



SERVICIO NACIONAL DE APRENDIZAJE
SISTEMA INTEGRADO DE GESTIÓN
Procedimiento Creación y Adecuación de Programas de
Formación Virtual y a Distancia
Guía de Aprendizaje para el Programa de Formación
Complementaria Virtual

Versión: 01
Fecha: 08-10-2013
Código: G001-
P002-GFPI

GUÍA DE APRENDIZAJE Nº 2

1. IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE:

Programa de Formación: Gestión de la seguridad informática	Código: 21720170 Versión: 2
Resultados de Aprendizaje: Reconocer las amenazas informáticas de la empresa, identificando la infraestructura tecnológica, organizacional y humana acorde con estándares de seguridad nacional e internacional	Competencia: Diagnosticar el nivel de seguridad de la información de acuerdo a las políticas de la organización
Duración de la guía (en horas):	10 horas

2. INTRODUCCIÓN

Bienvenido a la actividad de aprendizaje 2 del programa de formación *Gestión de la Seguridad Informática*

La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada. La información puede existir en diversas formas.

Cualquiera sea su forma o medio por el cual se comparte o almacena, siempre debería tener protección adecuada. La seguridad informática es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades de negocio (vistos en la semana 1).

Con la gestión de la seguridad en la información se deben alcanzar objetivos que permitan minimizar los riesgos, detectar los posibles problemas y las amenazas internas y externas a la seguridad.

La actividad preliminar para el desarrollo de esta guía de aprendizaje, requiere de la revisión detenida del material del programa de formación del RAP 2 “*SEGURIDAD INFORMÁTICA*”, del apoyo de documentos anexos, de la exploración de los enlaces externos y de las respectivas consultas en Internet.



3. ESTRUCTURACION DIDACTICA DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividades de Reflexión inicial.

Uno de los principales aspectos de esta actividad de aprendizaje, es la de Identificar los elementos vulnerables en el sistema de información, en el cual se deben tener en cuenta las amenazas internas y externas en la organización, con las cuales estamos expuestos a vulnerabilidades y riesgos. Reflexione sobre las siguientes preguntas:

- *¿Cómo se puede presentar un abuso de un empleado de un banco que tiene privilegios excesivos sobre las bases de datos (amenaza interna)?*
- *¿Cómo podríamos disminuir los riesgos o vulnerabilidades de nuestro negocio ante la presencia de hackers (amenaza externa)?*

Nota: esta actividad tiene como finalidad encaminarlo y motivarlo en el desarrollo de los temas de esta guía de aprendizaje, por tal motivo no es calificable.

3.2 Actividades de contextualización e identificación de conocimientos necesarios para el aprendizaje

Foro: Seguridad en redes

En esta semana se introdujo al conocimiento de la seguridad en las redes. Las intrusiones de personas no autorizadas en la red (interna o externa) causan interrupciones costosas y pérdidas de trabajo, las cuales generan amenazas de seguridad con diferentes riesgos.

Analice el ítem “Seguridad en redes” del objeto de aprendizaje (OA) “Seguridad informática”, el cual se encuentra en la ruta:

- *Opción del menú del curso “Materiales del programa”*
- *Subcarpeta Materiales de formación*
- *Subcarpeta Materiales Actividad de aprendizaje 2*

Y participe en el Foro “**Seguridad en redes**”, argumentando y debatiendo sus respuestas, a las siguientes preguntas orientadoras:

1. *¿Cuál cree usted son los delitos que ocurren con mayor frecuencia en la red interna o externa de la organización?*



2. *¿Cuál considera usted la posible solución o minimización de los riesgos de la seguridad en la red?*

Recuerde que debe retroalimentar la participación de mínimo dos compañeros con ideas suficientemente soportadas.

Este foro estará disponible en la opción del menú del curso Actividades, en la ruta:

- Carpeta *Actividad de aprendizaje 2: Identificar los elementos vulnerables en el sistema de información teniendo en cuenta las amenazas internas y externas en la organización*
 - Subcarpeta Evidencias *Actividad de Aprendizaje 2*
 - Enlace Foro: *“Seguridad en redes”*

3.3 Actividades de apropiación del conocimiento (Conceptualización y Teorización)

Cuestionario: Seguridad informática

Los conocimientos adquiridos mediante el seguimiento y aplicación de esta guía resultan claves para reconocer los conceptos básicos sobre seguridad informática. Le invitamos a avanzar en este proceso, teniendo en cuenta los requerimientos para el alcance de las competencias que propone el programa de formación “Gestión de la Seguridad Informática”.

