionalidad de la organización a un nivel mínimo aceptable durante una contingencia. Este plan debe de contemplar todas las medidas preventivas para cuando se produzca una contingencia que afecte al negocio; es un conjunto de procedimientos y estrategias definidos para asegurar la

reanudación oportuna y ordenada de los procesos de negocio generando un impacto mínimo ante un incidente (Gaspar, 2008).

El contar con un BCP es recomendable, independientemente del tamaño y giro de nuestra empresa, ya que éste nos va a ayudar a mitigar el impacto que pudiera presentarse en caso de un desastre. Asimismo, el BCP ayuda a mantenerse en el negocio, identificando los impactos potenciales que amenazan la organización, logrando así establecer un plan que permita continuar con la actividad de nuestra empresa en caso de una interrupción.

Algunos beneficios de contar con un plan de continuidad de negocio, se enlistan a continuación:

- Identifica los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto sobre el negocio.
- Obliga a conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.
- Previene o minimiza las pérdidas para el negocio en caso de desastre.
- Clasifica los activos para priorizar su protección en caso de desastre.
- Aporta una ventaja competitiva frente a la competencia.

Debes recordar que el objetivo final es mantener el negocio, por lo que se deberán priorizar las operaciones de negocio críticas necesarias para continuar en funcionamiento después de un incidente no planificado.

Consulta el documento *U3. Plan BCP* en los *Materiales de desarrollo de la unidad 3* donde encontrarás un ejemplo de formato BCP donde puedes apoyarte para elaborar tus propios planes BCP.

3.2.2. Plan de recuperación de desastre (DRP)

El Plan de recuperación de desastres es un conjunto de estrategias definidas para asegurar la reanudación oportuna y ordenada de los servicios informáticos críticos en caso de contingencia. Su método de gestión depende de varios departamentos de una

empresa y de diferentes fases: analizar, desarrollar, ejecutar y mantener (Chapman, 2006).

Lo primero que se debe realizar es un análisis de impacto al negocio (BIA). Éste es básicamente un informe que nos muestra el coste ocasionado por la interrupción de los procesos de negocio que se incluye en el Plan de continuidad de negocio (BCP). Con este informe la compañía tiene la capacidad de clasificar los procesos de negocio en función de su criticidad, y lo que es más importante: establecer la prioridad de recuperación (o su orden secuencial).

Hay tres aspectos de primordial importancia para el análisis, los cuales se exponen a continuación:

- Criticidad de los recursos de información relacionados con los procesos críticos del negocio.
- Periodo de recuperación crítico antes de incurrir en pérdidas significativas.
- Sistema de clasificación de riesgos.

Un DRP no se puede lograr sin personal dedicado, de tiempo completo, con la responsabilidad de mantener los planes, la coordinación de los componentes y las pruebas. Debe estar capacitado para asumir responsabilidades de recuperación y actualización de los planes, para reflejar los cambios en el procesamiento de la información y entornos empresariales. Mayoritariamente el personal implicado en el desarrollo de un DRP es el del departamento de sistemas de información y del equipo de soporte técnico.

Hay grandes beneficios que se pueden obtener a partir de la elaboración de un plan de recuperación de desastres, algunos de éstos son:

- La capacidad de proteger los sistemas críticos para la empresa.
- Reducción de pérdidas tras un incidente.
- Garantizar la fiabilidad de los sistemas de reserva.
- Proporcionar un sentido de seguridad.
- Minimizar el riesgo de retrasos.
- Proporcionar un estándar para probar el plan.

- Minimizar la toma de decisiones en caso de desastre.
- La reducción de las posibles responsabilidades legales.
- Mejora de la eficiencia general de la organización y la identificación de la relación de bienes y recursos humanos y financieros para los servicios críticos.

Todas las organizaciones están en riesgo de padecer cualquier desastre que haga perder los activos correspondientes a la información de su negocio. Un plan de recuperación es una herramienta que permite a las empresas no perder información crítica y seguir ofreciendo servicios a pesar de una interrupción.

Consulta el documento *U3. Formato de plan DRP* en los *Materiales de desarrollo de la unidad 3* donde encontrarás un ejemplo de formato DRP donde puedes apoyarte para elaborar tus propios planes de recuperación de desastres.