El desarrollo del resultado de aprendizaje *“Identificar los elementos vulnerables en el sistema de información teniendo en cuenta las amenazas internas y externas en la organización”*, hace necesario que usted como aprendiz apropie conocimientos basados en los siguientes conceptos:

- DEFINICIÓN DE LA SEGURIDAD INFORMÁTICA
- OBJETIVOS DE LA SEGURIDAD INFORMÁTICA
- SERVICIOS DE SEGURIDAD EN LA INFORMACIÓN
- TÉCNICAS Y MECANISMOS DE SEGURIDAD
- ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO
 - ✓ Amenazas lógicas
 - ✓ Amenazas físicas
 - ✓ Personas que pueden constituir riesgos
- SEGURIDAD EN REDES
 - ✓ Amenazas externas



SERVICIO NACIONAL DE APRENDIZAJE
SISTEMA INTEGRADO DE GESTIÓN
Procedimiento Creación y Adecuación de Programas de
Formación Virtual y a Distancia
Guía de Aprendizaje para el Programa de Formación
Complementaria Virtual

Versión: 01
Fecha: 08-10-2013
Código: G001-
P002-GFPI

- ✓ Amenazas internas
- ✓ Algunos tipos de ataques informáticos en redes
- **CONSECUENCIAS DE LA FALTA DE SEGURIDAD**

En el Ambiente Virtual de Aprendizaje dispuesto en el Sistema de Gestión de Aprendizaje (LMS), se encuentra el objeto de aprendizaje (OA) “Seguridad informática”, que debe leer, comprender y asimilar, toda vez que en él encontrará la información que le permitirá analizar la conceptualización técnica del presente tema de estudio.

El cuestionario estará disponible en la opción del menú del curso Actividades, en la ruta:

- Carpeta *Actividad de aprendizaje 2: Identificar los elementos vulnerables en el sistema de información teniendo en cuenta las amenazas internas y externas en la organización*
- Subcarpeta *Evidencias Actividad de Aprendizaje 2*
- Enlace *Cuestionario: “Seguridad informática”*

3.4 Actividades de transferencia del conocimiento.

Informe: Amenazas a las bases de datos

Las bases de datos son el “corazón” del negocio. Es el activo más importante: Almacenan registros de los clientes de la empresa y datos financieros confidenciales. Por lo tanto, constituyen uno de los objetivos más codiciados para los hackers o para cualquier intruso.

¿Por qué son tan vulnerables las bases de datos? Las empresas no invierten en la protección de éstas. Los piratas informáticos acceden a datos sensibles y pueden extraer valores, causar daños o afectar las operaciones comerciales causando pérdidas financieras.

En el año 2015, la OTA (Online Trust Alliance) menciona que más del 97% de estos ataques podrían haberse evitado si se aplicaban medidas simples, siguiendo “mejores prácticas” y controles internos.

La OTA menciona un top 10 de principales amenazas a las bases de datos (ver la siguiente tabla):

Ranking	Amenaza
1	Privilegios excesivos y privilegios no utilizados
2	Abuso de privilegios legítimos



SERVICIO NACIONAL DE APRENDIZAJE
SISTEMA INTEGRADO DE GESTIÓN
Procedimiento Creación y Adecuación de Programas de
Formación Virtual y a Distancia
Guía de Aprendizaje para el Programa de Formación
Complementaria Virtual

Versión: 01
Fecha: 08-10-2013
Código: G001-
P002-GFPI

3	Inyección SQL
4	Malware
5	Proceso de auditoría débil
6	Exposición de los medios de almacenamiento
7	Explotación de vulnerabilidades y bases de datos mal configuradas
8	Datos sensibles no administrados
9	Negación o denegación de servicios
10	Educación y experiencia limitada en seguridad

Usted como representante de la organización, debe dar a conocer al menos dos de las amenazas que se muestran en la tabla y sus posibles controles o la disminución de estos riesgos. Para ello, realice lo siguiente:

1. Analice el objeto de aprendizaje (OA) "Seguridad informática", el cual se encuentra en la ruta:
 - Opción del menú del curso "Materiales del programa"
 - Subcarpeta Materiales de formación
 - Subcarpeta Materiales Actividad de aprendizaje 2
2. Consulte por diferentes medios la definición o la descripción de las amenazas que se muestran en la tabla y que usted previamente escogió.
3. Una vez termine de leer debe entregar como evidencia lo siguiente:
 - Elabore un documento en Word donde defina cada una de las amenazas que seleccionó.
 - ¿Cómo le daría solución a estas amenazas? ¿Qué controles implementaría para disminuir los riesgos ocasionados por las posibles amenazas? Puede apoyarse con imágenes para justificar su respuesta.
 - Debe tener presente las normas Icontec en su última versión para la elaboración de documentos escritos.
 - Guarde el documento final y envíelo dentro del plazo señalado por su instructor, a través de la opción del menú del curso Actividades, en la ruta:
 - Carpeta *Actividad de aprendizaje 2: Identificar los elementos vulnerables en el sistema de información teniendo en cuenta las amenazas internas y externas en la organización*
 - Subcarpeta *Evidencias Actividad de Aprendizaje 2*
 - Enlace *Informe: "Amenazas a las bases de datos"*



SERVICIO NACIONAL DE APRENDIZAJE
SISTEMA INTEGRADO DE GESTIÓN
Procedimiento Creación y Adecuación de Programas de
Formación Virtual y a Distancia
Guía de Aprendizaje para el Programa de Formación
Complementaria Virtual

Versión: 01
Fecha: 08-10-2013
Código: G001-
P002-GFPI

- **Nota:** Si al momento de enviar el archivo (Actividad), el sistema genera el error: "Archivo inválido", debe tener en cuenta que este error se debe a que:

En el momento que está adjuntando el archivo, lo tiene abierto. Círralo y pruebe nuevamente adjuntándolo en "Adjuntar archivo", "Examinar mi equipo".

3.5 Actividades de evaluación.

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
De conocimiento : Cuestionario: Seguridad informática	Diagnostica los tipos de riesgos en la organización para establecer la seguridad informática acorde a los estándares de seguridad nacional e internacional. Identifica las amenazas de seguridad de la información en la organización teniendo en cuenta los estándares de seguridad nacional e internacional.	Enlace en LMS – Prueba de Conocimiento.
De desempeño: Foro: Seguridad en redes	Diagnostica los tipos de riesgos en la organización para establecer la seguridad informática acorde a los estándares de seguridad nacional e internacional. Identifica las amenazas de seguridad de la información en la organización teniendo en cuenta los estándares de seguridad nacional e internacional.	Enlace en LMS – Foro de discusión.



SERVICIO NACIONAL DE APRENDIZAJE
SISTEMA INTEGRADO DE GESTIÓN
Procedimiento Creación y Adecuación de Programas de
Formación Virtual y a Distancia
Guía de Aprendizaje para el Programa de Formación
Complementaria Virtual

Versión: 01
Fecha: 08-10-2013
Código: G001-
P002-GFPI

	internacional.	
De producto: Informe: Amenazas a las bases de datos.	Diagnostica los tipos de riegos en la organización para establecer la seguridad informática acorde a los estándares de seguridad nacional e internacional. Identifica las amenazas de seguridad de la información en la organización teniendo en cuenta los estándares de seguridad nacional e internacional.	Enlace en LMS – Actividad informe escrito.

4. RECURSOS PARA EL APRENDIZAJE

Ambiente requerido:

Ambiente de navegación (computador y conexión a Internet).

Material requerido:

- Material descargable de la actividad de aprendizaje 2
- Documentos de apoyo de la semana 2
- Material interactivo de la actividad de aprendizaje 2:
 - Seguridad informática

5. GLOSARIO DE TÉRMINOS



SERVICIO NACIONAL DE APRENDIZAJE
SISTEMA INTEGRADO DE GESTIÓN
Procedimiento Creación y Adecuación de Programas de
Formación Virtual y a Distancia
Guía de Aprendizaje para el Programa de Formación
Complementaria Virtual

Versión: 01
Fecha: 08-10-2013
Código: G001-
P002-GFPI

COMPUTADOR: También denominado ordenador (del francés *ordinateur*, y este del latín *ordinator*), es una máquina electrónica que recibe y procesa datos para convertirlos en información útil.