3.3. Nuevas tecnologías de seguridad de la informática

La implementación y desarrollo de nuevas tecnologías de seguridad son de vital importancia, ya que con ellas se puede evaluar y consultar el constante avance tecnológico, con el fin de mantener actualizados los equipos y sistemas de seguridad instalados en nuestra empresa, pero siempre es necesario realizar un análisis de costo–beneficio frente a la necesidad y requerimiento real. A continuación, se explicará lo relacionado con las nuevas tecnologías con base en Castellanos (2012). Las políticas de control y mantenimiento deben estar en un constante rediseño, ya que debe de ir a la par del crecimiento de nuestra empresa y de la estrategia comercial en la que se basa.
Con nuevas tecnologías vienen nuevas amenazas, y los hackers parecen estar desarrollando sus armas a una velocidad que está complicando a las empresas de seguridad, por lo cual es importante abordar los elementos técnicos y procedimentales de la seguridad, con base en las nuevas tecnologías, de modo que se reduzcan las vulnerabilidades. Algunas de ellas no son nuevas, sin embargo es importante considerarlas para respaldar la seguridad.

Seguridad física

Para tener una seguridad en los equipos, se debe definir, en el manual de operaciones del personal, los procedimientos para evitar malos manejos en la operación del equipo que puedan crear riesgo de negligencia o accidente.

Para asegurar los programas, es necesario restringir el acceso a programas y archivos, aplicar medidas antivirus, asegurar que los operadores puedan trabajar sin una supervisión rigurosa, y necesiten autorización para modificar programas y archivos, así como asegurar que se usen los datos, archivos y programas correctos.

Para manejar una protección contra acceso no autorizado y/o interferencia electrónica, se deben implantar medidas para evitar que personas no autorizadas ingresen remotamente a los sistemas (“hackers”). Se recomienda el uso de criptografía para el envío de información.

La protección de la identidad y autenticación se logra identificando a los usuarios, obligándolos a cambiar de clave con frecuencia, a usar criptografía en claves de acceso, emitir tarjetas de acceso y utilización de aparatos biométricos para resguardo de la información.

Existen diversos factores que pueden afectar la seguridad de un sistema de información:

- Manejo pobre de módems.
- Transmisión de archivos no criptografiados.
- Indiferencia ante la seguridad.
- Temor ante los costos de seguridad.
- No usar la criptografía.
- Claves de acceso débiles y obvias.
- No validar/verificar a los usuarios.
- No inspeccionar el software nuevo.
- No realizar procedimientos antivirus.
- Empleados descontentos o deshonestos.
- Errores de programación.

- Aplicaciones no autorizadas.
- No tener controles de auditoría.

Revisa los conceptos base de la gestión de la Seguridad informática, las políticas, planes de recuperación y continuidad.
USERS (2013). Gestión de la Seguridad Informática. RedUSers, P.P. 36 – 90

Seguridad de la aplicación

Para cubrir la protección de aplicación informática, se debe tener una comunicación entre el personal de computación y los usuarios; es decir, debe existir una unidad o encargado de canalizar todas las solicitudes de los usuarios referentes a quejas, solicitudes, modificación de programas, y otros servicios.El control de usuario se debe de llevar a cabo bajo la responsabilidad del mismo en asegurar que los datos recolectados estén completos y sean precisos, y una vez ingresados, se debe asegurar que los datos sean procesados e incluidos en los archivos correspondientes.

Para garantizar la seguridad de los archivos, se debe tener el almacenamiento de las copias de respaldo en un ligar distante, identificación y control de los archivos a través de etiquetas u otros medios, acceso físico restringido, y por último, realizar una revisión regular de los controles de aplicación, a través de la unidad de auditoría o contraloría interna, y de la auditoría de sistemas.

Seguridad en caso de contingencias

La seguridad siempre es el pilar de cualquier empresa, por lo cual se debe tener siempre la certeza de que, en caso de desastre, se tiene un respaldo informático, el cual nos va a permitir la continuidad del negocio. En ello radica la importancia de esta unidad, ya que todo va ligado a la seguridad y continuidad del negocio.

No existe la posibilidad de decir: con esto estás 100% seguro, porque esto evoluciona día a día, hay nuevo software y nuevas dinámicas con las que un hacker podría atacar a la empresa. Las empresas deben hacer una relación costo/beneficio y analizar con detalle qué desean proteger, analizar los riesgos potenciales y, desde ahí, ver un plan de trabajo

que incluya un presupuesto de trabajo. No tiene sentido si la protección me está costando más cara que lo que quiero proteger.

Para conocer las novedades en mecanismos, software y hardware de seguridad en los sistemas informáticos, investiga en diversas fuentes a tu alcance, en revistas especializadas, así como en sitios confiables, por ejemplo, Seguridad .NET, en los boletines de universidades e institutos nacionales o extranjeros que se dediquen a la investigación en el área informática, como el sitio de la UNAM-CERT, o la página del IPN Seguridad Informática.