DATOS: Es un valor o referente que recibe el computador por diferentes medios, los datos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo.

HARDWARE: Refiere a todas las partes tangibles de un sistema informático sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado; contrariamente, el soporte lógico es intangible y es llamado software.

INFORMÁTICA: Ciencia que estudia métodos, procesos, técnicas, con el fin de almacenar, procesar y transmitir información y datos en formato digital

INTERNET: Red de redes compartiendo información entre sí.

MODELO: Esquema teórico, generalmente en forma matemática, de un sistema o de una realidad compleja, como la evolución económica de un país, que se elabora para facilitar su comprensión y el estudio de su comportamiento.

NEGOCIO: Sistema, método o forma de obtener dinero, a cambio de ofrecer productos, bienes o servicios a otras personas.

ORGANIZACIÓN: Son estructuras sociales diseñadas para lograr metas o leyes por medio de los organismos humanos o de la gestión del talento humano y de otro tipo.

RED: Conjunto de operaciones centralizadas o distribuidas, con el fin de compartir recursos "Hardware y software"

RED INFORMÁTICA: Sistema formado por dos o más ordenadores interconectados entre sí, a través de tarjetas de red con transmisión por cable o de forma inalámbrica, para compartir ficheros, recursos, aplicaciones, conexión a internet etc.



SERVICIO NACIONAL DE APRENDIZAJE
SISTEMA INTEGRADO DE GESTIÓN
Procedimiento Creación y Adecuación de Programas de
Formación Virtual y a Distancia
Guía de Aprendizaje para el Programa de Formación
Complementaria Virtual

Versión: 01
Fecha: 08-10-2013
Código: G001-
P002-GFPI

RIESGO: Es la vulnerabilidad, un posible potencial de perjuicio o daño para las unidades o personas, organizaciones o entidades.

SEGURIDAD: Proviene de la palabra *securitas* del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien

SISTEMA INFORMÁTICO: Se compone de una unidad central de procesamiento (CP/CPU), encargada de procesar los datos, uno o varios periféricos de entrada, los que permiten el ingreso de la información y uno o varios periféricos de salida, los que posibilitan dar salida (normalmente en forma visual o auditiva) a los datos procesados.

SOFTWARE: Equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

TELECOMUNICACIONES: Proceso que consiste en transmitir e intercambiar mensajes de un punto a otro

TIC: (Tecnologías de la Información y las Comunicaciones) son un concepto muy asociado al de informática. Si se entiende esta última como el conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información.

6. BIBLIOGRAFÍA/ WEBGRAFÍA

Costas, S. J. (2011). Seguridad Informática. Editorial Ra-Ma. España.

Gómez V., Á. (2011). Seguridad informática: Básico. ECOE Ediciones, Bogotá.

Villarrubia, C. (Sin fecha). Seguridad y Alta disponibilidad adopción de pautas de seguridad informática. Consultado el 30 de noviembre en:

<http://arco.esi.uclm.es/~david.villa/seguridad/pautas.2x4.pdf>

Tanenbaum, A. (2003). Redes de Computadoras. Pearson Educación, México. Consultado el 26 de noviembre de 2013 en:



SERVICIO NACIONAL DE APRENDIZAJE
SISTEMA INTEGRADO DE GESTIÓN
Procedimiento Creación y Adecuación de Programas de
Formación Virtual y a Distancia
Guía de Aprendizaje para el Programa de Formación
Complementaria Virtual

Versión: 01
Fecha: 08-10-2013
Código: G001-
P002-GFPI

<http://www.fedora-es.com/manuales/redes/tanenbaum.pdf>

7. CONTROL DEL DOCUMENTO (ELABORADA POR)

Autores:

Expertos temáticos

Juan José Botello Castellanos

Centro Industrial de Mantenimiento Integral. Girón (Santander)

Julio de 2015

Asesores pedagógicos

Elsa Cristina Arenas Martínez

Juan José Botello Castellanos

Centro Industrial de Mantenimiento Integral. Girón (Santander)

Julio de 2015

Líder Línea de Producción Santander

Santiago Lozada Garcés

Centro Industrial de Mantenimiento Integral. Girón (Santander)

Julio de 2015