Cierre de la Unidad

Es importante reconocer que no se está en su totalidad exento de sufrir algún tipo de desastre, dentro y fuera de la institución en la que se esté laborando, pues, aunque se cuente con un sistema de gestión de seguridad muy completo, es importante tener en cuenta que no hay seguridad contra todo, pues todos los sistemas de información suelen tener alguna vulnerabilidad, pero, el implementar herramientas, protocolos y mecanismos de seguridad en los sistemas de información, minimiza y en la medida de lo posible, evitar pérdidas o daños que se pudieran presentar.
Existen metodologías mediante las cuales es posible planear e implementar seguridad informática, pero siempre se debe resguardar la confidencialidad, la integridad y la disponibilidad de la información, ya que son la base de cualquier sistema informático en toda organización.

Para saber más

Es recomendable visitar el siguiente sitio, donde encontrarás información sobre la planificación y preparación de un desastre, desde alertas, mejora de diseño de programas, análisis de la vulnerabilidad y de la capacidad de respuesta que se tiene frente a un desastre

http://www.ifrc.org/en/what-we-do/disaster-management/preparing-for-disaster/disaster-preparedness-tools/contingency-planning-and-disaster-response-planning/

Es una página en inglés, pero puedes utilizar diversos traductores que hay en internet en caso de que no domines este idioma. Es importante que trates de leer documentos en inglés, pues existe gran cantidad de literatura respecto a la seguridad informática y respecto al desarrollo de software en este lenguaje.

Para revisar algunas recomendaciones sobre la protección de bases de datos, consulta el siguiente sitio:
http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/6/bases_datos.pdf

Para analizar la seguridad de la familia de protocolos TCP/IP y sus servicios asociados, consulta el siguiente sitio:
https://www.rediris.es/cert/doc/segtcpip/Seguridad_en_TCP-IP_Ed1.pdf

Fuentes de consulta

Básica

- Andreu, F., Pellejero, I. Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN*. Barcelona: Marcombo. pp. 32-33, 35-40.
- Aguilera, P. (2010). *Seguridad informática.* Madrid: Editex.

- Castellanos, H. L.R. (2012). S*eguridad en Informática: Seguridad, Auditoría, Cortafuegos, Ingeniería Social, ISO 27000. Maracaibo:* Editorial Académica Española, Ingenieria Social, ISO 27000.
- Chapman, J. (2006). *Plan de Recuperación de negocios*. *En una semana*. Barcelona: Gestión 2000-Planeta DeAgostini Profesional y Formación, S. L.
- Fisher, R. P. (1998). *Seguridad en los sistemas informáticos.* Madrid: Díaz de Santos D.L. p. 228, 230-233.
- García, A., Cervigón H., y Alegre Ramos, M. P. (2011). *Seguridad Informática*. 1ª Ed. Madrid: Ediciones Paraninfo, S. A.
- Gaspar Martínez, J. (2010). *El plan de continuidad de negocio. Guía práctica para su elaboración*. Madrid: Díaz de Santos.
- Gaspar Martínez, J. (2010). *Planes de Contingencia – La continuidad del negocio en las organizaciones*. Madrid: Ediciones Días de Santos, S. A. Albasanz.
- Gutiérrez, J., y Tena, J. (2003). *Protocolos criptográficos y seguridad en redes*. Santander: Universidad de Cantabria. pp. 129-132.
- Guttman, B., Roback, E.A. (1995). *An Introduction to Computer Security: The NIST Handbook*. Gaithersburg, MD; Washington, D.C:Computer Systems Laboratory. National Institute of Standards and Technology
- Hiles, A. (2004). *Business continuity: Best practices. World-Class Business Continuity Management.* 2a Ed. Connecticut-Oxford: BCI-DRI.
- ISO/IEC 27031 (2011). *Tecnología de información-Técnicas de seguridad - Guías para preparación de tecnologías de información y comunicaciones para continuidad de negocios.* 1ª Ed. Ecuador: ISO IEC.
- ISO/IEC 24762 (2008). *Directrices para los servicios de recuperación de desastres de las tecnologías de información y comunicaciones.* 1a Ed. Ecuador: ISO-IEC.
- MSDN Microsoft Developer Network (2022). *Seguridad de bases de datos*. https://msdn.microsoft.com/es-es/library/cc434708%28v=vs.71%29.aspx
- Wellheiser, J. (2002). *An Ounce of Prevention: Integrated Disaster Planning for Archives, Libraries, and Record Centres*. 2nd edition. Toronto: Scarecrow Press, Inc. and Canadian Archives Foundation.